vce trainer

cisa.vce

CISA

CISA

Certified Information Systems Auditor

Version 14.0

Score: 800/1000

Version:

Time Limit: 120 Minutes

Licensed to Berend Post berend.post@it-university.nl

Exam A (2791 questions)

Question 1

Which of the following BEST describes the relationship between vulnerability scanning and penetration testing?

- ☐ For entities with regulatory drivers the two tests must be the same.
- ☐ Both are labor-intensive in preparation, planning and execution.
- ☐ Both utilize a risk-based analysis that considers treats scenarios.
- ☐ The scope of both is determined primarily by the likelihood of exploitation.

Question 2

During an audit, an IS auditor notes that an organization's business continuity plan (BCP) does not adequately address information confidentiality during a recovery process. The IS auditor should recommend that the plan be modified to include:

- ☐ the level of information security required when business recovery procedures are invoked.
- ☐ information security roles and responsibilities in the crisis management structure.
- ☐ information security resource requirements.
- ☐ change management procedures for information security that could affect business continuity arrangements.

Question 3

Which of the following metrics BEST evaluates the completeness of disaster-recovery preparations?

- ☐ Number of published applications-recovery plans
- ☐ Ratio of successful to unsuccessful tests
- ☐ Ratio of recovery-plan documents to total applications
- ☐ Ratio of tested application to total applications

Question 4

There are several methods of providing telecommunications continuity. The method of routing traffic through split cable or duplicate cable facilities is called:

- ☐ alternative routing.
- ☐ diverse routing.
- ☐ long-haul network diversity.
- ☐ last-mile circuit protection.

Licensed to Berend Post berend.post@it-university.nl

Question 5

To restore service at a large processing facility after a disaster, which of the following tasks should be performed FIRST?

- ☐ Launch the emergency action team.
- ☐ Inform insurance company agents.
- ☐ Contact equipment vendors.
- ☐ Activate the reciprocal agreement.

Question 6

Which of the following is the BEST approach to identify whether a vulnerability is actively being exploited?

- ☐ Implement key performance indicators (KPIs).
- ☐ Conduct a penetration test.
- ☐ Review service desk reports.
- ☐ Perform log analysis.

Question 7

The demilitarized zone (DMZ) is the part of a network where servers that are placed are:

- ☐ running internal department applications.
- ☐ running mission-critical, non-web applications.
- ☐ interacting with the public Internet.
- ☐ external to the organization.

Question 8

Which of the following should an IS auditor recommend be done FIRST upon learning that new data protection legislation may affect the organization?

- ☐ Implement data protection best practices
- ☐ Implement a new security baseline for achieving compliance
- ☐ Restrict system access for noncompliant business processes
- ☐ Perform a gap analysis of data protection practices

Question 9

Which of the following needs be established FIRST in order to categorize data properly?

- ☐ A data protection policy
- ☐ A data classification framework
- ☐ A data asset inventory
- ☐ A data asset protection standard

Licensed to Berend Post berend.post@it-university.nl

Question 10

An IS auditor should ensure that an application's audit trail:

- ☐ has adequate security
- ☐ does not impact operational efficiency.
- ☐ is accessible online.
- ☐ logs all database records.

Question 11

You may reduce a cracker's chances of success by (choose all that apply):

- ☐ keeping your systems up to date using a security scanner.
- ☐ hiring competent people responsible for security to scan and update your systems.
- ☐ using multiple firewalls.
- ☐ using multiple firewalls and IDS.
- ☐ None of the choices.

Question 12

Which of the following statement correctly describes one way SSL authentication between a client (e.g. browser) and a server (e.g. web server)?

- ☐ Only the server is authenticated while client remains unauthenticated
- ☐ Only the client is authenticated while server remains authenticated
- ☐ Client and server are authenticated
- ☐ Client and server are unauthenticated

Question 13

What would be an IS auditor's GREATEST concern when using a test environment for an application audit?

- ☐ Test and production environments lack data encryption.
- ☐ Developers have access to the test environment.
- ☐ Retention period of test data has been exceeded.
- ☐ Test and production environments do not mirror each other.

Licensed to Berend Post berend.post@it-university.nl

Question 14

Which of the following is appropriate when an IS auditor is conducting an exit meeting with senior management?

- ☐ Eliminate significant findings where audit and management agree on risk acceptance.
- ☐ Agree with senior management on the risk grading of the audit report.
- ☐ Document written responses from management along with an implementation plan.
- ☐ Escalate disputed recommendations to the audit committee.

Question 15

Which of the following controls is MOST appropriate against brute force attacks at login?

- ☐ Storing password files using one-way encryption
- ☐ Locking the account after three invalid passwords
- ☐ Storing passwords under a one-way hash function
- ☐ Increasing the minimum password length to 10 characters

Question 16

Which testing approach is MOST appropriate to ensure that internal application interface errors are identified as soon as possible?

- ☐ Bottom up
- ☐ Sociability testing
- ☐ Top-down
- ☐ System test

Question 17

Which of the following would MOST likely impact the integrity of a database backup?

- ☐ Record fields contain null information
- ☐ Open database files during backup
- ☐ Relational database model used
- ☐ Backing up the database to an optical disk

Question 18

Which of the following security processes will BEST prevent the exploitation of system vulnerabilities?

- ☐ Patch management
- ☐ Log monitoring
- ☐ Antivirus software
- ☐ Intrusion detection

Licensed to Berend Post berend.post@it-university.nl

Question 19

Which of the following technique is used for speeding up network traffic flow and making it easier to manage?

- ☐ Point-to-point protocol
- ☐ X.25
- ☐ MPLS
- ☐ ISDN

Question 20

An IS auditor determines that an online retailer processing credit card information does not have a data classification process. The auditor's NEXT step should be to:

- ☐ recommend encryption of all sensitive data at rest
- ☐ determine existing controls around sensitive data
- ☐ recommend the implementation of data loss prevention (DLP) tools
- ☐ inquire if there have been any data loss incidents

Question 21

Which of the following is the BEST approach to verify that internal help desk procedures are executed in compliance with policies?

- ☐ Benchmark help desk procedures.
- ☐ Interview end users.
- ☐ Test a sample of closed tickets.
- ☐ Evaluate help desk call metrics.

Question 22

Which should be reviewed FIRST by an IS auditor to ensure that data is being secured appropriately for an application?

- ☐ Data classification
- ☐ Data encryption
- ☐ Data access
- ☐ Data storage

Licensed to Berend Post berend.post@it-university.nl

Question 23

An information security manager reads a media report of a new type of malware attack. Who should be notified FIRST?

- ☐ Security operations team
- ☐ Data owners
- ☐ Communications department
- ☐ Application owners

Question 24

When using public key encryption to secure data being transmitted across a network:

- ☐ both the key used to encrypt and decrypt the data are public.
- ☐ the key used to encrypt is private, but the key used to decrypt the data is public.
- ☐ the key used to encrypt is public, but the key used to decrypt the data is private.
- ☐ both the key used to encrypt and decrypt the data are private.

Question 25

An IS auditor evaluates the test results of a modification to a system that deals with payment computation. The auditor finds that 50 percent of the calculations do not match predetermined totals. Which of the following would MOST likely be the next step in the audit?

- ☐ Design further tests of the calculations that are in error.
- ☐ Identify variables that may have caused the test results to be inaccurate.
- ☐ Examine some of the test cases to confirm the results.
- ☐ Document the results and prepare a report of findings, conclusions and recommendations.

Question 26

Which of the following procedures should be implemented prior to disposing of surplus computer equipment to employees?

- ☐ Use operating system commands to delete all files from the hard drive.
- ☐ Have the employee receiving the machine sign a nondisclosure agreement.
- ☐ Use application delete commands to remove files.
- ☐ Overwrite the hard drive with random data.

Licensed to Berend Post berend.post@it-university.nl

Question 27

Which of the following layer of the OSI model provides a standard interface for applications to communicate with devices on a network?

- ☐ Application layer
- ☐ Presentation layer
- ☐ Session layer
- ☐ Transport layer

Question 28

The CIO of an organization is concerned that the information security policies may not be comprehensive. Which of the following should an IS auditor recommend be performed FIRST?

- ☐ Obtain a copy of their competitor's policies.
- ☐ Determine if there is a process to handle exceptions to the policies.
- ☐ Establish a governance board to track compliance with the policies.
- ☐ Compare the policies against an industry framework.

Question 29

Which of the following attack could be avoided by creating more security awareness in the organization and provide adequate security knowledge to all employees?

- ☐ surf attack
- ☐ Traffic analysis
- ☐ Phishing
- ☐ Interrupt attack

Question 30

Which of the following findings should be an IS auditor's GREATEST concern when reviewing an organization's purchase of new IT infrastructure hardware?

- ☐ The new infrastructure arrived with default system settings.
- ☐ The new infrastructure has residual risk within the organization's risk tolerance.
- ☐ The new infrastructure's hardening requirements are stronger than required by policy.
- ☐ The new infrastructure has compatibility issues with existing systems.

Licensed to Berend Post berend.post@it-university.nl

Question 31

Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?

- ☐ Mobile
- ☐ Redundant
- ☐ Shared
- ☐ Warm

Question 32

Which of the following database controls would ensure that the integrity of transactions is maintained in an online transaction processing system's database?

- ☐ Authentication controls
- ☐ Data normalization controls
- ☐ Read/write access log controls
- ☐ Commitment and rollback controls

Question 33

When should an application-level edit check to verify that availability of funds was completed at the electronic funds transfer (EFT) interface?

- ☐ Before transaction completion
- ☐ Immediately after an EFT is initiated
- ☐ During run-to-run total testing
- ☐ Before an EFT is initiated

Question 34

Which of the following is the PRIMARY reason for database optimization in an environment with a high volume of transactions?

- ☐ Improving availability
- ☐ Maintaining integrity
- ☐ Preventing data leakage
- ☐ Improving performance

Licensed to Berend Post berend.post@it-university.nl

Question 35

Which of the following refers to a primary component of corporate risk management with the goal of minimizing the risk of prosecution for software piracy due to use of unlicensed software?

- ☐ Software audit
- ☐ System audit
- ☐ Application System audit
- ☐ Test audit
- ☐ Mainframe audit
- ☐ None of the choices.

Question 36

The GREATEST risk when performing data normalization is:

- ☐ the increased complexity of the data model
- ☐ duplication of audit logs
- ☐ reduced data redundancy
- ☐ decreased performance

Question 37

Which of the following BEST reduces the likelihood of leakage of private information via email?

- ☐ Strong user authentication protocols
- ☐ Email encryption
- ☐ Prohibition on the personal use of email
- ☐ User awareness training

Question 38

Which of the following protocol is used for electronic mail service?

- ☐ DNS
- ☐ FTP
- ☐ SSH
- ☐ SMTP

Licensed to Berend Post berend.post@it-university.nl

Question 39

Which of the following is BEST characterized by unauthorized modification of data before or during systems data entry?

- ☐ Data diddling
- ☐ Skimming
- ☐ Data corruption
- ☐ Salami attack

Question 40

Which of the following tests performed by an IS auditor would be the MOST effective in determining compliance with an organization's change control procedures?

- ☐ Review software migration records and verify approvals.
- ☐ identify changes that have occurred and verify approvals.
- ☐ Review change control documentation and verify approvals.
- ☐ Ensure that only appropriate staff can migrate changes into production.

Question 41

Which of the following will BEST ensure the successful offshore development of business applications?

- ☐ Stringent contract management practices
- ☐ Detailed and correctly applied specifications
- ☐ Awareness of cultural and political differences
- ☐ Post implementation reviews

Question 42

With Deep packet inspection, which of the following OSI layers are involved?

- ☐ Layer 2 through Layer 7
- ☐ Layer 3 through Layer 7
- ☐ Layer 2 through Layer 6
- ☐ Layer 3 through Layer 6
- ☐ Layer 2 through Layer 5
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 43

An IS auditor reviewing an incident management process identifies client information was lost due to ransomware attacks. Which of the following would MOST effectively minimize the impact of future occurrences?

- ☐ Change access to client data to read-only.
- ☐ Improve the ransomware awareness program.
- ☐ Back up client data more frequently.
- ☐ Monitor all client data changes.

Question 44

What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources?

- ☐ OSI Layer 2 switches with packet filtering enabled
- ☐ Virtual Private Networks
- ☐ Access Control Lists (ACL)
- ☐ Point-to-Point Tunneling Protocol

Question 45

IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

- ☐ desired result or purpose of implementing specific control procedures.
- ☐ best IT security control practices relevant to a specific entity.
- ☐ techniques for securing information.
- ☐ security policy.

Question 46

Who is responsible for providing technical support for the hardware and software environment by developing, installing and operating the requested system?

- ☐ System Development Management
- ☐ Quality Assurance
- ☐ User Management
- ☐ Senior Management

Licensed to Berend Post berend.post@it-university.nl

Question 47

The logical exposure associated with the use of a checkpoint restart procedure is:

- ☐ denial of service.
- ☐ an asynchronous attack
- ☐ wire tapping.
- ☐ computer shutdown.

Question 48

Which of the following is the BEST compensating control for a lack of proper segregation of duties in an IT department?

- ☐ Authorization forms
- ☐ Audit trail reviews
- ☐ System activity logging
- ☐ Control self-assessment (CSA)

Question 49

At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:

- ☐ report the error as a finding and leave further exploration to the auditee's discretion.
- ☐ attempt to resolve the error.
- ☐ recommend that problem resolution be escalated.
- ☐ ignore the error, as it is not possible to get objective evidence for the software error.

Question 50

The MAIN reason for requiring that all computer clocks across an organization be synchronized is to:

- ☐ prevent omission or duplication of transactions.
- ☐ ensure smooth data transition from client machines to servers.
- ☐ ensure that e-mail messages have accurate time stamps.
- ☐ support the incident investigation process.

Question 51

Which of the following is the MOST effective way for an organization to protect against data leakage?

- ☐ Conduct periodic security awareness training.
- ☐ Limit employee Internet access.
- ☐ Review firewall logs for anomalies.
- ☐ Develop a comprehensive data loss prevention policy.

Licensed to Berend Post berend.post@it-university.nl

Question 52

After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

- ☐ Project management and progress reporting is combined in a project management office which is driven by external consultants.
- ☐ The replacement effort consists of several independent projects without integrating the resource allocation in a portfolio management approach.
- ☐ The resources of each of the organizations are inefficiently allocated while they are being familiarized with the other company's legacy systems.
- ☐ The new platform will force the business areas of both organizations to change their work processes, which will result in extensive training needs.

Question 53

An IS auditor will be testing accounts payable controls by performing data analytics on the entire population transactions. Which of the following is MOST important for the auditor to confirm when sourcing the population data?

- ☐ There is no privacy information in the data.
- ☐ The data analysis tools have been recently updated.
- ☐ The data can be obtained in a timely manner.
- ☐ The data is taken directly from the system.

Question 54

While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The MOST important concern for an IS auditor is the:

- ☐ effectiveness of the QA function because it should interact between project management and user management
- ☐ efficiency of the QA function because it should interact with the project implementation team.
- ☐ effectiveness of the project manager because the project manager should interact with the QA function.
- ☐ efficiency of the project manager because the QA function will need to communicate with the project implementation team.

Licensed to Berend Post berend.post@it-university.nl

Question 55

From a control perspective, the key element in job descriptions is that they:

- ☐ provide instructions on how to do the job and define authority.
- ☐ are current, documented and readily available to the employee.
- ☐ communicate management's specific job performance expectations.
- ☐ establish responsibility and accountability for the employee's actions.

Question 56

Which of the following statement INCORRECTLY describes packet switching technique?

- ☐ Packet uses many different dynamic paths to get the same destination
- ☐ Traffic is usually burst in nature
- ☐ Fixed delays to reach each packet to destination
- ☐ Usually carries data-oriented data

Question 57

Which of the following cryptography options would increase overhead/cost?

- ☐ The encryption is symmetric rather than asymmetric.
- ☐ A long asymmetric encryption key is used.
- ☐ The hash is encrypted rather than the message.
- ☐ A secret key is used.

Question 58

Management decided to accept the residual risk of an audit finding and not take the recommended actions. The internal audit team believes the acceptance is inappropriate and has discussed the situation with executive management. After this discussion, there is still disagreement regarding the decision. Which of the following is the BEST course of action by internal audit?

- ☐ Report this matter to the audit committee without notifying executive management.
- ☐ Document in the audit report that management has accepted the residual risk and take no further actions.
- ☐ Report the issue to the audit committee in a joint meeting with executive management for resolution.
- ☐ Schedule another meeting with executive management to convince them of taking action as recommended.

Licensed to Berend Post berend.post@it-university.nl

Question 59

An IS auditor intends to accept a management position in the data processing department within the same organization. However, the auditor is currently working on an audit of a major application and has not yet finished the report. Which of the following would be the BEST step for the IS auditor to take?

- ☐ Start in the position and inform the application owner of the job change.
- ☐ Start in the position immediately.
- ☐ Disclose this issue to the appropriate parties.
- ☐ Complete the audit without disclosure and then start in the position.

Question 60

What is the GREATEST concern for an IS auditor reviewing contracts for licensed software that executes a critical business process?

- ☐ Software escrow was not negotiated.
- ☐ An operational level agreement (OLA) was not negotiated.
- ☐ The contract does not contain a right-to-audit clause.
- ☐ Several vendor deliverables missed the commitment date.

Question 61

Which of the following is the GREATEST risk associated with in-house program development and customization?

- ☐ The lack of a test environment
- ☐ The lack of a quality assurance function
- ☐ The lack of secure coding expertise
- ☐ The lack of documentation for programs developed.

Question 62

An organization was recently notified by its regulatory body of significant discrepancies in its reporting data. A preliminary investigation revealed that the discrepancies were caused by problems with the organization's data quality. Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be advisors to the process. To ensure that management concerns are addressed, which data set should internal audit recommend be reviewed FIRST?

- ☐ Data impacting business objectives
- ☐ Data supporting financial statements
- ☐ Data reported to the regulatory body
- ☐ Data with customer personal information

Licensed to Berend Post berend.post@it-university.nl

Question 63

Which of the following would represent an acceptable test of an organization's business continuity plan (BCP)?

- ☐ Benchmarking the plan against similar organizations
- ☐ Paper test involving functional areas
- ☐ Full test of computer operations at an emergency site
- ☐ Walk-through of the plan with technology suppliers

Question 64

The PRIMARY benefit of a centralized time server is that it:

- ☐ reduces individual time-of-day requests by client applications
- ☐ is required by password synchronization programs
- ☐ allows decentralized logs to be kept in synchronization
- ☐ decreases the likelihood of an unrecoverable systems failure

Question 65

The success of control self-assessment (CSA) highly depends on:

- ☐ having line managers assume a portion of the responsibility for control monitoring.
- ☐ assigning staff managers the responsibility for building, but not monitoring, controls.
- ☐ the implementation of a stringent control policy and rule-driven controls.
- ☐ the implementation of supervision and the monitoring of controls of assigned duties.

Question 66

While planning an audit, an assessment of risk should be made to provide:

- ☐ reasonable assurance that the audit will cover material items.
- ☐ definite assurance that material items will be covered during the audit work.
- ☐ reasonable assurance that all items will be covered by the audit.
- ☐ sufficient assurance that all items will be covered during the audit work.

Question 67

Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

- ☐ A neural network
- ☐ Database management software
- ☐ Management information systems
- ☐ Computer assisted audit techniques

Licensed to Berend Post berend.post@it-university.nl

Question 68

During an audit, the IS auditor finds that in many cases excessive rights were not removed from a system. Which of the following would be the auditor's BEST recommendation?

- ☐ IT security should regularly revoke excessive system rights.
- ☐ System administrators should ensure consistency of assigned rights.
- ☐ Line management should regularly review and request modification of access rights.
- ☐ Human resources should delete access rights of terminated employees.

Question 69

Which of the following is the MOST critical step prior to performing a network penetration test?

- ☐ Informing management of the potential risk involved with penetration testing
- ☐ Identifying a scanning tool for use in identifying vulnerabilities
- ☐ Communicating the location of the penetration test targets to management
- ☐ Reviewing the results of previous penetration tests

Question 70

The BEST method for assessing the effectiveness of a business continuity plan is to review the:

- ☐ plans and compare them to appropriate standards.
- ☐ results from previous tests.
- ☐ emergency procedures and employee training.
- ☐ offsite storage and environmental controls.

Question 71

While reviewing the project plan for a new system prior to go-live, an IS auditor notes that the project team has not documented a fallback plan. Which of the following would be the BEST go-live approach in this situation?

- ☐ Parallel processing
- ☐ Immediate cutover
- ☐ Real-time replication
- ☐ Load balancing

Licensed to Berend Post berend.post@it-university.nl

Question 72

To optimize an organization's business contingency plan (BCP), an IS auditor should recommend conducting a business impact analysis (BIA) in order to determine:

- ☐ the business processes that generate the most financial value for the organization and therefore must be recovered first.
- ☐ the priorities and order for recovery to ensure alignment with the organization's business strategy.
- ☐ the business processes that must be recovered following a disaster to ensure the organization's survival.
- ☐ he priorities and order of recovery which will recover the greatest number of systems in the shortest time frame.

Question 73

Which of the following is MOST important for an effective control self-assessment program?

- ☐ Determining the scope of the assessment
- ☐ Evaluating changes to the risk environment
- ☐ Understanding the business process
- ☐ Performing detailed test procedures

Question 74

A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual's experience and:

- ☐ length of service, since this will help ensure technical competence.
- ☐ age, as training in audit techniques may be impractical.
- ☐ IS knowledge, since this will bring enhanced credibility to the audit function.
- ☐ ability, as an IS auditor, to be independent of existing IS relationships.

Question 75

Which of the following should be the PRIMARY basis for prioritizing follow-up audits?

- ☐ Complexity of management's actions plans
- ☐ Recommendation from executive management
- ☐ Audit cycle defined in the audit plan
- ☐ Residual risk from the findings of previous audits

Licensed to Berend Post berend.post@it-university.nl

Question 76

Which of the following is the MOST appropriate responsibility of an IS auditor involved in a data center renovation project?

- ☐ Performing independent reviews of responsible parties engaged in the project
- ☐ Ensuring the project progresses as scheduled and milestones are achieved
- ☐ Performing day-to-day activities to ensure the successful completion of the project
- ☐ Providing sign off on the design of controls for the data center

Question 77

When auditing a quality assurance plan, an IS auditor should be MOST concerned if the:

- ☐ quality assurance function is separate from the programming function.
- ☐ SDLC is coupled with the quality assurance plan.
- ☐ quality assurance function is periodically reviewed by internal audit.
- ☐ scope of quality assurance activities is undefined.

Question 78

An audit team has a completed schedule approved by the audit committee. After starting some of the scheduled audits, executive management asked the team to immediately audit an additional process. There are not enough resources available to add the additional audit to the schedule. Which of the following is the BEST course of action?

- ☐ Revise the scope of scheduled audits.
- ☐ Propose a revised audit schedule.
- ☐ Approve overtime work to ensure the audit is completed.
- ☐ Consider scheduling the audit for the next period.

Question 79

During a vendor management database audit, an IS auditor identifies multiple instances of duplicate vendor records. In order to prevent recurrence of the same issue, which of the following would be the IS auditor's BEST recommendation to management?

- ☐ Perform system verification checks for unique data values on key fields.
- ☐ Request senior management approval of all new vendor details.
- ☐ Run system reports of full vendor listings periodically to identify duplication.
- ☐ Build a segregation of duties control into the vendor creation process.

Licensed to Berend Post berend.post@it-university.nl

Question 80

The information in the knowledge base can be expressed in several ways. Which of the following way uses questionnaires to lead the user through a series of choices until a conclusion is reached?

- ☐ Decision tree
- ☐ Rules
- ☐ Semantic nets
- ☐ Knowledge interface

Question 81

When reviewing an end-user computing (EUC) application, which of the following techniques is MOST appropriate for testing program logic?

- ☐ Integrated testing facility
- ☐ Test decking
- ☐ Re-performance
- ☐ Key calculation inspection

Question 82

An IS auditor doing penetration testing during an audit of internet connections would:

- ☐ evaluate configurations.
- ☐ examine security settings.
- ☐ ensure virus-scanning software is in use.
- ☐ use tools and techniques available to a hacker.

Question 83

To determine who has been given permission to use a particular system resource, an IS auditor should review:

- ☐ activity lists.
- ☐ access control lists.
- ☐ logon ID lists.
- ☐ password lists.

Question 84

What is the purpose of a hypervisor?

- ☐ Monitoring the performance of virtual machines
- ☐ Cloning virtual machines
- ☐ Deploying settings to multiple machines simultaneously
- ☐ Running the virtual machine environment

Licensed to Berend Post berend.post@it-university.nl

Question 85

Which of the following refers to a symmetric key cipher which operates on fixedlength groups of bits with an unvarying transformation?

- ☐ stream cipher
- ☐ block cipher
- ☐ check cipher
- ☐ string cipher
- ☐ None of the choices.

Question 86

The IS auditor learns that when equipment was brought into the data center by a vendor, the emergency power shutoff switch was accidentally pressed and the UPS was engaged. Which of the following audit recommendations should the IS auditor suggest?

- ☐ Relocate the shut off switch.
- ☐ Install protective covers.
- ☐ Escort visitors.
- ☐ Log environmental failures.

Question 87

While observing a full simulation of the business continuity plan, an IS auditor notices that the notification systems within the organizational facilities could be severely impacted by infra structural damage. The BEST recommendation the IS auditor can provide to the organization is to ensure:

- ☐ the salvage team is trained to use the notification system.
- ☐ the notification system provides for the recovery of the backup.
- ☐ redundancies are built into the notification system.
- ☐ the notification systems are stored in a vault.

Question 88

Which of the following would be MOST helpful when assessing how applications exchange data with other applications?

- ☐ List of servers and their applications
- ☐ Entity relationship diagram
- ☐ Results of a risk assessment on the applications
- ☐ Configuration management database

Licensed to Berend Post berend.post@it-university.nl

Question 89

An IS auditor is conducting a follow-up internal IS audit and determines that several recommendations from the prior year have not been implemented. Which of the following should be the auditor's FIRST course of action?

- ☐ Evaluate the recommendations in context of the current IT environment.
- ☐ Continue the audit and disregard prior audit recommendations.
- ☐ Request management implement recommendations from the prior year.
- ☐ Add unimplemented recommendations as findings for the new audit.

Question 90

Which of the following is MOST critical to include when developing a data loss prevention (DLP) policy?

- ☐ Identification of the relevant network channels requiring protection
- ☐ Identification of the users, groups and roles to whom the policy will apply
- ☐ Identification of enforcement actions
- ☐ Identification of the content to protect

Question 91

Performance of a biometric measure is usually referred to in terms of (Choose three.):

- ☐ failure to reject rate
- ☐ false accept rate
- ☐ false reject rate
- ☐ failure to enroll rate
- ☐ None of the choices.

Question 92

There are many firewall implementations provided by firewall manufacturers. Which of the following implementation utilize two packet filtering routers and a bastion host? This approach creates the most secure firewall system since it supports network and application level security while defining a separate DMZ.

- ☐ Dual Homed firewall
- ☐ Screened subnet firewall
- ☐ Screened host firewall
- ☐ Anomaly based firewall

Licensed to Berend Post berend.post@it-university.nl

Question 93

Which of the following situations would increase the likelihood of fraud?

- ☐ Application programmers are implementing changes to production programs.
- ☐ Application programmers are implementing changes to test programs.
- ☐ Operations support staff are implementing changes to batch schedules.
- ☐ Database administrators are implementing changes to data structures.

Question 94

Which of the following type of testing has two major categories: QAT and UAT?

- ☐ Interface testing
- ☐ Unit Testing
- ☐ System Testing
- ☐ Final acceptance testing

Question 95

Which of the following would provide the MOST assurance that an application will work in a live environment?

- ☐ Walking through the programs to view the results of error processing
- ☐ Processing of test data to prove that data can be passed between individual programs
- ☐ Walking through the programs to view the results of processing copies of production data.
- ☐ Processing of valid and erroneous data in an acceptance test environment

Question 96

The computer security incident response team (CSIRT) of an organization disseminates detailed descriptions of recent threats. An IS auditor's GREATEST concern should be that the users might:

- ☐ use this information to launch attacks.
- ☐ forward the security alert.
- ☐ implement individual solutions.
- ☐ fail to understand the threat.

Licensed to Berend Post berend.post@it-university.nl

Question 97

What can be used to help identify and investigate unauthorized transactions?

- ☐ Postmortem review
- ☐ Reasonableness checks
- ☐ Data-mining techniques
- ☐ Expert systems

Question 98

An organization recently experienced a phishing attack that resulted in a breach of confidential information. Which of the following would be MOST relevant for an IS auditor to review when determining the root cause of the incident?

- ☐ Email configurations
- ☐ Simple mail transfer protocol (SMTP) logging
- ☐ Browser configurations
- ☐ Audit logging

Question 99

While performing a risk-based audit, which of the following would BEST enable an IS auditor to identify and categorize risk?

- ☐ Understanding the control framework
- ☐ Developing a comprehensive risk model
- ☐ Understanding the business environment
- ☐ Adopting qualitative risk analysis

Question 100

When migrating critical systems to a cloud provider, the GREATEST data security concern for an organization would be that data from different clients may be:

- ☐ subject to different service level agreements (SLAs) for disaster recovery.
- ☐ subject to varying government compliance regulations.
- ☐ improperly separated from each other.
- ☐ requested during a legal discovery process.

Licensed to Berend Post berend.post@it-university.nl

Question 101

An organization is implementing an enterprise resource planning (ERP) application to meet its business objectives. Of the following, who is PRIMARILY responsible for overseeing the project in order to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results?

- ☐ Project sponsor
- ☐ System development project team (SPDT)
- ☐ Project steering committee
- ☐ User project team (UPT)

Question 102

Which of the following would BEST enable effective decision-making?

- ☐ Annualized loss estimates determined from past security events.
- ☐ A universally applied list of generic threats impacts, and vulnerabilities
- ☐ Formalized acceptance of risk analysis by business management
- ☐ A consistent process to analyze new and historical information risk

Question 103

Which of the following validation techniques would BEST prevent duplicate electronic vouchers?

- ☐ Cyclic redundancy check
- ☐ Edit check
- ☐ Reasonableness check
- ☐ Sequence check

Question 104

When auditing a proxy-based firewall, an IS auditor should:

- ☐ verify that the firewall is not dropping any forwarded packets.
- ☐ review Address Resolution Protocol (ARP) tables for appropriate mapping between media access control (MAC) and IP addresses.
- ☐ verify that the filters applied to services such as HTTP are effective.
- ☐ test whether routing information is forwarded by the firewall.

Licensed to Berend Post berend.post@it-university.nl

Question 105

An organization is considering outsourcing the processing of customer insurance claims. An IS auditor notes that customer data will be sent offshore for processing. Which of the following would be the BEST way to address the risk of exposing customer data?

- ☐ Require background checks on all service provider personnel involved in the processing of data.
- ☐ Recommend the use of a service provider within the same country as the organization.
- ☐ Consider whether the service provider has the ability to meet service level agreements (SLAs).
- ☐ Assess whether the service provider meets the organization's data protection policies.

Question 106

Disabling which of the following would make wireless local area networks more secure against unauthorized access?

- ☐ MAC (Media Access Control) address filtering
- ☐ WPA (Wi-Fi Protected Access Protocol)
- ☐ LEAP (Lightweight Extensible Authentication Protocol)
- ☐ SSID (service set identifier) broadcasting

Question 107

An organization has performance metrics to track how well IT resources are being used, but there has been little progress on meeting the organization's goals. Which of the following would be MOST helpful to determine the underlying reason?

- ☐ Conducting a root cause analysis
- ☐ Re-evaluating organizational goals
- ☐ Re-evaluating key performance indicators (KPIs)
- ☐ Conducting a business impact analysis (BIA)

Question 108

To install backdoors, hackers generally prefer to use:

- ☐ either Trojan horse or computer worm.
- ☐ either Tripwire or computer virus.
- ☐ either eavedropper or computer worm.
- ☐ either Trojan horse or eavedropper.
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 109

Which of the following is critical to the successful establishment of an enterprise IT architecture?

- ☐ A well-defined data migration policy
- ☐ Comparison of the architecture with that of other organizations
- ☐ An architecture encompassing only critical systems
- ☐ Organizational support for standardization

Question 110

Which of the following would help to ensure the portability of an application connected to a database?

- ☐ Verification of database import and export procedures
- ☐ Usage of a structured query language (SQL)
- ☐ Analysis of stored procedures/triggers
- ☐ Synchronization of the entity-relation model with the database physical schema

Question 111

The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures:

- ☐ information assets are overprotected.
- ☐ a basic level of protection is applied regardless of asset value.
- ☐ appropriate levels of protection are applied to information assets.
- ☐ an equal proportion of resources are devoted to protecting all information assets.

Question 112

The GREATEST advantage of rapid application development (RAD) over the traditional system development life cycle (SDLC) is that it:

- ☐ facilitates user involvement.
- ☐ allows early testing of technical features.
- ☐ facilitates conversion to the new system.
- ☐ shortens the development time frame.

Licensed to Berend Post berend.post@it-university.nl

Question 113

Talking about biometric authentication, which of the following is often considered as a mix of both physical and behavioral characteristics?

- ☐ Voice
- ☐ Finger measurement
- ☐ Body measurement
- ☐ Signature
- ☐ None of the choices.

Question 114

If inadequate, which of the following would be the MOST likely contributor to a denial-of- service attack?

- ☐ Router configuration and rules
- ☐ Design of the internal network
- ☐ Updates to the router system software
- ☐ Audit testing and review techniques

Question 115

A benefit of quality of service (QoS) is that the:

- ☐ entire network's availability and performance will be significantly improved.
- ☐ telecom carrier will provide the company with accurate service-level compliance reports.
- ☐ participating applications will have guaranteed service levels.
- ☐ communications link will be supported by security controls to perform secure online transactions.

Question 116

Which of the following is MOST important when an incident may lead to prosecution?

- ☐ Impact analysis
- ☐ Timely incident detection
- ☐ Independent assessment
- ☐ Preservation of evidence

Licensed to Berend Post berend.post@it-university.nl

Question 117

When reviewing a digital certificate verification process, which of the following findings represents the MOST significant risk?

- ☐ There is no registration authority (RA) for reporting key compromises
- ☐ The certificate revocation list(CRL) is not current.
- ☐ Digital certificates contain a public key that is used to encrypt messages and verify digital signatures.
- ☐ Subscribers report key compromises to the certificate authority (CA).

Question 118

An organization's marketing department has requested access to cloud-based collaboration sites for exchanging media files with external marketing companies. As a result, the information security manager has been asked to perform a risk assessment. Which of the following should be the MOST important consideration?

- ☐ The information to be exchanged
- ☐ Methods for transferring the information
- ☐ Reputations of the external marketing companies
- ☐ The security of the third-party cloud provider

Question 119

An IT governance framework provides an organization with:

- ☐ a basis for directing and controlling IT.
- ☐ assurance that there will be IT cost reductions.
- ☐ organizational structures to enlarge the market share through IT.
- ☐ assurance that there are surplus IT investments.

Question 120

Which of the following is MOST important for an IS auditor to consider when determining an appropriate sample size in situations where selecting the entire population is not feasible?

- ☐ Tolerable error
- ☐ Accessibility of the data
- ☐ Data integrity
- ☐ Responsiveness of the auditee

Licensed to Berend Post berend.post@it-university.nl

Question 121

Which of the following methods would be MOST effective in verifying that all changes have been authorized?

- ☐ Reconciling problem tickets with authorized change control entries
- ☐ Reconciling reports of changes in production libraries to authorized change log entries
- ☐ Validating authorized change log entries with individual(s) who promoted into production
- ☐ Reconciling reports of changes in development libraries to supporting documentation

Question 122

Well-written risk assessment guidelines for IS auditing should specify which of the following elements at the least (Choose four.)

- ☐ A maximum length for audit cycles.
- ☐ The timing of risk assessments.
- ☐ Documentation requirements.
- ☐ Guidelines for handling special cases.
- ☐ None of the choices.

Question 123

Which of the following would be MOST important to include in a data security policy to adequately manage the privacy of customer information?

- ☐ Information classification criteria
- ☐ Encryption technology
- ☐ Backup strategy
- ☐ Data ownership

Question 124

What method might an IS auditor utilize to test wireless security at branch office locations?

- ☐ War dialing
- ☐ Social engineering
- ☐ War driving
- ☐ Password cracking

Licensed to Berend Post berend.post@it-university.nl

Question 125

A hardware control that helps to detect errors when data are communicated from one computer to another is known as a:

- ☐ duplicate check.
- ☐ table lookup.
- ☐ validity check.
- ☐ parity check.

Question 126

Which of the following would BEST enable alignment of IT with business objectives?

- ☐ Leveraging an IT framework
- ☐ Completing an IT risk assessment
- ☐ Adopting industry best practices
- ☐ Monitoring key performance indicators (KPIs)

Question 127

Which of the following would BEST prevent data from being orphaned?

- ☐ Referential integrity
- ☐ Table partitioning
- ☐ Input validation checks
- ☐ Table indexes

Question 128

During an audit of a telecommunications system, an IS auditor finds that the risk of intercepting data transmitted to and from remote sites is very high. The MOST effective control for reducing this exposure is:

- ☐ encryption.
- ☐ callback modems.
- ☐ message authentication.
- ☐ dedicated leased lines.

Licensed to Berend Post berend.post@it-university.nl

Question 129

Which of the following should be performed FIRST when preparing to deploy a major upgrade to a critical online application?

- ☐ Update the disaster recovery process.
- ☐ Update the business impact analysis (BIA).
- ☐ Test the rollback process.
- ☐ Review data backup procedures.

Question 130

Documentation of workaround processes to keep a business function operational during recovery of IT systems is a core part of a:

- ☐ business impact analysis (BIA).
- ☐ threat and risk assessment.
- ☐ business continuity plan (BCP).
- ☐ disaster recovery plan (DRP).

Question 131

Which of the following should an IS auditor recommend as MOST critical to an effective performance improvement process for IT services?

- ☐ Progress on performance goals is regularly reported to the board.
- ☐ The performance goals are aligned with a commonly accepted framework.
- ☐ Root cause analysis of service issues is used to develop performance goals.
- ☐ Management accepts accountability for achieving performance goals.

Question 132

Accountability for the maintenance of appropriate security measures over information assets resides with the:

- ☐ security administrator.
- ☐ systems administrator.
- ☐ data and systems owners.
- ☐ systems operations group.

Licensed to Berend Post berend.post@it-university.nl

Question 133

An IS auditor discovered that a firewall has more services than needed. The IS auditor's FIRST recommendation should be to:

- ☐ ensure logging is turned on.
- ☐ deploy a network penetration team.
- ☐ review configurations.
- ☐ eliminate services except for HTTPS.

Question 134

When developing a business continuity plan (BCP), which of the following tools should be used to gain an understanding of the organization's business processes?

- ☐ Business continuity self-audit
- ☐ Resource recovery analysis
- ☐ Risk assessment
- ☐ Gap analysis

Question 135

An IS auditor is reviewing a project to implement a payment system between a parent bank and a subsidiary. The IS auditor should FIRST verify that the:

- ☐ technical platforms between the two companies are interoperable.
- ☐ parent bank is authorized to serve as a service provider.
- ☐ security features are in place to segregate subsidiary trades.
- ☐ subsidiary can join as a co-owner of this payment system.

Question 136

Functionality is a characteristic associated with evaluating the quality of software products throughout their life cycle, and is BEST described as the set of attributes that bear on the:

- ☐ existence of a set of functions and their specified properties.
- ☐ ability of the software to be transferred from one environment to another.
- ☐ capability of software to maintain its level of performance under stated conditions.
- ☐ relationship between the performance of the software and the amount of resources used.

Licensed to Berend Post berend.post@it-university.nl

Question 137

Your final audit report should be issued:

- ☐ after an agreement on the observations is reached.
- ☐ before an agreement on the observations is reached.
- ☐ if an agreement on the observations cannot reached.
- ☐ without mentioning the observations.
- ☐ None of the choices.

Question 138

To develop meaningful recommendations for findings, which of the following is MOST important for an IS auditor to determine and understand?

- ☐ Criteria
- ☐ Responsible party
- ☐ Impact
- ☐ Root cause

Question 139

An IS auditor considering the risks associated with spooling sensitive reports for off-line printing will be the MOST concerned that:

- ☐ data can easily be read by operators
- ☐ data can more easily be amended by unauthorized persons
- ☐ unauthorized copies of reports can be printed
- ☐ output will be lost if the system should fail

Question 140

A substantive test to verify that tape library inventory records are accurate is:

- ☐ determining whether bar code readers are installed.
- ☐ determining whether the movement of tapes is authorized.
- ☐ conducting a physical count of the tape inventory.
- ☐ checking if receipts and issues of tapes are accurately recorded.

Question 141

Which of the following is an example of audit risk?

- ☐ Audit work may be lost due to a malware attack.
- ☐ Management may disagree with audit conclusions.
- ☐ Sampling methods may not detect a material error.
- ☐ Newer auditors may require additional supervision and training.

Licensed to Berend Post berend.post@it-university.nl

Question 142

A programmer has made unauthorized changes to key fields in a payroll system report. Which of the following control weaknesses would have contributed MOST to this problem?

- ☐ The user requirements were not documented.
- ☐ Payroll files were not under the control of a librarian.
- ☐ The programmer did not involve the user in testing.
- ☐ The programmer has access to the production programs.

Question 143

When evaluating the recent implementation of an intrusion detection system (IDS), an IS auditor should be MOST concerned with inappropriate:

- ☐ encryption.
- ☐ training.
- ☐ tuning.
- ☐ patching.

Question 144

An IS auditor has been asked to review a recently implemented quality management system (QMS). Which of the following should be the auditor's PRIMARY focus?

- ☐ Training materials prepared for coaching employees
- ☐ Processes to measure the performance of business critical transactions
- ☐ Documentation standard of the implemented QMS system
- ☐ Stability of the implemented QMS system over a period of time

Question 145

Which of the following could an IS auditor recommend to improve the estimated resources required in system development?

- ☐ Business areas involvement
- ☐ Prototyping
- ☐ Function point analysis
- ☐ CASE tools

Licensed to Berend Post berend.post@it-university.nl

Question 146

The MOST important factors in determining the scope and timing for testing a business continuity plan are:

- ☐ manual processing capabilities and the test location.
- ☐ the importance of the function to be tested and the cost of testing.
- ☐ the experience level of personnel and the function location.
- ☐ prior testing results and the degree of detail of the business continuity plan.

Question 147

Which of the following audit include specific tests of control to demonstrate adherence to specific regulatory or industry standard?

- ☐ Compliance Audit
- ☐ Financial Audit
- ☐ Operational Audit
- ☐ Forensic audit

Question 148

Which of the following should be an IS auditor's FIRST activity when planning an audit?

- ☐ Gain an understanding of the area to be audited.
- ☐ Document specific questions in the audit program.
- ☐ Create a list of key controls to be reviewed.
- ☐ Identify proper resources for audit activities.

Question 149

Electrical surge protectors BEST protect from the impact of:

- ☐ electromagnetic interference.
- ☐ power outages.
- ☐ sags and spikes
- ☐ reduced voltage.

Question 150

The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:

- ☐ rules.
- ☐ decision trees.
- ☐ semantic nets.
- ☐ dataflow diagrams.

Licensed to Berend Post berend.post@it-university.nl

Question 151

An audit charter should:

- ☐ be dynamic and change often to coincide with the changing nature of technology and the audit profession.
- ☐ clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal controls.
- ☐ document the audit procedures designed to achieve the planned audit objectives.
- ☐ outline the overall authority, scope and responsibilities of the audit function.

Question 152

Which of the following is the process of feeding test data into two systems – the modified system and alternative system and comparing the result?

- ☐ Parallel Test
- ☐ Black box testing
- ☐ Regression Testing
- ☐ Pilot Testing

Question 153

An audit committee is reviewing an annual IT risk assessment. Which of the following is the BEST justification for the audits selected?

- ☐ Likelihood of an IT process failure
- ☐ Key IT general process controls
- ☐ Applications impacted
- ☐ Underlying business risks

Question 154

The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:

- ☐ integrity.
- ☐ authenticity.
- ☐ authorization.
- ☐ nonrepudiation.

Licensed to Berend Post berend.post@it-university.nl

Question 155

Which of the following transmission media would NOT be affected by cross talk or interference?

- ☐ Copper cable
- ☐ Radio System
- ☐ Satellite radio link
- ☐ Fiber optic cables

Question 156

Which of the following is a control over component communication failure/errors?

- ☐ Restricting operator access and maintaining audit trails
- ☐ Monitoring and reviewing system engineering activity
- ☐ Providing network redundancy
- ☐ Establishing physical barriers to the data transmitted over the network

Question 157

After initial investigation, an IS auditor has reasons to believe that fraud may be present.
The IS auditor should:

- ☐ expand activities to determine whether an investigation is warranted
- ☐ report the matter to the audit committee.
- ☐ report the possibility of fraud to top management and ask how they would like to be proceed.
- ☐ consult with external legal counsel to determine the course of action to be taken.

Question 158

A company undertakes a business process reengineering (BPR) project in support of a new and direct marketing approach to its customers. Which of the following would be an IS auditor's main concern about the new process?

- ☐ Whether key controls are in place to protect assets and information resources
- ☐ If the system addresses corporate customer requirements
- ☐ Whether the system can meet the performance goals (time and resources)
- ☐ Whether owners have been identified who will be responsible for the process

Licensed to Berend Post berend.post@it-university.nl

Question 159

Which of the following statements pertaining to IPSec is incorrect?

- ☐ A security association has to be defined between two IPSec systems in order for bi-directional communication to be established.
- ☐ Integrity and authentication for IP datagrams are provided by AH.
- ☐ ESP provides for integrity, authentication and encryption to IP datagram's.
- ☐ In transport mode, ESP only encrypts the data payload of each packet.

Question 160

Which of the following exploit vulnerabilities to cause loss or damage to the organization and its assets?

- ☐ Exposures
- ☐ Threats
- ☐ Hazards
- ☐ Insufficient controls

Question 161

Which of the following is an advantage of the top-down approach to software testing?

- ☐ Interface errors are identified early
- ☐ Testing can be started before all programs are complete
- ☐ it is more effective than other testing approaches
- ☐ Errors in critical modules are detected sooner

Question 162

An organization with a maturing incident response program conducts post-incident reviews for all major information security incidents. The PRIMARY goal of these reviews should be to:

- ☐ identify security program gaps or systemic weaknesses that need correction.
- ☐ prepare properly vetted notifications regarding the incidents to external parties.
- ☐ identify who should be held accountable for the security incidents.
- ☐ document and report the root cause of the incidents for senior management.

Licensed to Berend Post berend.post@it-university.nl

Question 163

Which of the following statement correctly describes the difference between symmetric key encryption and asymmetric key encryption?

- ☐ In symmetric key encryption the same key is used for encryption and decryption where as asymmetric key uses private key for encryption and decryption
- ☐ In symmetric key encryption the public key is used for encryption and the symmetric key for decryption. Where as in asymmetric key encryption the public key is used for encryption and private key is used for decryption
- ☐ In symmetric key encryption the same key is used for encryption and decryption where as in asymmetric key encryption the public key is used for encryption and private key is used for decryption.
- ☐ Both uses private key for encryption and the decryption process can be done using public key

Question 164

Which of the following would be the BEST way for an information security manager to justify ongoing annual maintenance fees associated with an intrusion prevention system (IPS)?

- ☐ Perform industry research annually and document the overall ranking of the IPS.
- ☐ Perform a penetration test to demonstrate the ability to protect.
- ☐ Establish and present appropriate metrics that track performance.
- ☐ Provide yearly competitive pricing to illustrate the value of the IPS.

Question 165

Which of the following is the PRIMARY concern if a business continuity plan (BCP) is not based on a business impact analysis (BIA)?

- ☐ The critical systems were not identified, but all systems are covered in the BCP.
- ☐ The knowledge of key people within the organization was not considered in the BCP.
- ☐ The strategy of the BCP does not reflect estimated potential losses.
- ☐ Management was not involved in the early stages of the BCP.

Question 166

An IS auditor is assigned to review the development of a specific application. Which of the following would be the MOST significant step following the feasibility study?

- ☐ Attend project progress meetings to monitor timely implementation of the application.
- ☐ Assist users in the design of proper acceptance-testing procedures.
- ☐ Follow up with project sponsor for project's budgets and actual costs.
- ☐ Review functional design to determine that appropriate controls are planned.

Licensed to Berend Post berend.post@it-university.nl

Question 167

What are intrusion-detection systems (IDS) primarily used for?

- ☐ To identify AND prevent intrusion attempts to a network
- ☐ To prevent intrusion attempts to a network
- ☐ Forensic incident response
- ☐ To identify intrusion attempts to a network

Question 168

When reviewing print systems spooling, an IS auditor is MOST concerned with which of the following vulnerabilities?

- ☐ The potential for unauthorized deletion of report copies
- ☐ The potential for unauthorized modification of report copies
- ☐ The potential for unauthorized printing of report copies
- ☐ The potential for unauthorized editing of report copies

Question 169

Which of the following is the MOST important role of the information security manager when the organization is in the process of adopting emerging technologies?

- ☐ Understanding the impact on existing resources
- ☐ Assessing how peer organizations using the same technologies have been impacted
- ☐ Developing training for end users to familiarize them with the new technology
- ☐ Reviewing vendor documentation and service levels agreements

Question 170

Which of the following refers to an important procedure when evaluating database security?

- ☐ performing vulnerability assessments against the database.
- ☐ performing data check against the database.
- ☐ performing dictionary check against the database.
- ☐ performing capacity check against the database system.
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 171

Which of the following is MOST important for an organization to complete when planning a new marketing platform that targets advertising based on customer behavior?

- ☐ Data privacy impact assessment
- ☐ Data quality assessment
- ☐ Cross-border data transfer assessment
- ☐ Security vulnerability assessment

Question 172

What does PKI use to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions?

- ☐ A combination of public-key cryptography and digital certificates and two-factor authentication
- ☐ A combination of public-key cryptography and two-factor authentication
- ☐ A combination of public-key cryptography and digital certificates
- ☐ A combination of digital certificates and two-factor authentication

Question 173

After installing a network, an organization installed a vulnerability assessment tool or security scanner to identify possible weaknesses. Which is the MOST serious risk associated with such tools?

- ☐ Differential reporting
- ☐ False-positive reporting
- ☐ False-negative reporting
- ☐ Less-detail reporting

Question 174

Which of the following is the MOST reliable form of single factor personal identification?

- ☐ Smart card
- ☐ Password
- ☐ Photo identification
- ☐ iris scan

Licensed to Berend Post berend.post@it-university.nl

Question 175

In planning an audit, the MOST critical step is the identification of the:

- ☐ areas of high risk.
- ☐ skill sets of the audit staff.
- ☐ test steps in the audit.
- ☐ time allotted for the audit.

Question 176

While auditing an IT department's cloud service provider, the IS auditor found that privileged access monitoring is not being performed as required by the contract. The provider disagrees with this issue and noted that compensating controls are in place. The IS auditor's NEXT course of action should be to:

- ☐ test compensating controls as part of the audit.
- ☐ define a remediation plan.
- ☐ review privileged access logs.
- ☐ recommend revising the service level agreement (SLA).

Question 177

Ensuring that security and control policies support business and IT objectives is a primary objective of:

- ☐ An IT security policies audit
- ☐ A processing audit
- ☐ A software audit
- ☐ A vulnerability assessment

Question 178

An IS auditor auditing the effectiveness of utilizing a hot site will MOST likely:

- ☐ review reciprocal agreements.
- ☐ review logical access controls.
- ☐ evaluate physical access controls.
- ☐ analyze system restoration procedures.

Licensed to Berend Post berend.post@it-university.nl

Question 179

An IS auditor reviewing the implementation of an intrusion detection system (IDS) should be MOST concerned if:

- ☐ IDS sensors are placed outside of the firewall.
- ☐ a behavior-based IDS is causing many false alarms.
- ☐ a signature-based IDS is weak against new types of attacks.
- ☐ the IDS is used to detect encrypted traffic.

Question 180

When determining whether a project in the design phase will meet organizational objectives, what is BEST to compare against the business case?

- ☐ Project plan
- ☐ Requirements analysis
- ☐ Implementation plan
- ☐ Project budget provisions

Question 181

Which of the following terms generally refers to small programs designed to take advantage of a software flaw that has been discovered?

- ☐ exploit
- ☐ patch
- ☐ quick fix
- ☐ service pack
- ☐ malware
- ☐ None of the choices.

Question 182

Which of the following BEST demonstrates to an IS auditor that an organization has implemented effective risk management processes?

- ☐ Critical business assets have additional controls.
- ☐ The risk register is reviewed periodically.
- ☐ A business impact analysis (BIA) has been completed.
- ☐ The inventory of IT assets includes asset classification.

Licensed to Berend Post berend.post@it-university.nl

Question 183

An organization has implemented an enhanced password policy for business applications which requires significantly more business unit resources to support clients. The BEST approach to obtain the support of business unit management would be to:

- ☐ elaborate on the positive impact to information security.
- ☐ present industry benchmarking results to business units.
- ☐ discuss the risk and impact of security incidents if not implemented.
- ☐ present an analysis of the cost and benefit of the changes.

Question 184

The PRIMARY objective of a logical access control review is to:

- ☐ review access controls provided through software.
- ☐ ensure access is granted per the organization's authorities.
- ☐ walk through and assess the access provided in the IT environment.
- ☐ provide assurance that computer hardware is adequately protected against abuse.

Question 185

Which of the following is the BEST way for management to ensure the effectiveness of the cybersecurity incident response process?

- ☐ Periodic update of incident response process documentation
- ☐ Periodic reporting of cybersecurity incidents to key stakeholders
- ☐ Periodic tabletop exercises involving key stakeholders
- ☐ Periodic cybersecurity training for staff involved in incident response

Question 186

Which of the following types of firewalls would BEST protect a network from an internet attack?

- ☐ Screened subnet firewall
- ☐ Application filtering gateway
- ☐ Packet filtering router
- ☐ Circuit-level gateway

Licensed to Berend Post berend.post@it-university.nl

Question 187

A data leakage prevention (DLP) solution has identified that several employees are sending confidential company data to their personal email addresses in violation of company policy. The information security manager should FIRST:

- ☐ initiate an investigation to determine the full extent of noncompliance
- ☐ notify senior management that employees are breaching policy
- ☐ limit access to the Internet for employees involved
- ☐ contact the employees involved to retake security awareness training

Question 188

When implementing an upgraded ERP system, which of the following is the MOST important consideration for a go-live decision?

- ☐ Test cases
- ☐ Rollback strategy
- ☐ Business case
- ☐ Post-implementation review objectives

Question 189

A review of wide area network (WAN) usage discovers that traffic on one communication line between sites, synchronously linking the master and standby database, peaks at 96 percent of the line capacity. An IS auditor should conclude that:

- ☐ analysis is required to determine if a pattern emerges that results in a service loss for a short period of time.
- ☐ WAN capacity is adequate for the maximum traffic demands since saturation has not been reached.
- ☐ the line should immediately be replaced by one with a larger capacity to provide approximately 85 percent saturation.
- ☐ users should be instructed to reduce their traffic demands or distribute them across all service hours to flatten bandwidth consumption.

Question 190

Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?

- ☐ System analysis
- ☐ Authorization of access to data
- ☐ Application programming
- ☐ Data administration

Licensed to Berend Post berend.post@it-university.nl

Question 191

A company converted its payroll system from an external service to an internal package. Payroll processing in April was run in parallel. To validate the completeness of data after the conversion, which of the following comparisons from the old to the new system would be MOST effective?

- ☐ Turnaround time for payroll processing
- ☐ Employee counts and year-to-date payroll totals
- ☐ Master file employee data to payroll journals
- ☐ Cut-off dates and overwrites for a sample of employees

Question 192

When planning an audit of a network setup, an IS auditor should give highest priority to obtaining which of the following network documentation?

- ☐ Wiring and schematic diagram
- ☐ Users' lists and responsibilities
- ☐ Application lists and their details
- ☐ Backup and recovery procedures

Question 193

When conducting a follow-up audit on an organization's firewall configuration, the IS auditor discovered that the firewall had been integrated into a new system that provides both firewall and intrusion detection capabilities. The IS auditor should:

- ☐ consider the follow-up audit unnecessary since the firewall is no longer being used.
- ☐ assess whether the integrated system addresses the identified risk.
- ☐ review the compatibility of the new system with existing network controls.
- ☐ evaluate whether current staff is able to support the new system.

Question 194

Which of the following is the MOST important element when developing an information security strategy?

- ☐ Identifying applicable laws and regulations
- ☐ Identifying information assets
- ☐ Determining the risk management methodology
- ☐ Aligning security activities with organizational goals

Licensed to Berend Post berend.post@it-university.nl

Question 195

Which device acting as a translator is used to connect two networks or applications from layer 4 up to layer 7 of the ISO/OSI Model?

- ☐ Bridge
- ☐ Repeater
- ☐ Router
- ☐ Gateway

Question 196

Which of the following is the MOST secure and economical method for connecting a private network over the Internet in a small- to medium-sized organization?

- ☐ Virtual private network
- ☐ Dedicated line
- ☐ Leased line
- ☐ integrated services digital network

Question 197

Which of the following is the PRIMARY safeguard for securing software and data within an information processing facility?

- ☐ Security awareness
- ☐ Reading the security policy
- ☐ Security committee
- ☐ Logical access controls

Question 198

An IS auditor should expect the responsibility for authorizing access rights to production data and systems to be entrusted to the:

- ☐ process owners.
- ☐ system administrators.
- ☐ security administrator.
- ☐ data owners.

Licensed to Berend Post berend.post@it-university.nl

Question 199

Which of the following fire suppression systems is MOST appropriate to use in a data center environment?

- ☐ Wet-pipe sprinkler system
- ☐ Dry-pipe sprinkler system
- ☐ FM-200system
- ☐ Carbon dioxide-based fire extinguishers

Question 200

What should be the MAIN goal of an organization's incident response plan?

- ☐ Keep stakeholders notified of incident status.
- ☐ Enable appropriate response according to criticality.
- ☐ Correlate incidents from different systems.
- ☐ Identify the root cause of the incident.

Question 201

Which of the following layer in an enterprise data flow architecture derives enterprise information from operational data, external data and nonoperational data?

- ☐ Data preparation layer
- ☐ Data source layer
- ☐ Data mart layer
- ☐ Data access layer

Question 202

An IS auditor's PRIMARY concern about a business partner agreement for the exchange of electronic information should be to determine whether there is:

- ☐ a clause that addresses the audit of shared systems.
- ☐ evidence of review and approval by each partner's legal department.
- ☐ an information classification framework.
- ☐ appropriate control and responsibility defined for each partner.

Licensed to Berend Post berend.post@it-university.nl

Question 203

Wi-Fi Protected Access implements the majority of which IEEE standard?

- ☐ 802.11i
- ☐ 802.11g
- ☐ 802.11x
- ☐ 802.11v
- ☐ None of the choices.

Question 204

Identify the INCORRECT statement from below mentioned testing types

- ☐ Recovery Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems
- ☐ Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour
- ☐ Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process
- ☐ Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process

Question 205

The MOST important reason to use a centralized mechanism to identify information security incidents is to:

- ☐ prevent unauthorized changes to networks.
- ☐ comply with corporate policies.
- ☐ detect potential fraud.
- ☐ detect threats across environments.

Question 206

An IS auditor who is reviewing incident reports discovers that, in one instance, an important document left on an employee's desk was removed and put in the garbage by the outsourced cleaning staff. Which of the following should the IS auditor recommend to management?

- ☐ Stricter controls should be implemented by both the organization and the cleaning agency.
- ☐ No action is required since such incidents have not occurred in the past.
- ☐ A clear desk policy should be implemented and strictly enforced in the organization.
- ☐ A sound backup policy for all important office documents should be implemented.

Licensed to Berend Post berend.post@it-university.nl

Question 207

During a software acquisition review, an IS auditor should recommend that there be a software escrow agreement when:

- ☐ the estimated life for the product is less than 3 years.
- ☐ the deliverables do not include the source code.
- ☐ the product is new in the market.
- ☐ there is no service level agreement (SLA).

Question 208

What often results in project scope creep when functional requirements are not defined as well as they could be?

- ☐ Inadequate software baselining
- ☐ Insufficient strategic planning
- ☐ Inaccurate resource allocation
- ☐ Project delays

Question 209

Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?

- ☐ Sensitive data can be read by operators.
- ☐ Data can be amended without authorization.
- ☐ Unauthorized report copies can be printed.
- ☐ Output can be lost in the event of system failure.

Question 210

What is the FIRST line of defense against criminal insider activities?

- ☐ Validating the integrity of personnel
- ☐ Monitoring employee activities
- ☐ Signing security agreements by critical personnel
- ☐ Stringent and enforced access controls

Licensed to Berend Post berend.post@it-university.nl

Question 211

A successful risk-based IT audit program should be based on:

- ☐ an effective scoring system.
- ☐ an effective PERT diagram.
- ☐ an effective departmental brainstorm session.
- ☐ an effective organization-wide brainstorm session.
- ☐ an effective yearly budget.
- ☐ None of the choices.

Question 212

When an operating system is being hardened, it is MOST important for an information security manager to ensure that:

- ☐ default passwords are changed.
- ☐ anonymous access is removed.
- ☐ file access is restricted.
- ☐ system logs are activated.

Question 213

In a contract with a hot, warm or cold site, contractual provisions should cover which of the following considerations?

- ☐ Physical security measures
- ☐ Total number of subscribers
- ☐ Number of subscribers permitted to use a site at one time
- ☐ References by other users

Question 214

When an organization is having new software implemented under contract, which of the following is key to controlling escalating costs due to scope creep?

- ☐ Problem management
- ☐ Quality management
- ☐ Change management
- ☐ Risk management

Licensed to Berend Post berend.post@it-university.nl

Question 215

In which of the following situations is it MOST appropriate to implement data mirroring as the recovery strategy?

- ☐ Disaster tolerance is high.
- ☐ Recovery time objective is high.
- ☐ Recovery point objective is low.
- ☐ Recovery point objective is high.

Question 216

A purpose of project closure is to determine the:

- ☐ potential risks affecting the quality of deliverables.
- ☐ lessons learned for use in future projects.
- ☐ project feasibility requirements
- ☐ professional expertise of the project manager.

Question 217

An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

- ☐ User acceptance testing (UAT) occur for all reports before release into production
- ☐ Organizational data governance practices be put in place
- ☐ Standard software tools be used for report development
- ☐ Management sign-off on requirements for new reports

Question 218

Proper segregation of duties normally does not prohibit a LAN administrator from also having programming responsibilities. True or false?

- ☐ True
- ☐ False

Question 219

Which of the following is the MOST important reason for updating and retesting a business continuity plan?

- ☐ Staff turnover
- ☐ Emerging technology
- ☐ Significant business change
- ☐ Matching industry best practices

Licensed to Berend Post berend.post@it-university.nl

Question 220

The members of an emergency incident response team should be:

- ☐ selected from multiple departments
- ☐ assigned at the time of each incident
- ☐ restricted to IT personnel
- ☐ appointed by the CISO

Question 221

A post-implementation review of a system implementation has identified that the defined objectives were changed several times without the approval of the project board. What should the IS auditor do NEXT?

- ☐ Notify the project sponsor and request that the project be reopened.
- ☐ Ask management to obtain retrospective approvals.
- ☐ Notify the project management office and raise a finding.
- ☐ Determine whether the revised objectives are appropriate.

Question 222

When planning for the implementation of a new system, an organization will opt for a parallel run PRIMARILY to:

- ☐ ensure that the system meets required user response time.
- ☐ validate system processing.
- ☐ facilitate the training of new personnel.
- ☐ verify that system interfaces were implemented.

Question 223

After discovering a security vulnerability in a third-party application that interfaces with several external systems, a patch is applied to a significant number of modules. Which of the following tests should an IS auditor recommend?

- ☐ Stress
- ☐ Black box
- ☐ Interface
- ☐ System

Licensed to Berend Post berend.post@it-university.nl

Question 224

During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

- ☐ test data to validate data input.
- ☐ test data to determine system sort capabilities.
- ☐ generalized audit software to search for address field duplications.
- ☐ generalized audit software to search for account field duplications.

Question 225

Which of the following is an example of a passive attack initiated through the Internet?

- ☐ Traffic analysis
- ☐ Masquerading
- ☐ Denial of service
- ☐ E-mail spoofing

Question 226

To determine which users can gain access to the privileged supervisory state, which of the following should an IS auditor review?

- ☐ System access log files
- ☐ Enabled access control software parameters
- ☐ Logs of access control violations
- ☐ System configuration files for control options used

Question 227

Which of the following will BEST protect the confidentiality of data stored on the hard drive of a laptop computer?

- ☐ Encryption of the data
- ☐ A boot password
- ☐ Physical locks and alarms
- ☐ Biometric access control

Licensed to Berend Post berend.post@it-university.nl

Question 228

An organization has implemented a distributed security administration system to replace the previous centralized one. The IS auditor's GREATEST concern should be that:

- ☐ security procedures may be inadequate to support the change.
- ☐ end-user acceptance of the new system is likely to be difficult to obtain.
- ☐ the new system will require additional training.
- ☐ a distributed security system is inherently a weak security system.

Question 229

When recommending a preventive control against cross-site scripting in web applications, an information security manager is MOST likely to suggest:

- ☐ using https in place of http.
- ☐ hardening of the web server's operating system.
- ☐ consolidating multiple sites into a single portal.
- ☐ coding standards and code review.

Question 230

By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:

- ☐ reliable products are guaranteed.
- ☐ programmers' efficiency is improved.
- ☐ security requirements are designed.
- ☐ predictable software processes are followed.

Question 231

For an auditor, it is very important to understand the different forms of project organization and their implication in the control of project management activities. In which of the following project organization form is management authority shared between the project manager and the department head?

- ☐ Influence project organization
- ☐ Pure project organization
- ☐ Matrix project organization
- ☐ Forward project organization

Licensed to Berend Post berend.post@it-university.nl

Question 232

In what way is a common gateway interface (CGI) MOST often used on a webserver?

- ☐ Consistent way for transferring data to the application program and back to the user
- ☐ Computer graphics imaging method for movies and TV
- ☐ Graphic user interface for web design
- ☐ interface to access the private gateway domain

Question 233

Which of the following would be the GREATEST risk associated with a new chat feature on a retailer's website?

- ☐ Productivity loss
- ☐ Reputational damage
- ☐ Data loss
- ☐ System downtime

Question 234

Which of the following is a risk of cross-training?

- ☐ Increases the dependence on one employee
- ☐ Does not assist in succession planning
- ☐ One employee may know all parts of a system
- ☐ Does not help in achieving a continuity of operations

Question 235

To determine how data are accessed across different platforms in a heterogeneous environment, an IS auditor should FIRST review:

- ☐ business software.
- ☐ infrastructure platform tools.
- ☐ application services.
- ☐ system development tools.

Licensed to Berend Post berend.post@it-university.nl

Question 236

Physical access controls are usually implemented based on which of the following means (Choose two.):

- ☐ mechanical locks
- ☐ guards
- ☐ operating systems
- ☐ transaction applications
- ☐ None of the choices.

Question 237

An IS auditor is asked to review a large organization's change management process. Which of the following practices presents the GREATEST risk?

- ☐ Emergency code changes are promoted without user acceptance testing.
- ☐ A system administrator performs code migration on planned downtime.
- ☐ Change management tickets do not contain specific documentation.
- ☐ Transaction data changes can be made by a senior developer.

Question 238

An integrated test facility is considered a useful audit tool because it:

- ☐ is a cost-efficient approach to auditing application controls.
- ☐ enables the financial and IS auditors to integrate their audit tests.
- ☐ compares processing output with independently calculated data.
- ☐ provides the IS auditor with a tool to analyze a large range of information

Question 239

During audit planning, an IS auditor walked through the design of controls related to a new data loss prevention (DLP) tool. It was noted that the tool will be configured to alert IT management when large files are sent outside of the organization via email. What type of control will be tested?

- ☐ Detective
- ☐ Corrective
- ☐ Directive
- ☐ Preventive

Licensed to Berend Post berend.post@it-university.nl

Question 240

An IS auditor should be MOST concerned with what aspect of an authorized honeypot?

- ☐ The data collected on attack methods
- ☐ The information offered to outsiders on the honeypot
- ☐ The risk that the honeypot could be used to launch further attacks on the organization's infrastructure
- ☐ The risk that the honeypot would be subject to a distributed denial-of-service attack

Question 241

The FIRST step in a successful attack to a system would be:

- ☐ gathering information.
- ☐ gaining access.
- ☐ denying services.
- ☐ evading detection.

Question 242

The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

- ☐ IT budget.
- ☐ existing IT environment.
- ☐ business plan.
- ☐ investment plan.

Question 243

Which of the following testing procedure is used by the auditor during accounting audit to check errors in balance sheet and other financial documentation?

- ☐ Compliance testing
- ☐ Sanity testing
- ☐ Recovery testing
- ☐ Substantive testing

Licensed to Berend Post berend.post@it-university.nl

Question 244

IS audit is asked to explain how local area network (LAN) servers can contribute to a rapid dissemination of viruses. The IS auditor's BEST response is that:

- ☐ the server's software is the prime target and is the first to be infected.
- ☐ the server's operating system exchanges data with each station starting at every log-on.
- ☐ the server's file sharing function facilitates the distribution of files and applications.
- ☐ users of a given server have similar usage of applications and files.

Question 245

In a follow-up audit, an IS auditor notes that management has addressed the original findings in a different way than originally agreed upon. The auditor should FIRST:

- ☐ mark the recommendation as satisfied and close the finding
- ☐ verify if management's action mitigates the identified risk
- ☐ re-perform the audit to assess the changed control environment
- ☐ escalate the deviation to the audit committee

Question 246

What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality?

- ☐ Rapid application development (RAD)
- ☐ GANTT
- ☐ PERT
- ☐ Decision trees

Question 247

Identify the WAN message switching technique being used from the description presented below:

"Data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, this WAN switching technology stores and delays the message until ample resources become available for effective transmission of the message. "

- ☐ Message Switching
- ☐ Packet switching
- ☐ Circuit switching
- ☐ Virtual Circuits

Licensed to Berend Post berend.post@it-university.nl

Question 248

COBIT 5 separates information goals into three sub-dimensions of quality. Which of the following sub-dimension of COBIT 5 describes the extent to which data values are in conformance with the actual true value?

- ☐ Intrinsic quality
- ☐ Contextual and representational quality
- ☐ Security quality
- ☐ Accessibility quality

Question 249

The PRIMARY goal of a web site certificate is:

- ☐ authentication of the web site that will be surfed.
- ☐ authentication of the user who surfs through that site.
- ☐ preventing surfing of the web site by hackers.
- ☐ the same purpose as that of a digital certificate.

Question 250

Which of the following is the MOST important reason for logging firewall activity?

- ☐ Intrusion detection
- ☐ Auditing purposes
- ☐ Firewall tuning
- ☐ Incident investigation

Question 251

Which of the following should be an IS auditor's PRIMARY concern when evaluating an organization's information security policies, procedures, and controls for third-party vendors?

- ☐ The third-party vendors have their own information security requirements.
- ☐ The organization is still responsible for protecting the data.
- ☐ Noncompliance is easily detected.
- ☐ The same procedures and controls are used for all third-party vendors.

Licensed to Berend Post berend.post@it-university.nl

Question 252

A multinational company wants to establish a mandatory global standard for information security including data protection and privacy. Which of the following should be the GREATEST concern to an IS auditor?

- ☐ Inconsistent roll-out of the standard across all countries.
- ☐ Increased organizational effort without any tangible benefit
- ☐ Noncompliance with local laws in the affected countries
- ☐ Lack of adoption by organized labor groups in all affected countries

Question 253

Which of the following E-commerce model covers all the transactions between companies and government organization?

- ☐ B-to-C relationships
- ☐ B-to-B relationships
- ☐ B-to-E relationships
- ☐ B-to-G relationships

Question 254

An IS auditor is performing a post-implementation review of a system deployed two years ago. Which of the following findings should be of MOST concern to the auditor?

- ☐ Maintenance costs were not included in the project lifecycle costs.
- ☐ Benefits as stated in the business case have not been realized.
- ☐ Workarounds due to remaining defects had to be used longer than anticipated.
- ☐ The system has undergone several change requests to further extend functionality.

Question 255

If concurrent update transactions to an account are not processed properly, which of the following will be affected?

- ☐ Integrity
- ☐ Confidentiality
- ☐ Availability
- ☐ Accountability

Licensed to Berend Post berend.post@it-university.nl

Question 256

During an audit, it is discovered that several suppliers with standing orders have been deleted from the supplier master file. Which of the following controls would have BEST prevented such an occurrence?

- ☐ Logical relationship check
- ☐ Existence check
- ☐ Table look-ups
- ☐ Referential integrity

Question 257

In the process of evaluating program change controls, an IS auditor would use source code comparison software to:

- ☐ examine source program changes without information from IS personnel.
- ☐ detect a source program change made between acquiring a copy of the source and the comparison run.
- ☐ confirm that the control copy is the current version of the production program.
- ☐ ensure that all changes made in the current source copy are detected.

Question 258

The MAIN consideration when designing an incident escalation plan should be ensuring that:

- ☐ information assets are classified.
- ☐ appropriate stakeholders are involved.
- ☐ high-impact risks have been identified.
- ☐ requirements cover forensic analysis.

Question 259

Which of the following tests is MOST likely to detect an error in one subroutine resulting from a recent change in another subroutine?

- ☐ Stress testing
- ☐ Regression testing
- ☐ User acceptance testing
- ☐ Black-box testing

Licensed to Berend Post berend.post@it-university.nl

Question 260

When protecting an organization's IT systems, which of the following is normally the next line of defense after the network firewall has been compromised?

- ☐ Personal firewall
- ☐ Antivirus programs
- ☐ Intrusion detection system (IDS)
- ☐ Virtual local area network (VLAN) configuration

Question 261

Which of the following is the PRIMARY objective of implementing privacy-related controls within an organization?

- ☐ To identify data at rest and data in transit for encryption
- ☐ To prevent confidential data loss
- ☐ To comply with legal and regulatory requirements
- ☐ To provide options to individuals regarding use of their data

Question 262

Which of the following INCORRECTLY describes the layer functions of the LAN or WAN Layer of the TCP/IP model?

- ☐ Combines packets into bytes and bytes into frame
- ☐ Providers logical addressing which routers use for path determination
- ☐ Provide address to media using MAC address
- ☐ Performs only error detection

Question 263

Which of the following provides the BEST single-factor authentication?

- ☐ Biometrics
- ☐ Password
- ☐ Token
- ☐ PIN

Question 264

What process is used to validate a subject’s identity?

- ☐ Identification
- ☐ Nonrepudiation
- ☐ Authorization
- ☐ Authentication

Licensed to Berend Post berend.post@it-university.nl

Question 265

To help ensure the accuracy and completeness of end-user computing output, it is MOST important to include strong:

- ☐ reconciliation controls.
- ☐ change management controls.
- ☐ access management controls.
- ☐ documentation controls.

Question 266

Which of the following is a step in establishing a security policy?

- ☐ Developing platform-level security baselines.
- ☐ Developing configurations parameters for the network,
- ☐ Implementing a process for developing and maintaining the policy.
- ☐ Creating a RACI matrix.

Question 267

An organization plans to implement a virtualization strategy enabling multiple operating systems on a single host. Which of the following should be the GREATEST concern with this strategy?

- ☐ Adequate storage space
- ☐ Complexity of administration
- ☐ Network bandwidth
- ☐ Application performance

Question 268

In a data center audit, an IS auditor finds that the humidity level is very low. The IS auditor would be MOST concerned because of an expected increase in:

- ☐ employee discomfort
- ☐ risk of fire
- ☐ static electricity problems
- ☐ backup tape failures

Licensed to Berend Post berend.post@it-university.nl

Question 269

What is an IS auditor's BEST course of action if informed by a business unit's representatives that they are too busy to cooperate with a scheduled audit?

- ☐ Reschedule the audit for a time more convenient to the business unit.
- ☐ Notify the chief audit executive who can negotiate with the head of the business unit.
- ☐ Begin the audit regardless and insist on cooperation from the business unit.
- ☐ Notify the audit committee immediately and request they direct the audit begin on schedule.

Question 270

Which of the following is the PRIMARY purpose of documenting and approving an information security policy?

- ☐ To communicate management's intent for securing the organization's information assets
- ☐ To mitigate the organization's information security risk to an acceptable level
- ☐ To ensure awareness of disciplinary procedures for security breaches by authorized users
- ☐ To determine the best approach for implementing information security within the organization

Question 271

A small startup organization does not have the resources to implement segregation of duties. Which of the following would be the MOST effective compensating control?

- ☐ Rotation of log monitoring and analysis responsibilities
- ☐ Additional management reviews and reconciliations
- ☐ Third-party assessments
- ☐ Mandatory vacations

Question 272

Which of the following is the PRIMARY reason an IS auditor should discuss observations with management before delivering a final report?

- ☐ Identify business risks associated with the observations.
- ☐ Assist the management with control enhancements.
- ☐ Record the proposed course of corrective action.
- ☐ Validate the audit observations.

Licensed to Berend Post berend.post@it-university.nl

Question 273

Which of the following is the BEST way to identify the potential impact of a successful attack on an organization's mission critical applications?

- ☐ Execute regular vulnerability scans
- ☐ Conduct penetration testing
- ☐ Perform an application vulnerability review
- ☐ Perform an independent code review

Question 274

When reviewing business continuity plan (BCP) test results, it is MOST important for the IS auditor to determine whether the test:

- ☐ verifies the ability to resume key business operations.
- ☐ considers changes to the systems environment.
- ☐ assesses the capability to retrieve vital records.
- ☐ follows up on activities that occurred since the previous test.

Question 275

Which of the following applet intrusion issues poses the GREATEST risk of disruption to an organization?

- ☐ A program that deposits a virus on a client machine
- ☐ Applets recording keystrokes and, therefore, passwords
- ☐ Downloaded code that reads files on a client's hard drive
- ☐ Applets opening connections from the client machine

Question 276

Data flow diagrams are used by IS auditors to:

- ☐ order data hierarchically.
- ☐ highlight high-level data definitions.
- ☐ graphically summarize data paths and storage.
- ☐ portray step-by-step details of data generation.

Licensed to Berend Post berend.post@it-university.nl

Question 277

In a large organization, IT deadlines on important projects have been missed because IT resources are not prioritized properly. Which of the following is the BEST recommendation to address this problem?

- ☐ Implement project portfolio management.
- ☐ Implement an integrated resource management system.
- ☐ Implement a comprehensive project scorecard.
- ☐ Revisit the IT strategic plan.

Question 278

The FIRST course of action an investigator should take when a computer is being attacked is to:

- ☐ terminate all active processes.
- ☐ copy the contents of the hard drive.
- ☐ disconnect it from the network.
- ☐ disconnect the power source.

Question 279

If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

- ☐ IT cannot be implemented if senior management is not committed to strategic planning.
- ☐ More likely.
- ☐ Less likely.
- ☐ Strategic planning does not affect the success of a company's implementation of IT.

Question 280

A database administrator (DBA) extracts a user listing for an auditor as testing evidence. Which of the following will provide the GREATEST assurance that the user listing is reliable?

- ☐ Requesting a query that returns the count of the users.
- ☐ Requesting a copy of the query that generated the user listing
- ☐ Obtaining sign-off from the DBA to attest that the list is complete
- ☐ Witnessing the DBA running the query in-person

Licensed to Berend Post berend.post@it-university.nl

Question 281

Which of the following provides the BEST audit evidence that a firewall is configured in compliance with the organization's security policy?

- ☐ Analyzing how the configuration changes are performed
- ☐ Performing penetration testing
- ☐ Analyzing log files
- ☐ Reviewing the rule base

Question 282

An IS auditor finds that confidential company data has been inadvertently leaked through social engineering. The MOST effective way to help prevent a recurrence of this issue is to implement:

- ☐ penalties to staff for security policy breaches.
- ☐ a third-party intrusion prevention solution.
- ☐ a security awareness program.
- ☐ data loss prevention (DLP) software.

Question 283

Which of the following is the BEST indication of a successful information security culture?

- ☐ Penetration testing is done regularly and findings remediated.
- ☐ End users know how to identify and report incidents.
- ☐ Individuals are given access based on job functions.
- ☐ The budget allocated for information security is sufficient.

Question 284

A manager of a project was not able to implement all audit recommendations by the target date. The IS auditor should:

- ☐ recommend that the project be halted until the issues are resolved.
- ☐ recommend that compensating controls be implemented.
- ☐ evaluate risks associated with the unresolved issues.
- ☐ recommend that the project manager reallocate test resources to resolve the issues.

Licensed to Berend Post berend.post@it-university.nl

Question 285

An IS auditor should recommend the use of library control software to provide reasonable assurance that:

- ☐ program changes have been authorized.
- ☐ only thoroughly tested programs are released.
- ☐ modified programs are automatically moved to production.
- ☐ source and executable code integrity is maintained.

Question 286

When evaluating the ability of a disaster recovery plan to enable the recovery of IT processing capabilities, it is MOST important for the IS auditor to verify the plan is:

- ☐ stored at an offsite location
- ☐ communicated to department heads
- ☐ regularly reviewed
- ☐ periodically tested

Question 287

An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address?

- ☐ Simple Object Access Protocol (SOAP)
- ☐ Address Resolution Protocol (ARP)
- ☐ Routing Information Protocol (RIP)
- ☐ Transmission Control Protocol (TCP)

Question 288

Due to the small size of the payroll department, an organization is unable to segregate the employee setup and payroll processing functions. Which of the following would be the BEST compensating control for the lack of segregation of duties?

- ☐ An independent payroll disbursement review is conducted.
- ☐ The system is configured to require secondary approval for changes to the employee master file.
- ☐ A review is conducted to verify that terminated employees are removed from the employee master file.
- ☐ A payroll variance report is reviewed for anomalies every pay period.

Licensed to Berend Post berend.post@it-university.nl

Question 289

Following the discovery of inaccuracies in a data warehouse, an organization has implemented data profiling, cleansing, and handling filters to enhance the quality of data obtained from connected sources. Which type of control has been applied?

- ☐ Preventive control
- ☐ Corrective control
- ☐ Compensating control
- ☐ Detective control

Question 290

Which of the following statement INCORRECTLY describes anti-malware?

- ☐ 2
- ☐ 3
- ☐ 2 and 3
- ☐ None of the choices listed

Question 291

An IS auditor notes that application of super-user activity was not recorded in system logs. What is the auditor's BEST course of action?

- ☐ Recommend a least-privilege access model.
- ☐ Investigate the reason for the lack of logging.
- ☐ Report the issue to the audit manager.
- ☐ Recommend activation of super-user activity logging.

Question 292

An IS auditor is reviewing a software-based configuration. Which of the following represents the GREATEST vulnerability? The firewall software:

- ☐ is configured with an implicit deny rule as the last rule in the rule base.
- ☐ is installed on an operating system with default settings.
- ☐ has been configured with rules permitting or denying access to systems or networks.
- ☐ is configured as a virtual private network (VPN) endpoint.

Licensed to Berend Post berend.post@it-university.nl

Question 293

During an audit of a business continuity plan (BCP), an IS auditor found that, although all departments were housed in the same building, each department had a separate BCP. The IS auditor recommended that the BCPs be reconciled. Which of the following areas should be reconciled FIRST?

- ☐ Evacuation plan
- ☐ Recovery priorities
- ☐ Backup storages
- ☐ Call tree

Question 294

Which of the following would be of MOST concern during an audit of an end user computing system containing sensitive information?

- ☐ Audit logging is not available.
- ☐ System data is not protected.
- ☐ Secure authorization is not available.
- ☐ The system is not included in inventory.

Question 295

The PRIMARY purpose of vulnerability assessments is to:

- ☐ detect deficiencies that could lead to a system compromise.
- ☐ provide clear evidence that the system is sufficiently secure.
- ☐ test intrusion detection systems (IDS) and response procedures.
- ☐ determine the impact of potential threats.

Question 296

Which of the following would help to ensure the completeness of batch file transfers?

- ☐ Input controls
- ☐ Self-checking digits
- ☐ Hash totals
- ☐ Parity check

Licensed to Berend Post berend.post@it-university.nl

Question 297

An e-commerce enterprise's disaster recovery (DR) site has 30% less processing capability than the primary site. Based on this information, which of the following presents the GREATEST risk?

- ☐ Network firewalls and database firewalls at the DR site do not provide high availability.
- ☐ No disaster recovery plan (DRP) testing has been performed during the last six months.
- ☐ The DR site is in a shared location that hosts multiple other enterprises.
- ☐ The DR site has not undergone testing to confirm its effectiveness.

Question 298

When developing a business continuity plan (BCP), which of the following should be performed FIRST?

- ☐ Develop business continuity training
- ☐ Classify operations
- ☐ Conduct a business impact analysis (BIA)
- ☐ Establish a disaster recovery plan (DRP)

Question 299

Which of the following method of expressing knowledge base consist of a graph in which nodes represent physical or conceptual objects and the arcs describes the relationship between nodes?

- ☐ Decision tree
- ☐ Rules
- ☐ Semantic nets
- ☐ Knowledge interface

Question 300

Which of the following audit combines financial and operational audit steps?

- ☐ Compliance Audit
- ☐ Financial Audit
- ☐ Integrated Audit
- ☐ Forensic audit

Licensed to Berend Post berend.post@it-university.nl

Question 301

Which of the following types of attack involves a program that creates an infinite loop, makes lots of copies of itself, and continues to open lots of files?

- ☐ Local DoS attacks
- ☐ Remote DoS attacks
- ☐ Distributed DoS attacks
- ☐ Local Virus attacks
- ☐ None of the choices.

Question 302

An IS auditor is reviewing an organization's primary router access control list. Which of the following should result in a finding?

- ☐ The network security group can change network address translation (NAT).
- ☐ There are conflicting permit and deny rules for the IT group.
- ☐ There is only one rule per group with access privileges.
- ☐ Individual permissions are overriding group permissions.

Question 303

Which of the following is MOST important for an IS auditor to evaluate when determining the effectiveness of an information security program?

- ☐ Percentage of users aware of the objectives of the security program
- ☐ Percentage of policy exceptions that were approved with justification
- ☐ Percentage of desired control objectives achieved
- ☐ Percentage of reported security incidents

Question 304

A large chain of shops with electronic funds transfer (EFT) at point-of-sale devices has a central communications processor for connecting to the banking network. Which of the following is the BEST disaster recovery plan for the communications processor?

- ☐ Offsite storage of daily backups
- ☐ Alternative standby processor onsite
- ☐ installation of duplex communication links
- ☐ Alternative standby processor at another network node

Licensed to Berend Post berend.post@it-university.nl

Question 305

Doing which of the following during peak production hours could result in unexpected downtime?

- ☐ Performing data migration or tape backup
- ☐ Performing preventive maintenance on electrical systems
- ☐ Promoting applications from development to the staging environment
- ☐ Replacing a failed power supply in the core router of the data center

Question 306

Which of the following is the most important element in the design of a data warehouse?

- ☐ Quality of the metadata
- ☐ Speed of the transactions
- ☐ Volatility of the data
- ☐ Vulnerability of the system

Question 307

During a review of information security procedures for disabling user accounts, an IS auditor discovers that IT is only disabling network access for terminated employees. IT management maintains if terminated users cannot access the network, they will not be able to access any applications. Which of the following is the GREATEST risk associated with application access?

- ☐ Unauthorized access to data
- ☐ Inability to access data
- ☐ Lack of segregation of duties
- ☐ Loss of non-repudiation

Question 308

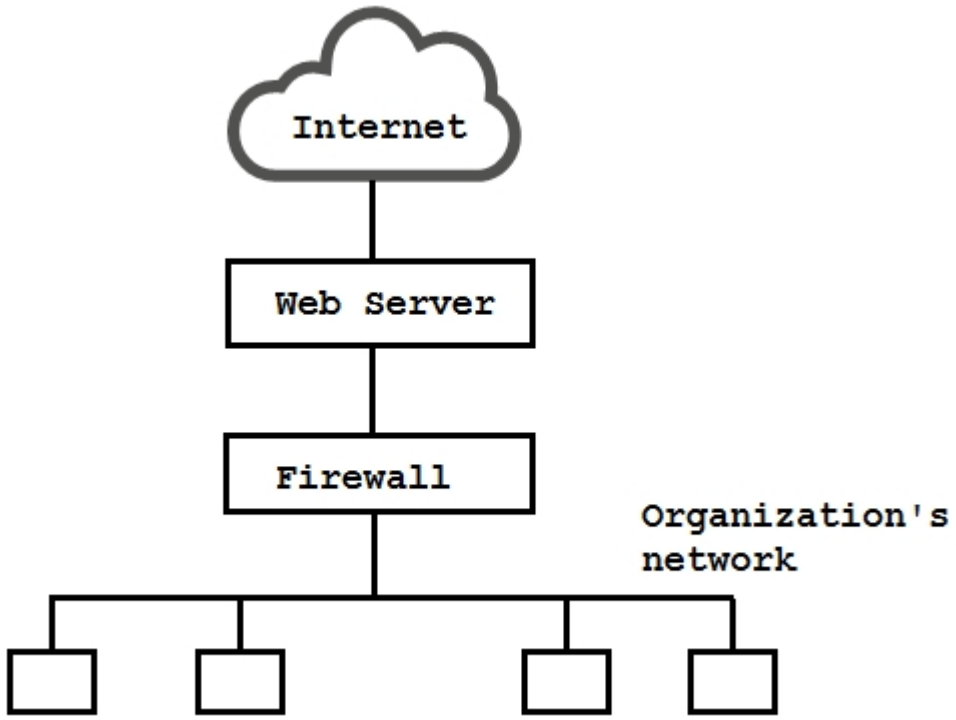
An IS auditor reviewing security incident processes realizes incidents are resolved and closed, but root causes are not investigated. Which of the following should be the MAJOR concern with this situation?

- ☐ Abuses by employees have not been reported.
- ☐ Vulnerabilities have not been properly addressed.
- ☐ Security incident policies are out of date.
- ☐ Lessons learned have not been properly documented.

Licensed to Berend Post berend.post@it-university.nl

Question 309

To detect attack attempts that the firewall is unable to recognize, an IS auditor should recommend placing a network intrusion detection system (IDS) between the:



- ☐ Firewall and the organization's network.
- ☐ Internet and the firewall.
- ☐ Internet and the web server.
- ☐ Web server and the firewall.

Question 310

Which of the following is MOST influential when defining disaster recovery strategies?

- ☐ Existing server redundancies
- ☐ Maximum tolerable downtime
- ☐ Data classification scheme
- ☐ Annual loss expectancy

Licensed to Berend Post berend.post@it-university.nl

Question 311

IS management has decided to install a level 1 Redundant Array of Inexpensive Disks (RAID) system in all servers to compensate for the elimination of offsite backups. The IS auditor should recommend:

- ☐ upgrading to a level 5 RAID.
- ☐ increasing the frequency of onsite backups.
- ☐ reinstating the offsite backups.
- ☐ establishing a cold site in a secure location.

Question 312

Which of the following is the BEST way to help ensure the security of privacy-related data stored by an organization?

- ☐ Encrypt personally identifiable information (PII).
- ☐ Publish the data classification scheme.
- ☐ Inform data owners of the purpose of collecting information.
- ☐ Classify privacy-related data as confidential.

Question 313

What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

- ☐ An organizational certificate
- ☐ A user certificate
- ☐ A website certificate
- ☐ Authenticode

Question 314

The MOST critical security weakness of a packet level firewall is that it can be circumvented by:

- ☐ using a dictionary attack of encrypted passwords.
- ☐ changing the source address on incoming packets.
- ☐ intercepting packets and viewing passwords sent in clear text.
- ☐ deciphering the signature information of the packets.

Licensed to Berend Post berend.post@it-university.nl

Question 315

Which of the following is the initial step in creating a firewall policy?

- ☐ A cost-benefit analysis of methods for securing the applications
- ☐ Identification of network applications to be externally accessed
- ☐ Identification of vulnerabilities associated with network applications to be externally accessed
- ☐ Creation of an applications traffic matrix showing protection methods

Question 316

An IS auditor performing a review of the backup processing facilities should be MOST concerned that:

- ☐ adequate fire insurance exists.
- ☐ regular hardware maintenance is performed.
- ☐ offsite storage of transaction and master files exists.
- ☐ backup processing facilities are fully tested.

Question 317

Which of the following is the BEST way to achieve high availability and fault tolerance for an e-business system?

- ☐ Network diversity
- ☐ Storage area network
- ☐ Robust systems architecture
- ☐ Secure offsite backup storage

Question 318

To create a digital signature in a message using asymmetric encryption, it is necessary to:

- ☐ first use a symmetric algorithm for the authentication sequence.
- ☐ encrypt the authentication sequence using a public key.
- ☐ transmit the actual digital signature in unencrypted clear text.
- ☐ encrypt the authentication sequence using a private key.

Question 319

The use of digital signatures:

- ☐ requires the use of a one-time password generator.
- ☐ provides encryption to a message.
- ☐ validates the source of a message.
- ☐ ensures message confidentiality.

Licensed to Berend Post berend.post@it-university.nl

Question 320

The MOST effective control for reducing the risk related to phishing is:

- ☐ centralized monitoring of systems.
- ☐ including signatures for phishing in antivirus software.
- ☐ publishing the policy on antiphishing on the intranet.
- ☐ security training for all users.

Question 321

Which of the following layer of an enterprise data flow architecture represents subsets of information from the core data warehouse?

- ☐ Presentation layer
- ☐ Desktop Access Layer
- ☐ Data Mart layer
- ☐ Data access layer

Question 322

Which of the following backup schemes is the BEST option when storage media is limited?

- ☐ Virtual backup
- ☐ Real-time backup
- ☐ Differential backup
- ☐ Full backup

Question 323

In a client-server architecture, a domain name service (DNS) is MOST important because it provides the:

- ☐ address of the domain server.
- ☐ resolution service for the name/address.
- ☐ IP addresses for the internet.
- ☐ domain name system.

Licensed to Berend Post berend.post@it-university.nl

Question 324

Which of the following disaster recovery/continuity plan components provides the GREATEST assurance of recovery after a disaster?

- ☐ The alternate facility will be available until the original information processing facility is restored.
- ☐ User management is involved in the identification of critical systems and their associated critical recovery times.
- ☐ Copies of the plan are kept at the homes of key decision-making personnel.
- ☐ Feedback is provided to management assuring them that the business continuity plans are indeed workable and that the procedures are current.

Question 325

A 5-year audit plan provides for general audits every year and application audits on alternating years. To achieve higher efficiency, the IS audit manager would MOST likely:

- ☐ proceed with the plan and integrate all new applications.
- ☐ alternate between control self-assessment (CSA) and general audits every year.
- ☐ implement risk assessment criteria to determine audit priorities.
- ☐ have control self-assessments (CSAs) and formal audits of applications on alternating years.

Question 326

Which of the following protocol does NOT work at the Application layer of the TCP/IP Models?

- ☐ HTTP
- ☐ FTP
- ☐ NTP
- ☐ TCP

Question 327

An organization was severely impacted after an advanced persistent threat (APT) attack. Afterwards, it was found that the initial breach happened a month prior to the attack. Management's GREATEST concern should be:

- ☐ results of the past internal penetration test
- ☐ the effectiveness of monitoring processes
- ☐ the installation of critical security patches
- ☐ external firewall policies

Licensed to Berend Post berend.post@it-university.nl

Question 328

An internal audit department recently established a quality assurance (QA) program as part of its overall audit program. Which of the following activities is MOST important to include as part of the QA program requirements?

- ☐ Implementing corrective action plans.
- ☐ Reviewing audit standards periodically
- ☐ Analyzing user satisfaction reports from business lines
- ☐ Creating a long-term plan for internal audit staffing

Question 329

An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

- ☐ dependency on a single person.
- ☐ inadequate succession planning.
- ☐ one person knowing all parts of a system.
- ☐ a disruption of operations.

Question 330

An organization has agreed to perform remediation related to high risk audit findings. The remediation process involves a complex reorganization of user roles as well as the implementation of several compensating controls that may not be completed within the next audit cycle. Which of the following is the BEST way for an IS auditor to follow up on the activities?

- ☐ Review the progress of remediation on a regular basis.
- ☐ Provide management with a remediation timeline and verify adherence.
- ☐ Continue to audit the failed controls according to the audit schedule.
- ☐ Schedule a review of the controls after the projected remediation date.

Question 331

Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?

- ☐ Applications may not be subject to testing and IT general controls
- ☐ increased development and maintenance costs
- ☐ increased application development time
- ☐ Decision-making may be impaired due to diminished responsiveness to requests for information

Licensed to Berend Post berend.post@it-university.nl

Question 332

As part of a post-implementation review, the BEST way to assess the realization of outcomes is by:

- ☐ obtaining feedback from the user community.
- ☐ performing a comprehensive risk analysis.
- ☐ evaluating the actual performance of the system.
- ☐ comparing the business case benefits to the archived benefits.

Question 333

During a privileged access review, an IS auditor observes many help desk employees have privileges within systems not required for their job functions. Implementing which of the following would have prevented this situation?

- ☐ Separation of duties
- ☐ Multi-factor authentication
- ☐ Least privilege access
- ☐ Privileged access reviews

Question 334

Which of the following provides the BEST assurance that security policies are applied across business operations?

- ☐ Organizational standards are required to be formally accepted.
- ☐ Organizational standards are enforced by technical controls.
- ☐ Organizational standards are included in awareness training.
- ☐ Organizational standards are documented in operational procedures.

Question 335

Java applets and ActiveX controls are distributed executable programs that execute in the background of a web browser client. This practice is considered reasonable when:

- ☐ a firewall exists.
- ☐ a secure web connection is used.
- ☐ the source of the executable file is certain.
- ☐ the host web site is part of the organization.

Licensed to Berend Post berend.post@it-university.nl

Question 336

Which of the following is the BEST source of information for assessing the effectiveness of IT process monitoring?

- ☐ Participative management techniques
- ☐ Quality assurance (QA) reviews
- ☐ Performance data
- ☐ Real-time audit software

Question 337

An organization has software that is not compliant with data protection requirements. To help ensure that appropriate and relevant data protection controls are implemented in the future, the auditor's BEST course of action would be to:

- ☐ conduct a privacy impact assessment to identity gaps in the organization's privacy.
- ☐ recommend that privacy checks are included within the solution development life cycle.
- ☐ recommend an executive be appointed to oversee privacy program improvements.
- ☐ map the organization's business processes to identify personally identifiable information (PII).

Question 338

The specific advantage of white box testing is that it:

- ☐ verifies a program can operate successfully with other parts of the system.
- ☐ ensures a program's functional operating effectiveness without regard to the internal program structure.
- ☐ determines procedural accuracy or conditions of a program's specific logic paths.
- ☐ examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host system.

Question 339

An employee uses a personal mobile device to access corporate data and email, but also allows friends to use it as a mobile hotspot for Internet access when not at work. The information security manager is concerned this situation may expose confidential data. The manager's FIRST step should be to:

- ☐ update the mobile device usage standards to address the issue and communicate to all employees
- ☐ activate the incident response plan to mitigate the impact and stop the compromise
- ☐ review the associated risks to determine if additional controls are needed
- ☐ implement additional security controls that will mitigate the situation and then reassess risks

Licensed to Berend Post berend.post@it-university.nl

Question 340

In the event of a data center disaster, which of the following would be the MOST appropriate strategy to enable a complete recovery of a critical database?

- ☐ Daily data backup to tape and storage at a remote site
- ☐ Real-time replication to a remote site
- ☐ Hard disk mirroring to a local server
- ☐ Real-time data backup to the local storage area network (SAN)

Question 341

A new system development project is running late against a critical implementation deadline. Which of the following is the MOST important activity?

- ☐ Document last-minute enhancements.
- ☐ Perform user acceptance testing.
- ☐ Perform a pre-implementation audit.
- ☐ Ensure that code has been reviewed.

Question 342

When evaluating whether the expected benefits of a project have been achieved, it is MOST important for an IS auditor to review:

- ☐ post-implementation issues.
- ☐ quality assurance results.
- ☐ the project schedule.
- ☐ the business case.

Question 343

To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

- ☐ O/S and hardware refresh frequencies
- ☐ Gain-sharing performance bonuses
- ☐ Penalties for noncompliance
- ☐ Charges tied to variable cost metrics

Licensed to Berend Post berend.post@it-university.nl

Question 344

An organization has outsourced its help desk activities. An IS auditor's GREATEST concern when reviewing the contract and associated service level agreement (SLA) between the organization and vendor should be the provisions for:

- ☐ documentation of staff background checks.
- ☐ independent audit reports or full audit access.
- ☐ reporting the year-to-year incremental cost reductions.
- ☐ reporting staff turnover, development or training.

Question 345

Which of the following is a type of computer network used for data transmission among devices such as computers, telephones and personal digital assistants?

- ☐ LAN
- ☐ WAN
- ☐ SAN
- ☐ PAN

Question 346

During a follow-up audit, an IS auditor learns the organization implemented an automated process instead of the originally agreed upon enhancement of the manual process. The auditor should:

- ☐ report the finding that recommendations were not acted upon
- ☐ perform a cost-benefit analysis on the new process
- ☐ verify that the new process satisfies control objectives
- ☐ report the recommendation as implemented

Question 347

Which of the following is MOST helpful in preventing a systems failure from occurring when an application is replaced using the abrupt changeover technique?

- ☐ Comprehensive documentation
- ☐ Comprehensive testing
- ☐ Threat and risk assessment
- ☐ Change management

Licensed to Berend Post berend.post@it-university.nl

Question 348

Which of the following types of controls would be MOST important to implement when digitizing human resource (HR) records?

- ☐ Change management controls
- ☐ Software development controls
- ☐ Project management controls
- ☐ Access management controls

Question 349

An IS auditor is observing transaction processing and notes that a high-priority update job ran out of sequence. What is the MOST significant risk from this observation?

- ☐ Previous jobs may have failed.
- ☐ The job may not have run to completion.
- ☐ Daily schedules may not be accurate.
- ☐ The job competes with invalid data.

Question 350

To affix a digital signature to a message, the sender must first create a message digest by applying a cryptographic hashing algorithm against:

- ☐ the entire message and thereafter enciphering the message digest using the sender's private key.
- ☐ any arbitrary part of the message and thereafter enciphering the message digest using the sender's private key.
- ☐ the entire message and thereafter enciphering the message using the sender's private key.
- ☐ the entire message and thereafter enciphering the message along with the message digest using the sender's private key.

Question 351

Intrusion detection systems (IDSs) can:

- ☐ substitute for a firewall.
- ☐ compensate for weak authentication mechanisms.
- ☐ conduct investigations of attacks from within the network.
- ☐ provide information to enhance the security infrastructure.

Licensed to Berend Post berend.post@it-university.nl

Question 352

Performance monitoring tools report that servers are consistently above the recommended utilization capacity. Which of the following is the BEST recommendation of the IS auditor?

- ☐ Develop a capacity plan based on usage projections.
- ☐ Deploy load balancers.
- ☐ Monitor activity logs.
- ☐ Add servers until utilization is at target capacity.

Question 353

In a typical SDLC, which group is PRIMARILY responsible for confirming compliance with requirements?

- ☐ Steering committee
- ☐ Risk management
- ☐ Quality assurance
- ☐ Internal audit

Question 354

Code changes are compiled and placed in a change folder by the developer. An implementation team migrates changes to production from the change folder. Which of the following BEST indicates separation of duties is in place during the migration process?

- ☐ A second individual performs code review before the change is released to production.
- ☐ The developer approves changes prior to moving them to the change folder.
- ☐ The implementation team does not have experience writing code.
- ☐ The implementation team does not have access to change the source code.

Question 355

A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

- ☐ recovery.
- ☐ retention.
- ☐ rebuilding.
- ☐ reuse.

Licensed to Berend Post berend.post@it-university.nl

Question 356

Which of the following strategies BEST optimizes data storage without compromising data retention practices?

- ☐ Limiting the size of the file attachments being sent via email
- ☐ Automatically deleting emails older than one year
- ☐ Moving emails to a virtual email vault after 30 days
- ☐ Allowing employees to store large emails on flash drives

Question 357

Which of the following is the MOST important prerequisite for implementing a data loss prevention (DLP) tool?

- ☐ Identifying where existing data resides and establishing a data classification matrix.
- ☐ Requiring users to save files in secured folders instead of a company-wide shared drive
- ☐ Reviewing data transfer logs to determine historical patterns of data flow
- ☐ Developing a DLP policy and requiring signed acknowledgement by users

Question 358

When continuous monitoring systems are being implemented, an IS auditor should FIRST identify:

- ☐ the location and format of output files
- ☐ applications that provide the highest financial risk
- ☐ high-risk areas within the organization
- ☐ the controls on which to focus

Question 359

The use of object-oriented design and development techniques would MOST likely:

- ☐ facilitate the ability to reuse modules.
- ☐ improve system performance.
- ☐ enhance control effectiveness.
- ☐ speed up the system development life cycle.

Licensed to Berend Post berend.post@it-university.nl

Question 360

Organizations should use off-site storage facilities to maintain _____ (fill in the blank) of current and critical information within backup files.

- ☐ Confidentiality
- ☐ Integrity
- ☐ Redundancy
- ☐ Concurrency

Question 361

The responsibility for authorizing access to a business application system belongs to the:

- ☐ data owner.
- ☐ security administrator.
- ☐ IT security manager.
- ☐ requestor's immediate supervisor.

Question 362

A legacy payroll application is migrated to a new application. Which of the following stakeholders should be PRIMARILY responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

- ☐ IS auditor
- ☐ Database administrator
- ☐ Project manager
- ☐ Data owner

Question 363

Which of the following is the FIRST step in initiating a data classification program?

- ☐ Risk appetite assessment
- ☐ Inventory of data assets
- ☐ Assignment of data ownership
- ☐ Assignment of sensitivity levels

Licensed to Berend Post berend.post@it-university.nl

Question 364

What is the MOST difficult aspect of access control in a multiplatform, multiple-site client/server environment?

- ☐ Creating new user IDs valid only on a few hosts
- ☐ Maintaining consistency throughout all platforms
- ☐ Restricting a local user to necessary resources on a local platform
- ☐ Restricting a local user to necessary resources on the host server

Question 365

Which of the following type of computer is a large, general purpose computer that are made to share their processing power and facilities with thousands of internal or external users?

- ☐ Thin client computer
- ☐ Midrange servers
- ☐ Personal computers
- ☐ Mainframe computers

Question 366

The BEST reason for implementing a virtual private network (VPN) is that it:

- ☐ eases the implementation of data encryption.
- ☐ allows for public use of private networks.
- ☐ enables use of existing hardware platforms.
- ☐ allows for private use of public networks.

Question 367

What can be implemented to provide the highest level of protection from external attack?

- ☐ Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
- ☐ Configuring the firewall as a screened host behind a router
- ☐ Configuring the firewall as the protecting bastion host
- ☐ Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts

Licensed to Berend Post berend.post@it-university.nl

Question 368

Which of the following methods BEST ensures that a comprehensive approach is used to direct information security activities?

- ☐ Creating communication channels
- ☐ Promoting security training
- ☐ Establishing a steering committee
- ☐ Holding periodic meetings with business owners

Question 369

The MOST important difference between hashing and encryption is that hashing:

- ☐ is irreversible.
- ☐ output is the same length as the original message.
- ☐ is concerned with integrity and security.
- ☐ is the same at the sending and receiving end.

Question 370

In the context of effective information security governance, the primary objective of value delivery is to:

- ☐ optimize security investments in support of business objectives.
- ☐ implement a standard set of security practices.
- ☐ institute a standards-based solution.
- ☐ implement a continuous improvement culture.

Question 371

Which of the following is a passive attack on a network?

- ☐ Message service interruption
- ☐ Message modification
- ☐ Traffic analysis
- ☐ Sequence analysis

Question 372

In an online transaction processing system, data integrity is maintained by ensuring that a transaction is either completed in its entirety or not at all. This principle of data integrity is known as:

- ☐ isolation.
- ☐ consistency.
- ☐ atomicity.
- ☐ durability.

Licensed to Berend Post berend.post@it-university.nl

Question 373

Which of the following activities should the business continuity manager perform FIRST after the replacement of hardware at the primary information processing facility?

- ☐ verify compatibility with the hot site.
- ☐ Review the implementation report.
- ☐ Perform a walk-through of the disaster recovery plan.
- ☐ Update the IS assets inventory.

Question 374

In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:

- ☐ implementation.
- ☐ compliance.
- ☐ documentation.
- ☐ sufficiency.

Question 375

A financial services organization is developing and documenting business continuity measures. In which of the following cases would an IS auditor MOST likely raise an issue?

- ☐ The organization uses good practice guidelines instead of industry standards and relies on external advisors to ensure the adequacy of the methodology.
- ☐ The business continuity capabilities are planned around a carefully selected set of scenarios which describe events that might happen with a reasonable probability.
- ☐ The recovery time objectives (RTOs) do not take IT disaster recovery constraints into account, such as personnel or system dependencies during the recovery phase.
- ☐ The organization plans to rent a shared alternate site with emergency workplaces which has only enough room for half of the normal staff.

Question 376

Library control software restricts source code to:

- ☐ Read-only access
- ☐ Write-only access
- ☐ Full access
- ☐ Read-write access

Licensed to Berend Post berend.post@it-university.nl

Question 377

An organization has created a policy that defines the types of web sites that users are forbidden to access. What is the MOST effective technology to enforce this policy?

- ☐ Stateful inspection firewall
- ☐ Web content filter
- ☐ Web cache server
- ☐ Proxy server

Question 378

Which of the following should be of MOST concern to an IS auditor during the review of a quality management system?

- ☐ The quality management system includes training records for IT personnel.
- ☐ There are no records to document actions for minor business processes.
- ☐ Important quality checklists are maintained outside the quality management system.
- ☐ Indicators are not fully represented in the quality management system.

Question 379

The MOST effective way to determine if IT is meeting business requirements is to establish:

- ☐ industry benchmarks.
- ☐ organizational goals.
- ☐ a capability model.
- ☐ key performance indicators (KPIs).

Question 380

When using a newly implemented security information and event management (SIEM) infrastructure, which of the following should be considered FIRST?

- ☐ Report distribution
- ☐ Encryption
- ☐ Tuning
- ☐ Retention

Licensed to Berend Post berend.post@it-university.nl

Question 381

An emergency change was made to an IT system as a result of a failure. Which of the following should be of GREATEST concern to the organization's information security manager?

- ☐ The operations team implemented the change without regression testing.
- ☐ The change did not include a proper assessment of risk.
- ☐ Documentation of the change was made after implementation.
- ☐ The information security manager did not review the change prior to implementation.

Question 382

A financial institution that processes millions of transactions each day has a central communications processor (switch) for connecting to automated teller machines (ATMs). Which of the following would be the BEST contingency plan for the communications processor?

- ☐ Reciprocal agreement with another organization
- ☐ Alternate processor in the same location
- ☐ Alternate processor at another network node
- ☐ Installation of duplex communication links

Question 383

Which of the following is a form of Hybrid Cryptography where the sender encrypts the bulk of the data using Symmetric Key cryptography and then communicates securely a copy of the session key to the receiver?

- ☐ Digital Envelope
- ☐ Digital Signature
- ☐ Symmetric key encryption
- ☐ Asymmetric

Question 384

Establishing the level of acceptable risk is the responsibility of:

- ☐ quality assurance management.
- ☐ senior business management.
- ☐ the chief information officer.
- ☐ the chief security officer.

Licensed to Berend Post berend.post@it-university.nl

Question 385

Which of the following would BEST support 24/7 availability?

- ☐ Daily backup
- ☐ offsite storage
- ☐ Mirroring
- ☐ Periodic testing

Question 386

Which of the following term in business continuity defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 387

Which of the following access rights presents the GREATEST risk when granted to a new member of the system development staff?

- ☐ Execute access to development program libraries
- ☐ Write access to development data libraries
- ☐ Execute access to production program libraries
- ☐ Write access to production program libraries

Question 388

What is a common vulnerability, allowing denial-of-service attacks?

- ☐ Assigning access to users according to the principle of least privilege
- ☐ Lack of employee awareness of organizational security policies
- ☐ Improperly configured routers and router access lists
- ☐ Configuring firewall access rules

Question 389

The PRIMARY benefit of implementing a security program as part of a security governance framework is the:

- ☐ alignment of the IT activities with IS audit recommendations.
- ☐ enforcement of the management of security risks.
- ☐ implementation of the chief information security officer's (CISO) recommendations.
- ☐ reduction of the cost for IT security.

Licensed to Berend Post berend.post@it-university.nl

Question 390

Attribute sampling is BEST suited to estimate:

- ☐ compliance with approved procedures.
- ☐ the true monetary value of a population.
- ☐ the total error amount in the population.
- ☐ whether a recorded balance is within limits of materiality.

Question 391

A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

- ☐ Establishing an inter-networked system of client servers with suppliers for increased efficiencies
- ☐ Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing
- ☐ Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format
- ☐ Reengineering the existing processing and redesigning the existing system

Question 392

To ensure appropriate control of information processed in IT systems, security safeguards should be based PRIMARILY on:

- ☐ established guidelines.
- ☐ overall IT capacity and operational constraints.
- ☐ efficient technical processing considerations.
- ☐ criteria consistent with classification levels.

Question 393

Why is it not preferable for a firewall to treat each network frame or packet in isolation?

- ☐ Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.
- ☐ Such a firewall is costly to setup.
- ☐ Such a firewall is too complicated to maintain.
- ☐ Such a firewall is CPU hungry.
- ☐ Such a firewall offers poor compatibility.
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 394

Which of the following is used in providing logical access control to restrict updating or deleting business information in a relational database?

- ☐ Trigger
- ☐ View
- ☐ Join
- ☐ Primary key

Question 395

Which of the following IS functions can be performed by the same group or individual while still providing the proper segregation of duties?

- ☐ Computer operations and application programming
- ☐ Database administration and computer operations
- ☐ Security administration and application programming
- ☐ Application programming and systems analysis

Question 396

Which of the following would be of MOST concern for an IS auditor evaluating the design of an organization's incident management processes?

- ☐ Metrics are not reported to senior management.
- ☐ Service management standards are not followed.
- ☐ Expected time to resolve incidents is not specified.
- ☐ Prioritization criteria are not defined.

Question 397

The reason for establishing a stop or freezing point on the design of a new system is to:

- ☐ prevent further changes to a project in process.
- ☐ indicate the point at which the design is to be completed.
- ☐ require that changes after that point be evaluated for cost-effectiveness.
- ☐ provide the project management team with more control over the project design.

Licensed to Berend Post berend.post@it-university.nl

Question 398

What are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information?

- ☐ Referential integrity controls
- ☐ Normalization controls
- ☐ Concurrency controls
- ☐ Run-to-run totals

Question 399

A computer program used by multiple departments has data quality issues. There is no agreement as to who should be responsible for corrective action. Which of the following is an IS auditor's BEST course of action?

- ☐ Recommend the IT department be assigned data cleansing responsibility.
- ☐ Modify the program to automatically cleanse the data and close the issue.
- ☐ Assign responsibility to the primary department using the program.
- ☐ Note the disagreement and recommend establishing data governance.

Question 400

John has been hired to fill a new position in one of the well-known financial institute. The position is for IS auditor. He has been assigned to complete IS audit of one of critical financial system. Which of the following should be the first step for John to be perform during IS audit planning?

- ☐ Perform risk assessment
- ☐ Determine the objective of the audit
- ☐ Gain an understanding of the business process
- ☐ Assign the personnel resource to audit

Question 401

Which of the following ACID property in DBMS requires that each transaction is "all or nothing"?

- ☐ Atomicity
- ☐ Consistency
- ☐ Isolation
- ☐ Durability

Licensed to Berend Post berend.post@it-university.nl

Question 402

During the design of a business continuity plan, the business impact analysis (BIA) identifies critical processes and supporting applications. This will PRIMARILY influence the:

- ☐ responsibility for maintaining the business continuity plan.
- ☐ criteria for selecting a recovery site provider.
- ☐ recovery strategy.
- ☐ responsibilities of key personnel.

Question 403

An IS auditor is mapping controls to risk for an accounts payable system. What is the BEST control to detect errors in the system?

- ☐ Alignment of the process to business objectives
- ☐ Quality control review of new payments
- ☐ Management approval of payments
- ☐ Input validation

Question 404

Which of the following is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality?

- ☐ Function point analysis
- ☐ Critical path methodology
- ☐ Rapid application development
- ☐ Program evaluation review technique

Question 405

Which of the following should be the MOST important consideration when deciding areas of priority for IT governance implementation?

- ☐ Process maturity
- ☐ Performance indicators
- ☐ Business risk
- ☐ Assurance reports

Licensed to Berend Post berend.post@it-university.nl

Question 406

While reviewing an organization's business continuity plan (BCP), an IS auditor observes that a recently developed application is not included. The IS auditor should:

- ☐ ensure that the criticality of the application is determined.
- ☐ ignore the observation as the application is not mission critical.
- ☐ include in the audit findings that the BCP is incomplete.
- ☐ recommend that the application be incorporated in the BCP.

Question 407

Which of the following do digital signatures provide?

- ☐ Authentication and integrity of data
- ☐ Authentication and confidentiality of data
- ☐ Confidentiality and integrity of data
- ☐ Authentication and availability of data

Question 408

An internal IS auditor discovers that a service organization did not notify its customers following a data breach. Which of the following should the auditor do FIRST?

- ☐ Notify audit management of the finding.
- ☐ Report the finding to regulatory authorities.
- ☐ Notify the service organization's customers.
- ☐ Require the service organization to notify its customers.

Question 409

Which of the following weaknesses would have the GREATEST impact on the effective operation of a perimeter firewall?

- ☐ Ad-hoc monitoring of firewall activity
- ☐ Potential back doors to the firewall software
- ☐ Misconfiguration on the firewall rules
- ☐ Use of stateful firewalls with default configuration

Licensed to Berend Post berend.post@it-university.nl

Question 410

An organization which uses external cloud services extensively is concerned with risk monitoring and timely response. The BEST way to address this concern is to ensure:

- ☐ the availability of continuous technical support
- ☐ internal security standards are in place
- ☐ a right-to-audit clause is included in contracts
- ☐ appropriate service level agreements (SLAs) are in place

Question 411

Which of the following should be the PRIMARY objective of an information security governance framework?

- ☐ Increase the organization's return on security investment.
- ☐ Provide a baseline for optimizing the security profile of the organization.
- ☐ Ensure that users comply with the organization's information security policies.
- ☐ Demonstrate compliance with industry best practices to external stakeholders.

Question 412

The BEST way to assure an organization's board of directors that IT strategies support business objectives is to:

- ☐ provide regular assessments of emerging technologies
- ☐ identify and report on the achievement of critical success factors
- ☐ confirm that IT strategies have been fully documented and disseminated
- ☐ ensure that senior business managers review IT budgets

Question 413

An information security team has discovered that users are sharing a login account to an application with sensitive information, in violation of the access policy. Business management indicates that the practice creates operational efficiencies. The information security manager's BEST course of action should be to:

- ☐ modify the policy
- ☐ present the risk to senior management
- ☐ enforce the policy
- ☐ create an exception for the deviation

Licensed to Berend Post berend.post@it-university.nl

Question 414

In computer forensic which of the following describe the process that converts the information extracted into a format that can be understood by investigator?

- ☐ Investigation
- ☐ Interrogation
- ☐ Reporting
- ☐ Extraction

Question 415

Inherent risk ratings are determined by assessing the impact and likelihood of a threat or vulnerability occurring:

- ☐ after internal controls are taken into account.
- ☐ before the risk appetite is established.
- ☐ after compensating controls have been applied.
- ☐ before internal controls are taken into account.

Question 416

Which of the following is a project management technique for defining and deploying software deliverables within a relatively short and fixed period of time, and with predetermined specific resources?

- ☐ Functional Point analysis
- ☐ Gantt Chart
- ☐ Critical path methodology
- ☐ Time box management

Question 417

An IS auditor is reviewing security controls related to collaboration tools for a business unit responsible for intellectual property and patents. Which of the following observations should be of MOST concern to the auditor?

- ☐ Training was not provided to the department that handles intellectual property and patents.
- ☐ Logging and monitoring for content filtering is not enabled.
- ☐ The collaboration tool is hosted and can only be accessed via an Internet browser.
- ☐ Employees can share files with users outside the company through collaboration tools.

Licensed to Berend Post berend.post@it-university.nl

Question 418

Which of the following is the MOST effective way to assess whether an outsourcer's controls are following the service level agreement (SLA)?

- ☐ Perform an onsite review of the outsourcer.
- ☐ Review the outsourcer's monthly service reports.
- ☐ Perform a review of penalty clauses for non-performance.
- ☐ Review an internal audit report from the outsourcer's auditor.

Question 419

During the procurement process, which of the following would be the BEST indication that prospective vendors will meet the organization's needs?

- ☐ An account transition manager has been identified.
- ☐ Expected service levels are defined.
- ☐ The vendor's subcontractors have been identified.
- ☐ The service catalog is documented.

Question 420

Which of the following ensures confidentiality of information sent over the internet?

- ☐ Digital signature
- ☐ Digital certificate
- ☐ Online Certificate Status Protocol
- ☐ Private key cryptosystem

Question 421

When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

- ☐ There could be a question regarding the legal jurisdiction.
- ☐ Having a provider abroad will cause excessive costs in future audits.
- ☐ The auditing process will be difficult because of the distance.
- ☐ There could be different auditing norms.

Licensed to Berend Post berend.post@it-university.nl

Question 422

Which of the following type of a computer network is a WAN that are limited to a city?

- ☐ LAN
- ☐ MAN
- ☐ SAN
- ☐ PAN

Question 423

Which of the following concerns associated with the World Wide Web would be addressed by a firewall?

- ☐ Unauthorized access from outside the organization
- ☐ Unauthorized access from within the organization
- ☐ A delay in Internet connectivity
- ☐ A delay in downloading using File Transfer Protocol (FTP)

Question 424

As part of an IS audit, the auditor notes the practices listed below. Which of the following would be a segregation of duties concern?

- ☐ Operators are degaussing magnetic tapes during night shifts.
- ☐ System programmers have logged access to operating system parameters.
- ☐ System programmers are performing the duties of operators.
- ☐ Operators are acting as tape librarians on alternate shifts.

Question 425

An organization has replaced all of the storage devices at its primary data center with new, higher capacity units. The replaced devices have been installed at the disaster recovery site to replace older units. An IS auditor's PRIMARY concern would be whether:

- ☐ the procurement was in accordance with corporate policies and procedures
- ☐ the relocation plan has been communicated to all concerned parties
- ☐ a hardware maintenance contract is in place for both old and new storage devices
- ☐ the recovery site devices can handle the storage requirements

Licensed to Berend Post berend.post@it-university.nl

Question 426

Introducing inhomogeneity to your network for the sake of robustness would have which of the following drawbacks?

- ☐ poorer performance.
- ☐ poor scalability.
- ☐ weak infrastructure.
- ☐ high costs in terms of training and maintenance.
- ☐ None of the choices.

Question 427

Which of the following should an IS auditor expect to find in an organization's information security policies?

- ☐ Authentication requirements
- ☐ Asset provisioning lifecycle
- ☐ Security configuration settings
- ☐ Secure coding procedures

Question 428

Who is primarily responsible for storing and safeguarding the data?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Steward
- ☐ Security Administrator

Question 429

An employee who denies accusations of sending inappropriate images to other employees has been discharged. For evidential purposes, the mail database for the discharged employee's computer should be:

- ☐ deleted as it could subject the organization to further legal liability
- ☐ impounded by physically removing the disk drive
- ☐ backed up to the server, where its access can be tightly restricted
- ☐ copied to write-once, read-many media using the computer's OS tools

Licensed to Berend Post berend.post@it-university.nl

Question 430

Which of the following controls would BEST ensure that payroll system rate changes are valid?

- ☐ Only a payroll department manager can input the new rate.
- ☐ Rate changes require visual verification before acceptance.
- ☐ Rate changes must be entered twice to ensure that they are entered correctly.
- ☐ Rate changes are reported to and independently verified by a manager.

Question 431

Which of the following is a PRIMARY security responsibility of an information owner?

- ☐ Determining the controls associated with information classification
- ☐ Testing information classification controls
- ☐ Maintaining the integrity of data in the information systems
- ☐ Deciding what level of classification the information requires

Question 432

An IS auditor finds the log management system is overwhelmed with false positive alerts. The auditor's BEST recommendation would be to:

- ☐ recruit more monitoring personnel.
- ☐ fine tune the intrusion detection system (IDS).
- ☐ reduce the firewall rules.
- ☐ establish criteria for reviewing alerts.

Question 433

The independence of an IS auditor auditing an application is maintained if the auditor's role is limited to:

- ☐ creating system specifications.
- ☐ defining user requirements.
- ☐ recommending system enhancements.
- ☐ designing access control rules.

Question 434

Which of the following is the BEST reason to perform root cause analysis after a critical server failure?

- ☐ To enable appropriate corrective measures
- ☐ To enable the gathering of system availability data
- ☐ To enable timely follow-up audits
- ☐ To enable the optimization of IT investments

Licensed to Berend Post berend.post@it-university.nl

Question 435

An IS auditor is reviewing the process followed in identifying and prioritizing the critical business processes. This process is part of the:

- ☐ balanced scorecard.
- ☐ business impact analysis (BIA).
- ☐ operations component of the business continuity plan (BCP).
- ☐ enterprise risk management plan.

Question 436

Which of the following attack best describe “Computer is the target of a crime” and “Computer is the tool of a crime”?

- ☐ Denial of Service (DoS) and Installing Key loggers
- ☐ War Driving and War Chalking
- ☐ Piggybacking and Race Condition
- ☐ Traffic analysis and Eavesdropping

Question 437

An IS auditor is reviewing an organization’s sales and purchasing system due to ongoing data quality issues. An analysis of which of the following would provide the MOST useful information to determine the revenue loss?

- ☐ Correlation between the number of issues and average downtime
- ☐ Cost of implementing data validation controls within the system
- ☐ Comparison of the cost of data acquisition and loss in sales revenue
- ☐ Correlation between data errors and loss in value of transactions

Question 438

Which of the following is the BEST way to evaluate the effectiveness of access controls to an internal network?

- ☐ Perform a system penetration test
- ☐ Test compliance with operating procedures
- ☐ Review access rights
- ☐ Review router configuration tables

Licensed to Berend Post berend.post@it-university.nl

Question 439

An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

- ☐ Appoint data quality champions across the organization
- ☐ Obtain error codes indicating failed data feeds
- ☐ Purchase data cleansing tools from a reputable vendor
- ☐ Implement business rules to reject invalid data

Question 440

ISO 9126 is a standard to assist in evaluating the quality of a product. Which of the following is defined as a set of attributes that bear on the existence of a set of functions and their specified properties?

- ☐ Reliability
- ☐ Usability
- ☐ Functionality
- ☐ Maintainability

Question 441

What can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program?

- ☐ Network-monitoring software
- ☐ A system downtime log
- ☐ Administration activity reports
- ☐ Help-desk utilization trend reports

Question 442

Which of the following should an IS auditor recommend to BEST enforce alignment of an IT project portfolio with strategic organizational priorities?

- ☐ Define a balanced scorecard (BSC) for measuring performance
- ☐ Consider user satisfaction in the key performance indicators (KPIs)
- ☐ Select projects according to business benefits and risks
- ☐ Modify the yearly process of defining the project portfolio

Licensed to Berend Post berend.post@it-university.nl

Question 443

When reviewing capacity monitoring, an IS auditor notices several incidents where storage capacity limits were reached, while the average utilization was below 30%. Which of the following would the IS auditor MOST likely identify as the root cause?

- ☐ The IT response to the alerts was too slow.
- ☐ The amount of data produced was unacceptable for operations.
- ☐ The storage space should have been enlarged in time.
- ☐ The dynamics of the utilization were not properly taken into account.

Question 444

Which of the following is the MOST effective mitigation strategy to protect confidential information from insider threats?

- ☐ Implementing authentication mechanisms
- ☐ Performing an entitlement review process
- ☐ Defining segregation of duties
- ☐ Establishing authorization controls.

Question 445

A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

- ☐ digest signature.
- ☐ electronic signature.
- ☐ digital signature.
- ☐ hash signature.

Question 446

An IT department has given a vendor remote access to the internal network for troubleshooting network performance problems. After discovering the remote activity during a firewall log review, which of the following is the BEST course of action for an information security manager?

- ☐ Revoke the access.
- ☐ Review the related service level agreement (SLA).
- ☐ Determine the level of access granted.
- ☐ Declare a security incident.

Licensed to Berend Post berend.post@it-university.nl

Question 447

An organization has established three IT processing environments: development, test, and production. The MAJOR reason for separating the development and test environments is to:

- ☐ obtain segregation of duties between IT staff and end users.
- ☐ limit the users' access rights to the test environment.
- ☐ perform testing in a stable environment.
- ☐ protect the programs under development from unauthorized testing.

Question 448

An IS auditor has imported data from the client's database. The next step-confirming whether the imported data are complete-is performed by:

- ☐ matching control totals of the imported data to control totals of the original data.
- ☐ sorting the data to confirm whether the data are in the same order as the original data.
- ☐ reviewing the printout of the first 100 records of original data with the first 100 records of imported data.
- ☐ filtering data for different categories and matching them to the original data.

Question 449

How is the risk of improper file access affected upon implementing a database system?

- ☐ Risk varies.
- ☐ Risk is reduced.
- ☐ Risk is not affected.
- ☐ Risk is increased.

Question 450

An IS auditor has been invited to join an IT project team responsible for building and deploying a new digital customer marketing platform. Which of the following is the BEST way for the auditor to support this project while maintaining independence?

- ☐ Develop selection criteria for potential digital technology vendors.
- ☐ Conduct an industry peer benchmarking exercise and advise on alternative solutions.
- ☐ Conduct a risk assessment of the proposed initiative.
- ☐ Design controls based on current regulatory requirements for digital technologies.

Licensed to Berend Post berend.post@it-university.nl

Question 451

The information security function in a large organization is MOST effective when:

- ☐ decentralized as close to the user as possible.
- ☐ the function reports directly to the IS operations manager.
- ☐ partnered with the IS development team to determine access rights.
- ☐ established at a corporate-wide level.

Question 452

Which of the following metrics would be MOST helpful to an IS auditor in evaluating an organization's security incident response management capability?

- ☐ Number of business interruptions due to IT security incidents per year.
- ☐ Number of IT security incidents reported per month
- ☐ Number of malware infections in business applications detected per day.
- ☐ Number of alerts generated by intrusion detection systems (IDS) per minute.

Question 453

Regarding digital signature implementation, which of the following answers is correct?

- ☐ A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's private key. Upon receiving the data, the recipient can decrypt the data using the sender's public key.
- ☐ A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's public key.
- ☐ A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value or message digest from the entire message contents. Upon receiving the data, the recipient can independently create it.
- ☐ A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's private key.

Question 454

In which of the following payment mode, an issuer attempts to emulate physical cash by creating digital certificates, which are purchased by users who redeem them with the issuer at a later date?

- ☐ Electronic Money Model
- ☐ Electronics Checks model
- ☐ Electronic transfer model
- ☐ Electronic withdraw model

Licensed to Berend Post berend.post@it-university.nl

Question 455

Which of the following roles combined with the role of a database administrator (DBA) will create a segregation of duties conflict?

- ☐ Quality assurance
- ☐ Systems analyst
- ☐ Application end user
- ☐ Security administrator

Question 456

Which of the following provides the framework for designing and developing logical access controls?

- ☐ Information systems security policy
- ☐ Access control lists
- ☐ Password management
- ☐ System configuration files

Question 457

An IS auditor should aware of various analysis models used by data architecture. Which of the following analysis model depict data entities and how they relate?

- ☐ Context Diagrams
- ☐ Activity Diagrams
- ☐ Swim-lane diagrams
- ☐ Entity relationship diagrams

Licensed to Berend Post berend.post@it-university.nl

Question 458

An IS auditor conducting a review of disaster recovery planning (DRP) at a financial processing organization has discovered the following:

-The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.
-The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting their attention.
- the plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.

The IS auditor's report should recommend that:

- ☐ the deputy CEO be censured for their failure to approve the plan.
- ☐ a board of senior managers is set up to review the existing plan.
- ☐ the existing plan is approved and circulated to all key management and staff.
- ☐ a manager coordinates the creation of a new or revised plan within a defined time limit.

Question 459

When reviewing an organization’s IT governance processes, which of the following provides the BEST indication that information security expectations are being met at all levels?

- ☐ Achievement of established security metrics
- ☐ Approval of the security program by senior management
- ☐ Utilization of an internationally recognized security standard
- ☐ Implementation of a comprehensive security awareness program

Question 460

What should IS auditors always check when auditing password files?

- ☐ That deleting password files is protected
- ☐ That password files are encrypted
- ☐ That password files are not accessible over the network
- ☐ That password files are archived

Licensed to Berend Post berend.post@it-university.nl

Question 461

Which of the following BEST ensures the integrity of a server's operating system?

- ☐ Protecting the server in a secure location
- ☐ Setting a boot password
- ☐ Hardening the server configuration
- ☐ Implementing activity logging

Question 462

Which of the following is the MOST effective data loss control when connecting a personally owned mobile device to the corporate email system?

- ☐ A senior manager must approve each new connection.
- ☐ Email synchronization must be prevented when connected to a public Wi-Fi hotspot.
- ☐ Email must be stored in an encrypted format on the mobile device.
- ☐ Users must agree to allow the mobile device to be wiped if it is lost.

Question 463

Which of the following is the unique identifier within and IPSec packet that enables the sending host to reference the security parameter to apply?

- ☐ SPI
- ☐ SA
- ☐ ESP
- ☐ AH

Question 464

In a public key infrastructure (PKI), which of the following may be relied upon to prove that an online transaction was authorized by a specific customer?

- ☐ Nonrepudiation
- ☐ Encryption
- ☐ Authentication
- ☐ Integrity

Licensed to Berend Post berend.post@it-university.nl

Question 465

An IS auditor is reviewing documentation of application systems change control and identifies several patches that were not tested before being put into production. Which of the following is the MOST significant risk from this situation?

- ☐ Developer access to production
- ☐ Lack of system integrity
- ☐ Outdated system documentation
- ☐ Loss of application support

Question 466

The PRIMARY objective of performing a postincident review is that it presents an opportunity to:

- ☐ improve internal control procedures.
- ☐ harden the network to industry best practices.
- ☐ highlight the importance of incident response management to management.
- ☐ improve employee awareness of the incident response process.

Question 467

Which of the following is a good tool to use to help enforcing the deployment of good passwords?

- ☐ password cracker
- ☐ local DoS attacker
- ☐ network hacker
- ☐ remote windowing tool
- ☐ None of the choices.

Question 468

Which of the following is a prerequisite to help ensure that IS hardware and software support the delivery of mission-critical functions?

- ☐ Control over IS infrastructure expenditure
- ☐ An independent audit of the process
- ☐ A comprehensive IS applications architecture
- ☐ Documented emergency change procedures

Licensed to Berend Post berend.post@it-university.nl

Question 469

Which of the following is MOST important to consider when developing a disaster recovery plan?

- ☐ Business continuity plan (BCP)
- ☐ Feasibility assessment
- ☐ Business impact analysis (BIA)
- ☐ Cost-benefit analysis

Question 470

An IS auditor is reviewing database log settings and notices that only INSERT and DELETE operations are being monitored in the database. What is the MOST significant risk?

- ☐ Metadata may not be logged
- ☐ Newly added records may not be logged
- ☐ Purged records may not be logged
- ☐ Changes to existing records may not be logged

Question 471

Which of the following methodologies is MOST appropriate to use for developing software with incomplete requirements?

- ☐ Process-based
- ☐ Critical chain
- ☐ Waterfall
- ☐ Agile

Question 472

In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

- ☐ Automated logging of changes to development libraries
- ☐ Additional staff to provide separation of duties
- ☐ Procedures that verify that only approved program changes are implemented
- ☐ Access controls to prevent the operator from making program modifications

Licensed to Berend Post berend.post@it-university.nl

Question 473

One major improvement in WPA over WEP is the use of a protocol which dynamically changes keys as the system is used. What protocol is this?

- ☐ SKIP
- ☐ RKIP
- ☐ OKIP
- ☐ EKIP
- ☐ TKIP
- ☐ None of the choices.

Question 474

An IS auditor discovers that validation controls in a web application have been moved from the server side into the browser to boost performance. This would MOST likely increase the risk of a successful attack by:

- ☐ phishing
- ☐ structured query language (SQL) injection
- ☐ denial of service (DoS)
- ☐ buffer overflow

Question 475

Which of the following is by far the most common prevention system from a network security perspective?

- ☐ Firewall
- ☐ IDS
- ☐ IPS
- ☐ Hardened OS
- ☐ Tripwire
- ☐ None of the choices.

Question 476

Which of the following would be MOST useful when analyzing computer performance?

- ☐ Report of off-peak utilization and response time
- ☐ Tuning of system software to optimize resource usage
- ☐ Operations report of user dissatisfaction with response time
- ☐ Statistical metrics measuring capacity utilization

Licensed to Berend Post berend.post@it-university.nl

Question 477

Which of the following is an attribute of the control self-assessment (CSA) approach?

- ☐ Broad stakeholder involvement
- ☐ Auditors are the primary control analysts
- ☐ Limited employee participation
- ☐ Policy driven

Question 478

Which of the following data validation edits is effective in detecting transposition and transcription errors?

- ☐ Range check
- ☐ Check digit
- ☐ Validity check
- ☐ Duplicate check

Question 479

Which of the following are valid examples of Malware:

- ☐ viruses
- ☐ worms
- ☐ trojan horses
- ☐ spyware
- ☐ All of the above

Question 480

Which of the following is the MOST important advantage of participating in beta testing of software products?

- ☐ It improves vendor support and training.
- ☐ It enables an organization to gain familiarity with new products and their functionality.
- ☐ It increases an organization's ability to retain staff who prefer to work with new technology.
- ☐ It enhances security and confidentiality.

Licensed to Berend Post berend.post@it-university.nl

Question 481

Which of the following provides the MOST helpful information to determine how much data an organization can afford to lose when a critical system failure occurs?

- ☐ Industry data loss statistics
- ☐ Risk assessment results
- ☐ Recovery point objective (RPO)
- ☐ Recovery time objective (RTO)

Question 482

Which of the following is the MOST important benefit of involving IS audit when implementing governance of enterprise IT?

- ☐ Identifying relevant roles for an enterprise IT governance framework
- ☐ Verifying that legal, regulatory and contractual requirements are being met
- ☐ Making decisions regarding risk response and monitoring of residual risk
- ☐ Providing independent and objective feedback to facilitate improvement of IT processes

Question 483

Which of the following is the PRIMARY objective of implementing IT governance?

- ☐ Resource management
- ☐ Performance measurement
- ☐ Value delivery
- ☐ Strategic planning

Question 484

A contract bid is digitally signed and electronically mailed. The PRIMARY advantage to using a digital signature is that:

- ☐ the bid cannot be forged even if the keys are compromised.
- ☐ the bid and the signature can be copied from one document to another.
- ☐ the signature can be authenticated even if no encryption is used.
- ☐ any alteration of the bid will invalidate the signature.

Licensed to Berend Post berend.post@it-university.nl

Question 485

Which of the following is the BEST way to improve the timely reporting of information security incidents?

- ☐ Perform periodic simulations with the incident response team.
- ☐ Incorporate security procedures in help desk processes.
- ☐ Integrate an intrusion detection system (IDS) in the DMZ.
- ☐ Regularly reassess and update the incident response plan.

Question 486

Which of the following is MOST important to include in a contract with a critical service provider to help ensure alignment with the organization's information security program?

- ☐ Escalation paths
- ☐ Right-to-audit clause
- ☐ Termination language
- ☐ Key performance indicators (KPIs)

Question 487

Which of the following layer of an enterprise data flow architecture is concerned with transporting information between the various layers?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☐ Application messaging layer
- ☐ Data access layer

Question 488

During what process should router access control lists be reviewed?

- ☐ Environmental review
- ☐ Network security review
- ☐ Business continuity review
- ☐ Data integrity review

Licensed to Berend Post berend.post@it-university.nl

Question 489

An IS auditor has completed an audit of an organization's accounts payable system. Which of the following should be rated as the HIGHEST risk in the audit report and requires immediate remediation?

- ☐ Lack of segregation of duty controls for reconciliation of payment transactions
- ☐ Lack of segregation of duty controls for removal of vendor records
- ☐ Lack of segregation of duty controls for updating the vendor master file
- ☐ Lack of segregation of duty controls for reversing payment transactions

Question 490

An IS auditor discovers a recurring software control process issue that severely impacts the efficiency of a critical business process. Which of the following is the BEST recommendation?

- ☐ Replace the malfunctioning system.
- ☐ Determine the compensating controls.
- ☐ Identify other impacted processes.
- ☐ Determine the root cause of the issue.

Question 491

Digital signatures are an effective control method for information exchange over an insecure network because they:

- ☐ enable nonrepudiation.
- ☐ are under the sole custody of the receiver.
- ☐ are constant over time.
- ☐ authenticate the user biometrically.

Question 492

A development team has designed a new application and incorporated best practices for secure coding. Prior to launch, which of the following is the IS auditor's BEST recommendation to mitigate the associated security risk?

- ☐ User acceptance testing
- ☐ Unit testing
- ☐ Integration testing
- ☐ Penetration testing

Licensed to Berend Post berend.post@it-university.nl

Question 493

Who is responsible for restricting and monitoring access of a data user?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☐ Security Administrator

Question 494

To BEST evaluate the effectiveness of a disaster recovery plan, the IS auditor should review the:

- ☐ test plan and results of past tests.
- ☐ plans and procedures in the business continuity plan.
- ☐ capacity of backup facilities.
- ☐ hardware and software inventory.

Question 495

Which of the following protocols would be involved in the implementation of a router and an interconnectivity device monitoring system?

- ☐ Simple Network Management Protocol
- ☐ File Transfer Protocol
- ☐ Simple Mail Transfer Protocol
- ☐ Telnet

Question 496

The MOST important success factor in planning a penetration test is:

- ☐ the documentation of the planned testing procedure.
- ☐ scheduling and deciding on the timed length of the test.
- ☐ the involvement of the management of the client organization.
- ☐ the qualifications and experience of staff involved in the test.

Question 497

A reduction in which of the following would indicate improved performance in the administration of information security?

- ☐ IT security awareness training days
- ☐ Number of staff involved in security administration
- ☐ Systems subject to an intrusion detection process
- ☐ Turnaround time for requests for new user access

Licensed to Berend Post berend.post@it-university.nl

Question 498

An IS auditor is reviewing an organization's incident management processes and procedures. Which of the following observations should be the auditor's GREATEST concern?

- ☐ Ineffective incident classification
- ☐ Ineffective incident prioritization
- ☐ Ineffective incident detection
- ☐ Ineffective post-incident review

Question 499

Adopting a service-oriented architecture would MOST likely:

- ☐ inhibit integration with legacy systems.
- ☐ compromise application software security.
- ☐ facilitate connectivity between partners.
- ☐ streamline all internal processes.

Question 500

Which of the following antivirus software implementation strategies would be the MOST effective in an interconnected corporate network?

- ☐ Server antivirus software
- ☐ Virus walls
- ☐ Workstation antivirus software
- ☐ Virus signature updating

Question 501

Which of the following should an IS auditor use to detect duplicate invoice records within an invoice master file?

- ☐ Attribute sampling
- ☐ Generalized audit software (GAS)
- ☐ Test data
- ☐ Integrated test facility (ITF)

Question 502

Diskless workstation is an example of:

- ☐ Handheld devices
- ☐ Thin client computer
- ☐ Personal computer
- ☐ Midrange server

Licensed to Berend Post berend.post@it-university.nl

Question 503

An IS auditor is evaluating a virtual server environment and learns that the production server, development server, and management console are housed in the same physical host. What should be the auditor's PRIMARY concern?

- ☐ The physical host is a single point of failure
- ☐ The management console is a single point of failure
- ☐ The development server and management console share the same host
- ☐ The development and production servers share the same host

Question 504

An IS auditor is analyzing a sample of accesses recorded on the system log of an application. The auditor intends to launch an intensive investigation if one exception is found. Which sampling method would be appropriate?

- ☐ Discovery sampling
- ☐ Variable sampling
- ☐ Stratified sampling
- ☐ Judgmental sampling

Question 505

An IS auditor is performing an audit of a large organization's operating system maintenance procedures. Which of the following findings presents the GREATEST risk?

- ☐ Some internal servers cannot be patched due to software incompatibility.
- ☐ The configuration management database is not up-to-date.
- ☐ Vulnerability testing is not performed on the development servers.
- ☐ Critical patches are applied immediately while others follow quarterly release cycles.

Question 506

Which of the following is a key success factor for implementing IT governance?

- ☐ Embedding quality assurance processes
- ☐ Establishing an IT governance committee
- ☐ Aligning IT and business strategies
- ☐ Delivering IT projects within budget

Licensed to Berend Post berend.post@it-university.nl

Question 507

An IS auditor reviewing a new application for compliance with information privacy principles should be the MOST concerned with:

- ☐ nonrepudiation
- ☐ collection limitation
- ☐ availability
- ☐ awareness

Question 508

An organization is using a single account shared by personnel for its social networking marketing page. Which of the following is the BEST method to maintain accountability over the account?

- ☐ Reviewing access rights on a periodic basis
- ☐ Integrating the account with a single sign-on
- ☐ Regular monitoring of proxy server logs
- ☐ Implementing an account password check-out process

Question 509

Which of the following is MOST important for the IS auditor to verify when reviewing the development process of a security policy?

- ☐ Evidence of active involvement of key stakeholders
- ☐ Output from the enterprise's risk management system
- ☐ Identification of the control framework
- ☐ Evidence of management approval

Question 510

An organization is disposing of a number of laptop computers. Which of the following data destruction methods would be the MOST effective?

- ☐ Run a low-level data wipe utility on all hard drives
- ☐ Erase all data file directories
- ☐ Format all hard drives
- ☐ Physical destruction of the hard drive

Licensed to Berend Post berend.post@it-university.nl

Question 511

Following an IS audit, which of the following types of risk would be MOST critical to communicate to key stakeholders?

- ☐ Control
- ☐ Residual
- ☐ Audit
- ☐ Inherent

Question 512

Which of the following would BEST ensure the confidentiality of sensitive data during transmission?

- ☐ Restricting the recipient through destination IP addresses
- ☐ Sending data over public networks using Secure Sockets Layer (SSL)
- ☐ Password protecting data over virtual local area networks (VLAN)
- ☐ Sending data through proxy servers

Question 513

An IS auditor determines that a business continuity plan has not been reviewed and approved by management. Which of the following is the MOST significant risk associated with this situation?

- ☐ Continuity planning may be subject to resource constraints.
- ☐ The plan may not be aligned with industry best practice.
- ☐ Critical business processes may not be addressed adequately.
- ☐ The plan has not been reviewed by risk management.

Question 514

Following an IS audit recommendation, all Telnet and File Transfer Protocol (FTP) connections have been replaced by Secure Socket Shell (SSH) and Secure File Transfer Protocol (SFTP). Which risk treatment approach has the organization adopted?

- ☐ Acceptance
- ☐ Mitigation
- ☐ Avoidance
- ☐ Transfer

Licensed to Berend Post berend.post@it-university.nl

Question 515

Which of the following is the MOST effective type of antivirus software?

- ☐ Scanners
- ☐ Active monitors
- ☐ integrity checkers
- ☐ Vaccines

Question 516

Which of the following is the BEST method for determining the criticality of each application system in the production environment?

- ☐ interview the application programmers.
- ☐ Perform a gap analysis.
- ☐ Review the most recent application audits.
- ☐ Perform a business impact analysis.

Question 517

Which of the following is the MOST effective way to verify an organization's ability to continue its essential business operations after a disruption event? Analysis of:

- ☐ end-to-end recovery flow
- ☐ recovery point objectives (RPOs)
- ☐ call trees
- ☐ business impact analysis (BIA)

Question 518

Which of the following is a standard secure email protection protocol?

- ☐ S/MIME
- ☐ SSH
- ☐ SET
- ☐ S/HTTP

Question 519

Which of the following application input controls would MOST likely detect data input errors in the customer account number field during the processing of an accounts receivable transaction?

- ☐ Validity check
- ☐ Reasonableness check
- ☐ Parity check
- ☐ Limit check

Licensed to Berend Post berend.post@it-university.nl

Question 520

Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

- ☐ Response
- ☐ Correction
- ☐ Detection
- ☐ Monitoring

Question 521

Which of the following attack includes social engineering, link manipulation or web site forgery techniques?

- ☐ surf attack
- ☐ Traffic analysis
- ☐ Phishing
- ☐ Interrupt attack

Question 522

Management considered two projections for its business continuity plan; plan A with two months to recover and plan B with eight months to recover. The recovery objectives are the same in both plans. It is reasonable to expect that plan B projected higher:

- ☐ downtime costs.
- ☐ resumption costs.
- ☐ recovery costs.
- ☐ walkthrough costs.

Question 523

Which of the following process consist of identification and selection of data from the imaged data set in computer forensics?

- ☐ Investigation
- ☐ Interrogation
- ☐ Reporting
- ☐ Extraction

Licensed to Berend Post berend.post@it-university.nl

Question 524

Which of the following is the BEST method for converting a file into a format suitable for data analysis in a forensic investigation?

- ☐ Extraction
- ☐ Normalization
- ☐ Data acquisition
- ☐ Imaging

Question 525

The IS auditor of a power company finds that the radio link to a remote mountain site is experiencing systematic outages under specific weather conditions. The communications manager explains that increasing the radio power would require a new license and would help little. What is the MOST appropriate action by the IS auditor?

- ☐ Recommend that the site's data collection and transmission be non-interruptible.
- ☐ Review the installation license, permissions and associated costs.
- ☐ Recommend that the site's hardware be upgraded to record data during outages.
- ☐ Gather additional information to identify threats, vulnerabilities, and impact.

Question 526

The MOST likely explanation for the use of applets in an Internet application is that:

- ☐ it is sent over the network from the server.
- ☐ the server does not run the program and the output is not sent over the network.
- ☐ they improve the performance of the web server and network.
- ☐ it is a JAVA program downloaded through the web browser and executed by the web server of the client machine.

Question 527

Performance monitoring tools report that servers are significantly below their planned utilization. Which of the following would be the BEST recommendation?

- ☐ Consolidate physical servers.
- ☐ Review the capacity plan.
- ☐ Deploy load balancing.
- ☐ Reconfigure server settings.

Licensed to Berend Post berend.post@it-university.nl

Question 528

Which of the following Confidentiality, Integrity, Availability (CIA) attribute supports the principle of least privilege by providing access to information only to authorized and intended users?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Accuracy

Question 529

Which of the following transmission media uses a transponder to send information?

- ☐ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Coaxial cable

Question 530

What type of risk is associated with authorized program exits (trap doors)?

- ☐ Business risk
- ☐ Audit risk
- ☐ Detective risk
- ☐ Inherent risk

Question 531

An organization developed a comprehensive three-year IT strategic plan. Halfway into the plan, a major legislative change impacting the organization is enacted. Which of the following should be management's NEXTcourse of action?

- ☐ Develop specific procedural documentation related to the changed legislation.
- ☐ Assess the legislation to determine whether are required to the strategic IT plan.
- ☐ Perform a risk management of the legislative changes.
- ☐ Develop a new IT strategic plan that encompasses the new legislation.

Licensed to Berend Post berend.post@it-university.nl

Question 532

The BEST data backup strategy for mobile users is to:

- ☐ synchronize data directories automatically over the network.
- ☐ have them regularly back up data directories onto CD and courier the backups to the head office.
- ☐ mirror all data to a portable storage device.
- ☐ have them regularly go to branch offices to perform backups.

Question 533

Which of the following should be the MOST important criterion in evaluating a backup solution for sensitive data that must be retained for a long period of time due to regulatory requirements?

- ☐ Full backup window
- ☐ Media costs
- ☐ Restore window
- ☐ Media reliability

Question 534

An IS auditor is involved with a project and finds an IT project stakeholder wants to make a change that could affect both the project scope and schedule. Which of the following would be the MOST appropriate action for the project manager with respect to the change request?

- ☐ Recommend to the project sponsor whether to approve the change
- ☐ Modify the project plan as a result of the change
- ☐ Evaluate the impact of the change
- ☐ Ignore out-of-scope requests

Question 535

What would be of GREATEST concern to an IS auditor observing shared key cards being utilized to access an organization's data center?

- ☐ The lack of a multi-factor authentication system
- ☐ The inability to identify who has entered the data center
- ☐ The inability to track the number of misplaced cards
- ☐ The lack of enforcement of organizational policy and procedures

Licensed to Berend Post berend.post@it-university.nl

Question 536

The use of the Transport Layer Security (TLS) protocol enables the client in a network to be:

- ☐ provided with a digital certificate.
- ☐ identified by a password.
- ☐ registered by the server.
- ☐ assured of the server's identity.

Question 537

Which of the following areas of responsibility would cause the GREATEST segregation of duties conflict if the individual who performs the related tasks also has approval authority?

- ☐ Purchase requisitions and purchase orders
- ☐ Invoices and reconciliations
- ☐ Vendor selection and statements of work
- ☐ Good receipts and payments

Question 538

Which of the following layer of an enterprise data flow architecture is concerned with the assembly and preparation of data for loading into data marts?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☐ Data Mart layer
- ☐ Data access layer

Question 539

Which of the following would BEST justify spending for a compensating control?

- ☐ Peer benchmarking
- ☐ Risk analysis
- ☐ Threat analysis
- ☐ Vulnerability analysis

Licensed to Berend Post berend.post@it-university.nl

Question 540

An IS auditor observes a weakness in the tape management system at a data center in that some parameters are set to bypass or ignore tape header records. Which of the following is the MOST effective compensating control for this weakness?

- ☐ Staging and job set up
- ☐ Supervisory review of logs
- ☐ Regular back-up of tapes
- ☐ Offsite storage of tapes

Question 541

When evaluating the controls of an EDI application, an IS auditor should PRIMARILY be concerned with the risk of:

- ☐ excessive transaction turnaround time.
- ☐ application interface failure.
- ☐ improper transaction authorization.
- ☐ no validated batch totals.

Question 542

During a business continuity audit an IS auditor found that the business continuity plan (BCP) covered only critical processes. The IS auditor should:

- ☐ recommend that the BCP cover all business processes.
- ☐ assess the impact of the processes not covered.
- ☐ report the findings to the IT manager.
- ☐ redefine critical processes.

Question 543

A technology service organization has recently acquired a new subsidiary. What should be the IS auditor's NEXT course of action when considering the impact on the development of the IT audit plan?

- ☐ Review the revised business impact analysis (BIA).
- ☐ Proceed with the current audit plan.
- ☐ Perform a risk assessment.
- ☐ Include the new systems in the audit plan.

Licensed to Berend Post berend.post@it-university.nl

Question 544

During an audit of an organization's financial statements, an IS auditor finds that the IT general controls are deficient. What should the IS auditor recommend?

- ☐ Increase the compliance testing of the application controls.
- ☐ Place greater reliance on the application controls.
- ☐ Increase the substantive testing of the financial balances.
- ☐ Place greater reliance on the framework of control.

Question 545

An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance. Which of the following would provide the MOST useful information for planning purposes?

- ☐ Results from a business impact analysis
- ☐ Results from a gap analysis
- ☐ An inventory of security controls currently in place
- ☐ Deadline and penalties for noncompliance

Question 546

Which of the following should be PRIMARILY included in a security training program for business process owners?

- ☐ Application vulnerabilities
- ☐ List of security incidents reported
- ☐ Application recovery time
- ☐ Impact of security risks

Question 547

Which of the following should be an IS auditor's PRIMARY focus when developing a risk-based IS audit program?

- ☐ Business plans
- ☐ Business processes
- ☐ IT strategic plans
- ☐ Portfolio management

Licensed to Berend Post berend.post@it-university.nl

Question 548

Which of the following would be the MOST likely reason for an intrusion prevention system (IPS) being unable to block an ongoing web attack?

- ☐ The firewall is not configured properly.
- ☐ The network design contains flaws.
- ☐ Monitoring personnel are not proactive.
- ☐ Signatures are outdated.

Question 549

The sender of a public key would be authenticated by a:

- ☐ certificate authority,
- ☐ digital signature.
- ☐ digital certificate.
- ☐ registration authority.

Question 550

Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a pattern of behaviors, effects, assumptions, attitude and ways of doing things?

- ☐ Governing
- ☐ Culture
- ☐ Enabling and support
- ☐ Emergence

Question 551

From a risk management perspective, which of the following is MOST important to be tracked in continuous monitoring?

- ☐ Number of prevented attacks
- ☐ Changes in the threat environment
- ☐ Changes in user privileges
- ☐ Number of failed logins

Licensed to Berend Post berend.post@it-university.nl

Question 552

An IS auditor has completed a network audit. Which of the following is the MOST significant logical security finding?

- ☐ Network workstations are not disabled automatically after a period of inactivity.
- ☐ Wiring closets are left unlocked
- ☐ Network operating manuals and documentation are not properly secured.
- ☐ Network components are not equipped with an uninterruptible power supply.

Question 553

Which of the following refers to a method of bypassing normal system authentication procedures?

- ☐ virus
- ☐ worm
- ☐ trojan horse
- ☐ spyware
- ☐ rootkits
- ☐ backdoor
- ☐ None of the choices.

Question 554

A multinational organization is integrating its existing payroll system with a human resource information system. Which of the following should be of GREATEST concern to the IS auditor?

- ☐ System documentation
- ☐ Currency conversion
- ☐ Application interfaces
- ☐ Scope creep

Question 555

Which of the following is the MOST important issue for an IS auditor to consider with regard to VoIP communications?

- ☐ Continuity of service
- ☐ Homogeneity of the network
- ☐ Nonrepudiation
- ☐ Identity management

Licensed to Berend Post berend.post@it-university.nl

Question 556

In a small organization, developers may release emergency changes directly to production. Which of the following will BEST control the risk in this situation?

- ☐ Approve and document the change the next business day
- ☐ Limit developer access to production to a specific timeframe
- ☐ Obtain secondary approval before releasing to production
- ☐ Disable the compiler option in the production machine

Question 557

Which of the following statement correctly describes the difference between total flooding and local application extinguishing agent?

- ☐ The local application design contain physical barrier enclosing the fire space where as physical barrier is not present in total flooding extinguisher
- ☐ The total flooding design contain physical barrier enclosing the fire space where as physical barrier is not present in local application design extinguisher
- ☐ The physical barrier enclosing fire space is not present in total flooding and local application extinguisher agent
- ☐ The physical barrier enclosing fire space is present in total flooding and local application extinguisher agent

Question 558

Who assumes ownership of a systems-development project and the resulting system?

- ☐ User management
- ☐ Project steering committee
- ☐ IT management
- ☐ Systems developers

Question 559

During a follow-up audit, an IS auditor concludes that a previously identified issue has not been adequately remediated. The auditee insists the risk has been addressed. The auditor should:

- ☐ recommend an independent assessment by a third party
- ☐ report the disagreement according to established procedures
- ☐ follow-up on the finding next year
- ☐ accept the auditee's position and close the finding

Licensed to Berend Post berend.post@it-university.nl

Question 560

During an audit, an IS auditor notices that the IT department of a medium-sized organization has no separate risk management function, and the organization's operational risk documentation only contains a few broadly described IT risks. What is the MOST appropriate recommendation in this situation?

- ☐ Create an IT risk management department and establish an IT risk framework with the aid of external risk management experts.
- ☐ Use common industry standard aids to divide the existing risk documentation into several individual risks which will be easier to handle.
- ☐ No recommendation is necessary since the current approach is appropriate for a medium-sized organization.
- ☐ Establish regular IT risk management meetings to identify and assess risks, and create a mitigation plan as input to the organization's risk management.

Question 561

Which of the following should be performed immediately after a computer security incident has been detected and analyzed by an incident response team?

- ☐ Assess the impact of the incident on critical systems
- ☐ Categorize the incident
- ☐ Eradicate the component that caused the incident
- ☐ Contain the incident before it spreads

Question 562

An IS auditor has been asked to advise on the design and implementation of IT management best practices. Which of the following actions would impair the auditor’s independence?

- ☐ Providing consulting advice for managing applications
- ☐ Designing an embedded audit module
- ☐ Implementing risk response on management’s behalf
- ☐ Evaluating the risk management process

Question 563

The PRIMARY purpose of implementing Redundant Array of Inexpensive Disks (RAID) level 1 in a file server is to:

- ☐ achieve performance improvement.
- ☐ provide user authentication.
- ☐ ensure availability of data.
- ☐ ensure the confidentiality of data.

Licensed to Berend Post berend.post@it-university.nl

Question 564

Which of the following is the INCORRECT “layer - protocol data unit (PDU)" mapping within the TCP/IP model?

- ☐ Application layer – Data
- ☐ Transport layer – Segment
- ☐ Network layer – Frame
- ☐ Physical layer – bits

Question 565

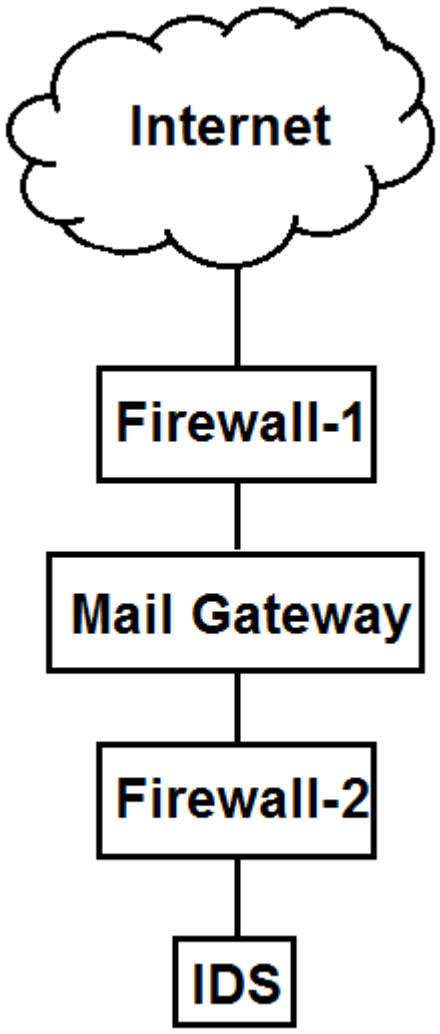
An IS auditor has found that a vendor has gone out of business and the escrow has an older version of the source code. What is the auditor’s BEST recommendation for the organization?

- ☐ Continue using the existing application since it meets the current requirements
- ☐ Prepare a maintenance plan that will support the application using the existing code
- ☐ Bring the escrow version up to date
- ☐ Undertake an analysis to determine the business risk

Licensed to Berend Post berend.post@it-university.nl

Question 566

E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network.



The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

- ☐ alert the appropriate staff.
- ☐ create an entry in the log.
- ☐ close firewall-2.
- ☐ close firewall-1.

Licensed to Berend Post berend.post@it-university.nl

Question 567

When testing segregation of duties, which of the following audit techniques provides the MOST reliable evidence?

- ☐ Observing daily operations for the area in scope
- ☐ Evaluating the department structure via the organizational chart
- ☐ Reviewing departmental procedure handbooks
- ☐ Interviewing managers and end users

Question 568

The PRIMARY reason for allocating sufficient time between the "go-live" phase of a new system and conducting a post-implementation review is to:

- ☐ update project requirements and design documentation
- ☐ increase availability of system implementation team resources
- ☐ allow the system to stabilize in production
- ☐ obtain sign-off on the scope of post-implementation review

Question 569

When implementing an IT governance framework in an organization the MOST important objective is:

- ☐ IT alignment with the business.
- ☐ accountability.
- ☐ value realization with IT.
- ☐ enhancing the return on IT investments.

Question 570

The PRIMARY purpose of audit trails is to:

- ☐ improve response time for users.
- ☐ establish accountability and responsibility for processed transactions.
- ☐ improve the operational efficiency of the system.
- ☐ provide useful information to auditors who may wish to track transactions

Licensed to Berend Post berend.post@it-university.nl

Question 571

Which of the following is the BEST approach to identify noncompliance issues with legal, regulatory, and contractual requirements?

- ☐ Vulnerability assessment
- ☐ Risk assessment
- ☐ Business impact analysis (BIA)
- ☐ Gap analysis

Question 572

What is an IS auditor's BEST course of action when provided with a status update indicating audit recommendations related to segregation of duties for financial staff have been implemented?

- ☐ Verify sufficient segregation of duties controls are in place.
- ☐ Request documentation of the segregation of duties policy and procedures.
- ☐ Note the department's response in the audit workpapers and records.
- ☐ Confirm with the business that the recommendations are implemented.

Question 573

A shared resource matrix is a technique commonly used to locate:

- ☐ Malicious code
- ☐ Security flaws
- ☐ Trap doors
- ☐ Covert channels

Question 574

A business has requested an IS audit to determine whether information stored in an application system is adequately protected. Which of the following is the MOST important action before the audit work begins?

- ☐ Establish control objectives
- ☐ Conduct a vulnerability analysis
- ☐ Perform penetration testing
- ☐ Review remediation reports

Licensed to Berend Post berend.post@it-university.nl

Question 575

Which of the following is the BEST approach for determining the maturity level of an information security program?

- ☐ Review internal audit results.
- ☐ Engage a third-party review.
- ☐ Perform a self-assessment.
- ☐ Evaluate key performance indicators (KPIs).

Question 576

Which of the following BEST describes a common risk in implementing a new application software package?

- ☐ Parameter settings are incorrect
- ☐ Transaction volume is excessive
- ☐ Sensitivity of transactions is high
- ☐ The application lacks audit trails

Question 577

Disaster recovery planning for network connectivity to a hot site over a public-switched network would be MOST likely to include:

- ☐ minimizing the number of points of presence
- ☐ contracts for acquiring new leased lines
- ☐ reciprocal agreements with customers of that network
- ☐ redirecting private virtual circuits

Question 578

An IS auditor needs to consider many factors while evaluating an encryption system. Which of the following is LEAST important factor to be considered while evaluating an encryption system?

- ☐ Encryption algorithm
- ☐ Encryption keys
- ☐ Key length
- ☐ Implementation language

Licensed to Berend Post berend.post@it-university.nl

Question 579

Which of the following is the client organization's responsibility in a Software as a Service (SaaS) environment?

- ☐ Detecting unauthorized access
- ☐ Ensuring that users are properly authorized
- ☐ Ensuring the data is available when needed
- ☐ Preventing insertion of malicious code

Question 580

A third-party service provider has proposed a data loss prevention (DLP) solution. Which of the following MUST be in place for this solution to be relevant to the organization?

- ☐ An adequate data testing environment
- ☐ Senior management support
- ☐ A business case
- ☐ A data classification

Question 581

What is the BEST approach to mitigate the risk of a phishing attack?

- ☐ implement an intrusion detection system (IDS)
- ☐ Assess web site security
- ☐ Strong authentication
- ☐ User education

Question 582

Which of the following MOST effectively prevents internal users from modifying sensitive data?

- ☐ Network segmentation
- ☐ Multi-factor authentication
- ☐ Acceptable use policies
- ☐ Role-based access controls

Question 583

When reviewing a hardware maintenance program, an IS auditor should assess whether:

- ☐ the schedule of all unplanned maintenance is maintained.
- ☐ it is in line with historical trends.
- ☐ it has been approved by the IS steering committee.
- ☐ the program is validated against vendor specifications.

Licensed to Berend Post berend.post@it-university.nl

Question 584

An organization has suffered a number of incidents in which USB flash drives with sensitive data have been lost. Which of the following would be MOST effective in preventing loss of sensitive data?

- ☐ Modifying the disciplinary policy to be more stringent
- ☐ Implementing a check-in/check-out process for USB flash drives
- ☐ Issuing encrypted USB flash drives to staff
- ☐ Increasing the frequency of security awareness training

Question 585

An internal IS auditor recommends that incoming accounts payable payment files be encrypted. Which type of control is the auditor recommending?

- ☐ Corrective
- ☐ Detective
- ☐ Preventive
- ☐ Directive

Question 586

An IS auditor finds that a company is using a payroll provider hosted in a foreign country. Of the following, the MOST important audit consideration is whether the provider's operations:

- ☐ meet industry best practice and standards
- ☐ comply with applicable laws and regulations
- ☐ are shared with other companies using the provider
- ☐ are aligned with the company's culture

Question 587

The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

- ☐ testing stage.
- ☐ evaluation stage.
- ☐ maintenance stage.
- ☐ early stages of planning.

Licensed to Berend Post berend.post@it-university.nl

Question 588

John had implemented a validation check on the marital status field of a payroll record. A payroll record contains a field for marital status and acceptable status code are M for Married or S for Single. If any other code is entered, record should be rejected. Which of the following data validation control was implemented by John?

- ☐ Range Check
- ☐ Validity Check
- ☐ Existence check
- ☐ Reasonableness check

Question 589

An IS auditor plans to review all access attempts to a video-monitored and proximity card-controlled communications room. Which of the following would be MOST useful to the auditor?

- ☐ System electronic log
- ☐ Security incident log
- ☐ Manual sign-in and sign-out log
- ☐ Alarm system with CCTV

Question 590

Which of the following encrypt/decrypt steps provides the GREATEST assurance of achieving confidentiality, message integrity and nonrepudiation by either sender or recipient?

- ☐ The recipient uses their private key to decrypt the secret key.
- ☐ The encrypted prehash code and the message are encrypted using a secret key.
- ☐ The encrypted prehash code is derived mathematically from the message to be sent.
- ☐ The recipient uses the sender's public key, verified with a certificate authority, to decrypt the prehash code.

Question 591

An organization's IT department is undertaking a large virtualization project to reduce its physical server footprint. Which of the following should be the HIGHEST priority of the information security manager?

- ☐ Determining how incidents will be managed
- ☐ Selecting the virtualization software
- ☐ Being involved as the design stage of the project
- ☐ Ensuring the project has appropriate security funding

Licensed to Berend Post berend.post@it-university.nl

Question 592

Which of the following controls would be the MOST comprehensive in a remote access network with multiple and diverse subsystems?

- ☐ Proxy server
- ☐ Firewall installation
- ☐ Network administrator
- ☐ Password implementation and administration

Question 593

Which of the following issues should be the GREATEST concern to the IS auditor when reviewing an IT disaster recovery test?

- ☐ Due to the limited test time window, only the most essential systems were tested. The other systems were tested separately during the rest of the year.
- ☐ During the test it was noticed that some of the backup systems were defective or not working, causing the test of these systems to fail.
- ☐ The procedures to shut down and secure the original production site before starting the backup site required far more time than planned.
- ☐ Every year, the same employees perform the test. The recovery plan documents are not used since every step is well known by all participants.

Question 594

Most access violations are:

- ☐ Accidental
- ☐ Caused by internal hackers
- ☐ Caused by external hackers
- ☐ Related to Internet

Question 595

An IS auditor is evaluating the log management system for an organization with devices and systems in multiple geographic locations. Which of the following is MOST important for the auditor to verify?

- ☐ Log files are encrypted and digitally signed.
- ☐ Log files of the servers are synchronized.
- ☐ Log files are reviewed in multiple locations.
- ☐ Log files are concurrently updated.

Licensed to Berend Post berend.post@it-university.nl

Question 596

During an annual security review of an organization's servers, it was found that the customer service team's file server, which contains sensitive customer data, is accessible to all user IDs in the organization. Which of the following should the information security manager do FIRST?

- ☐ Report the situation to the data owner.
- ☐ Remove access privileges to the folder containing the data.
- ☐ Train the customer service team on properly controlling file permissions.
- ☐ Isolate the server from the network.

Question 597

A company is planning to implement a new administrative system at many sites. The new system contains four integrated modules. Which of the following implementation approaches would be MOST appropriate?

- ☐ Parallel implementation module by module
- ☐ Pilot run of the new system
- ☐ Full implementation of the new system
- ☐ Parallel run at all locations

Question 598

The FIRST step in managing the risk of a cyber-attack is to:

- ☐ assess the vulnerability impact.
- ☐ evaluate the likelihood of threats.
- ☐ identify critical information assets.
- ☐ estimate potential damage.

Question 599

Which of the following is the GREATEST risk of cloud computing?

- ☐ Reduced performance
- ☐ Disclosure of data
- ☐ Lack of scalability
- ☐ Inflexibility

Licensed to Berend Post berend.post@it-university.nl

Question 600

Which of the following should the IS auditor use to BEST determine whether a project has met its business objectives?

- ☐ Earned-value analysis
- ☐ Completed project plan
- ☐ Issues log with resolutions
- ☐ Benefits realization document

Question 601

In an organization that has undergone an expansion through an acquisition, which of the following would BEST secure the enterprise network?

- ☐ Business or role-based segmentation
- ☐ Using security groups
- ☐ Log analysis of system access
- ☐ Encryption of data traversing networks.

Question 602

An IS auditor can BEST help management fulfill risk management responsibilities by:

- ☐ highlighting specific risks not being addressed.
- ☐ ensuring the roles for managing IT risk are defined.
- ☐ developing an IT risk management framework.
- ☐ adopting a mechanism for reporting issues.

Question 603

An organization has an approved bring your own device (BYOD) program. Which of the following is the MOST effective method to enforce application control on personal devices?

- ☐ Implement a mobile device management solution.
- ☐ Establish a mobile device acceptable use policy.
- ☐ Implement a web application firewall.
- ☐ Educate users regarding the use of approved applications.

Licensed to Berend Post berend.post@it-university.nl

Question 604

A retailer normally uses a scanner to read product labels and input product codes and prices. The unit is not functioning and staff are keying information manually. With respect to the accuracy of the input, it is likely that:

- ☐ audit risk has increased.
- ☐ control risk has increased.
- ☐ inherent risk has decreased.
- ☐ detection risk has decreased.

Question 605

Which of the following term related to network performance refers to the delay that packet may experience on their way to reach the destination from the source?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Jitter

Question 606

An organization considers implementing a system that uses a technology that is not in line with the organization's IT strategy. Which of the following is the BEST justification for deviating from the IT strategy?

- ☐ The system has a reduced cost of ownership.
- ☐ The organization has staff familiar with the technology.
- ☐ The business benefits are achieved even with extra costs.
- ☐ The system makes use of state-of-the-art technology.

Question 607

An IS auditor finds that periodic reviews of read-only users for a reporting system are not being performed. Which of the following should be the IS auditor's NEXT course of action?

- ☐ Obtain a verbal confirmation from IT for this exemption.
- ☐ Review the list of end-users and evaluate for authorization.
- ☐ Verify management's approval for this exemption.
- ☐ Report this control process weakness to senior management.

Licensed to Berend Post berend.post@it-university.nl

Question 608

Which of the following represents the GREATEST potential risk in an EDI environment?

- ☐ Transaction authorization
- ☐ Loss or duplication of EDI transmissions
- ☐ Transmission delay
- ☐ Deletion or manipulation of transactions prior to or after establishment of application controls

Question 609

Which of the following findings would be of GREATEST concern to an IS auditor reviewing an organization's newly implemented online security awareness program?

- ☐ Only new employees are required to attend the program
- ☐ The timing for program updates has not been determined
- ☐ Metrics have not been established to assess training results
- ☐ Employees do not receive immediate notification of results

Question 610

Which of the following BEST describes the role of a directory server in a public key infrastructure (PKI)?

- ☐ Encrypts the information transmitted over the network
- ☐ Makes other users' certificates available to applications
- ☐ Facilitates the implementation of a password policy
- ☐ Stores certificate revocation lists (CRLs)

Question 611

In a public key infrastructure, a registration authority:

- ☐ verifies information supplied by the subject requesting a certificate.
- ☐ issues the certificate after the required attributes are verified and the keys are generated.
- ☐ digitally signs a message to achieve nonrepudiation of the signed message.
- ☐ registers signed messages to protect them from future repudiation.

Licensed to Berend Post berend.post@it-university.nl

Question 612

An organization's data retention policy states that all data will be backed up, retained for 10 years, and then destroyed. When conducting an audit of the long-term offsite backup program, an IS auditor should:

- ☐ verify that business owners review data before it is destroyed.
- ☐ verify that there is a process to ensure readability and restore capability.
- ☐ confirm that business interruption insurance coverage is in place.
- ☐ review data classification schemes for appropriate security levels.

Question 613

When auditing the effectiveness of a biometric system, which of the following indicators would be MOST important to review?

- ☐ False negatives
- ☐ False acceptance rate
- ☐ Failure to enroll rate
- ☐ System response time

Question 614

Which of the following is the MOST important requirement for an IS auditor to evaluate when reviewing a transmission of personally identifiable information (PII) between two organizations?

- ☐ Completeness
- ☐ Timeliness
- ☐ Necessity
- ☐ Accuracy

Question 615

One advantage of monetary unit sampling is the fact that:

- ☐ results are stated in terms of the frequency of items in error
- ☐ it can easily be applied manually when computer resources are not available
- ☐ it increases the likelihood of selecting material items from the population
- ☐ large-value population items are segregated and audited separately

Licensed to Berend Post berend.post@it-university.nl

Question 616

During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

- ☐ address audit objectives.
- ☐ collect sufficient evidence.
- ☐ specify appropriate tests.
- ☐ minimize audit resources.

Question 617

Which of the following should be the PRIMARY concern of an IS auditor during a review of an external IT service level agreement (SLA) for computer operations?

- ☐ No employee succession plan
- ☐ Changes in services are not tracked
- ☐ Lack of software escrow provisions
- ☐ Vendor has exclusive control of IT resources

Question 618

An IS auditor reviewing the acquisition of new equipment would consider which of the following to be a significant weakness?

- ☐ Staff involved in the evaluation were aware of the vendors being evaluated.
- ☐ Independent consultants prepared the request for proposal (RFP) documents.
- ☐ Evaluation criteria were finalized after the initial assessment of responses.
- ☐ The closing date for responses was extended after a request from potential vendors.

Question 619

Which of the following is the MOST important control to implement when senior managers use smartphones to access sensitive company information?

- ☐ Mandatory virtual private network (VPN) connectivity
- ☐ Centralized device administration
- ☐ Strong passwords
- ☐ Anti-malware on the devices

Licensed to Berend Post berend.post@it-university.nl

Question 620

Change control for business application systems being developed using prototyping could be complicated by the:

- ☐ iterative nature of prototyping.
- ☐ rapid pace of modifications in requirements and design.
- ☐ emphasis on reports and screens.
- ☐ lack of integrated tools.

Question 621

What should the information security manager do FISRT when end users express that new security controls are too restrictive?

- ☐ Perform a risk assessment on modifying the control environment.
- ☐ Perform a cost-benefit analysis on modifying the control environment.
- ☐ Conduct a business impact analysis (BIA).
- ☐ Obtain process owner buy-in to remove the controls.

Question 622

Which of the following statement correctly describes difference between SSL and S/HTTP?

- ☐ Both works at application layer of OSI model
- ☐ SSL works at transport layer where as S/HTTP works at application layer of OSI model
- ☐ Both works at transport layer
- ☐ S/HTTP works at transport layer where as SSL works at the application layer of OSI model

Question 623

To select a sample for testing, which must include the 80 largest client balances and a random sample of the rest, the IS auditor should recommend:

- ☐ sorting the file with a utility.
- ☐ use of generalized audit software.
- ☐ applying attribute sampling using software.
- ☐ development of an integrated test facility (ITF).

Licensed to Berend Post berend.post@it-university.nl

Question 624

A business unit cannot achieve desired segregation of duties between operations and programming due to size constraints. Which of the following is MOST important for the IS auditor to identify?

- ☐ Unauthorized user controls
- ☐ Compensating controls
- ☐ Controls over operational effectiveness
- ☐ Additional control weaknesses

Question 625

To integrate security into system development life cycle (SDLC) processes, an organization MUST ensure that security:

- ☐ is a prerequisite for completion of major phases.
- ☐ performance metrics have been met.
- ☐ roles and responsibilities have been defined.
- ☐ is represented on the configuration control board.

Question 626

Which of the following is the PRIMARY role of a data custodian?

- ☐ Processing information
- ☐ Securing information
- ☐ Classifying information
- ☐ Validating information

Question 627

An information security manager is preparing an incident response plan. Which of the following is the MOST important consideration when responding to an incident involving sensitive customer data?

- ☐ The assignment of a forensics teams
- ☐ The ability to recover from the incident in a timely manner
- ☐ Following defined post-incident review procedures
- ☐ The ability to obtain incident information in a timely manner

Licensed to Berend Post berend.post@it-university.nl

Question 628

Which of the following is the MOST important consideration when deploying closed-circuit television (CCTV) systems that use wireless communication links to transmit images between cameras and a receiver?

- ☐ Encryption of transmissions
- ☐ Monitoring by security guards
- ☐ Retention period of recordings
- ☐ Strategic placement of cameras

Question 629

After an external IS audit, which of the following should be IT management's MAIN consideration when determining the prioritization of follow-up activities?

- ☐ The amount of time since the initial audit was completed.
- ☐ The materiality of the reported findings
- ☐ The availability of the external auditors
- ☐ The scheduling of major changes in the control environment

Question 630

Which of the following is the PRIMARY purpose of conducting a business impact analysis (BIA)?

- ☐ Identifying risk mitigation options
- ☐ Identifying key business risks
- ☐ Identifying critical business processes
- ☐ Identifying the threat environment

Question 631

Which of the following should be the MOST important consideration when determining which information system application to audit?

- ☐ Cost-benefit analysis
- ☐ Available resources
- ☐ Business impact analysis
- ☐ Newly implemented systems

Licensed to Berend Post berend.post@it-university.nl

Question 632

Data confidentiality is a requirement for an organization's new web service. Which of the following would provide the BEST protection?

- ☐ Telnet
- ☐ Secure Sockets Layer (SSL)
- ☐ Transport Layer Security (TLS)
- ☐ Secure File Transfer Protocol (SFTP)

Question 633

An IS auditor has been asked to audit the proposed acquisition of new computer hardware. The auditor's PRIMARY concern is that:

- ☐ the implementation plan meets user requirements.
- ☐ a clear business case has been established.
- ☐ the new hardware meets established security standards.
- ☐ a full, visible audit trail will be included.

Question 634

Which of the following are the characteristics of a good password?

- ☐ It has mixed-case alphabetic characters, numbers, and symbols.
- ☐ It has mixed-case alphabetic characters and numbers.
- ☐ It has mixed-case alphabetic characters and symbols.
- ☐ It has mixed-case alphabetic characters, numbers, and binary codes.
- ☐ None of the choices.

Question 635

The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

- ☐ financial results.
- ☐ customer satisfaction.
- ☐ internal process efficiency.
- ☐ innovation capacity.

Licensed to Berend Post berend.post@it-university.nl

Question 636

When developing a risk-based IS audit plan, the PRIMARY focus should be on functions:

- ☐ considered important by IT management.
- ☐ with the most ineffective controls.
- ☐ with the greatest number of threats.
- ☐ considered critical to business operations.

Question 637

When developing a risk-based audit strategy, an IS auditor conduct a risk assessment to ensure that:

- ☐ controls needed to mitigate risks are in place.
- ☐ vulnerabilities and threats are identified.
- ☐ audit risks are considered.
- ☐ a gap analysis is appropriate.

Question 638

An IS auditor is conducting a review of an organization's information systems and discovers data that is no longer needed by business applications. Which of the following would be the IS auditor's BEST recommendation?

- ☐ Ask the data custodian to remove it after confirmation from the business user.
- ☐ Assess the data according to the retention policy.
- ☐ Back up the data to removable media and store in a secure area.
- ☐ Keep the data and protect it using a data classification policy.

Question 639

An IS auditor is assessing the results of an organization's post-implementation review of a newly developed information system. Which of the following should be the auditor's MAIN focus?

- ☐ The procurement contract has been closed.
- ☐ Lessons learned have been identified.
- ☐ The disaster recovery plan has been updated.
- ☐ Benefits realization analysis has been completed.

Question 640

The BEST way to evaluate the effectiveness of a newly developed application is to:

- ☐ perform a post-implementation review.
- ☐ analyze load-testing results.
- ☐ review acceptance-testing results.
- ☐ perform a pre-implementation review.

Licensed to Berend Post berend.post@it-university.nl

Question 641

Which of the following is the process of repeating a portion of a test scenario or test plan to ensure that changes in information system have not introduced any errors?

- ☐ Parallel Test
- ☐ Black box testing
- ☐ Regression Testing
- ☐ Pilot Testing

Question 642

Which of the following is the dominating objective of BCP and DRP?

- ☐ To protect human life
- ☐ To mitigate the risk and impact of a business interruption
- ☐ To eliminate the risk and impact of a business interruption
- ☐ To transfer the risk and impact of a business interruption

Question 643

The final acceptance testing of a new application system should be the responsibility of the:

- ☐ IS audit team.
- ☐ user group
- ☐ IS management
- ☐ quality assurance team

Question 644

Which of the following is the MOST important difference between end-user computing (EUC) applications and traditional applications?

- ☐ Traditional application documentation is typically less comprehensive than EUC application documentation.
- ☐ Traditional applications require roll-back procedures whereas EUC applications do not.
- ☐ Traditional applications require periodic patching whereas EUC applications do not.
- ☐ Traditional application input controls are typically more robust than EUC application input controls.

Licensed to Berend Post berend.post@it-university.nl

Question 645

In which of the following payment mode, the payer creates payment transfer instructions, signs it digitally and sends it to issuer?

- ☐ Electronic Money Model
- ☐ Electronics Checks model
- ☐ Electronic transfer model
- ☐ Electronic withdraw model

Question 646

What is often the most difficult part of initial efforts in application development?

- ☐ Configuring software
- ☐ Planning security
- ☐ Determining time and resource requirements
- ☐ Configuring hardware

Question 647

Two organizations will share ownership of a new enterprise resource management (ERM) system. To help ensure the successful implementation of the system, it is MOST important to define:

- ☐ access to data
- ☐ the governance model
- ☐ custody of assets
- ☐ appropriate procedures

Question 648

Which of the following is MOST important to the effective management of an end user-developed application?

- ☐ Implementing best practice folder structures
- ☐ Continuous monitoring to facilitate prompt escalation of issues
- ☐ Assigning risk ratings based on probability and impact
- ☐ Stress testing the application through use of data outliers

Licensed to Berend Post berend.post@it-university.nl

Question 649

An existing system is being replaced with a new application package. User acceptance testing (UAT) should ensure that:

- ☐ data from the old system has been converted correctly
- ☐ the new system functions as expected
- ☐ the new system is better than the old system
- ☐ there is a business need for the new system

Question 650

Effective transactional controls are often capable of offering which of the following benefits (Choose four.):

- ☐ reduced administrative and material costs
- ☐ shortened contract cycle times
- ☐ enhanced procurement decisions
- ☐ diminished legal risk
- ☐ None of the choices.

Question 651

A clerk changed the interest rate for a loan on a master file. The rate entered is outside the normal range for such a loan. Which of the following controls is MOST effective in providing reasonable assurance that the change was authorized?

- ☐ The system will not process the change until the clerk's manager confirms the change by entering an approval code.
- ☐ The system generates a weekly report listing all rate exceptions and the report is reviewed by the clerk's manager.
- ☐ The system requires the clerk to enter an approval code.
- ☐ The system displays a warning message to the clerk.

Question 652

In wireless communication, which of the following controls allows the device receiving the communications to verify that the received communications have not been altered in transit?

- ☐ Device authentication and data origin authentication
- ☐ Wireless intrusion detection (IDS) and prevention systems (IPS)
- ☐ The use of cryptographic hashes
- ☐ Packet headers and trailers

Licensed to Berend Post berend.post@it-university.nl

Question 653

Which of the following should be an IS auditor's PRIMARY consideration when evaluating the development and design of a privacy program?

- ☐ Data governance and data classification procedures
- ☐ Policies and procedures consistent with privacy guidelines
- ☐ Industry practice and regulatory compliance guidance
- ☐ Information security and incident management practices

Question 654

Which of the following is the BEST way to protect the confidentiality of data on a corporate smartphone?

- ☐ Disabling public wireless connections
- ☐ Using remote data wipe capabilities
- ☐ Using encryption
- ☐ Changing the default PIN for Bluetooth connections

Question 655

IS management recently replaced its existing wired local area network (LAN) with a wireless infrastructure to accommodate the increased use of mobile devices within the organization. This will increase the risk of which of the following attacks?

- ☐ Port scanning
- ☐ Back door
- ☐ Man-in-the-middle
- ☐ War driving

Question 656

Which of the following would be the MOST effective method to address software license violations on employee workstations?

- ☐ Restricting administrative rights on employee workstations
- ☐ Requiring automated installation of software
- ☐ Scanning of workstations daily for unauthorized software use
- ☐ Implementing real-time monitoring software on employee workstations

Licensed to Berend Post berend.post@it-university.nl

Question 657

Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

- ☐ Specific developments only
- ☐ Business requirements only
- ☐ All phases of the installation must be documented
- ☐ No need to develop a customer specific documentation

Question 658

Which of the following should an IS auditor verify when auditing the effectiveness of virus protection?

- ☐ Frequency of IDS log reviews
- ☐ Currency of software patch application
- ☐ Schedule for migration to production
- ☐ Frequency of external Internet access

Question 659

Which of the following correctly describes the purpose of an Electronic data processing audit?

- ☐ to collect and evaluate evidence of an organization's information systems, practices, and operations.
- ☐ to ensure document validity.
- ☐ to verify data accuracy.
- ☐ to collect and evaluate benefits brought by an organization's information systems to its bottom line.
- ☐ None of the choices.

Question 660

When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. The IS auditor should recommend that the:

- ☐ project be discontinued.
- ☐ business case be updated and possible corrective actions be identified.
- ☐ project be returned to the project sponsor for reapproval.
- ☐ project be completed and the business case be updated later.

Licensed to Berend Post berend.post@it-university.nl

Question 661

Which of the following is the GREATEST concern when an organization's disaster recovery strategy utilizes a cold site?

- ☐ The lack of electrical power connections
- ☐ The lack of networking infrastructure
- ☐ The lack of appropriate environmental controls
- ☐ The lack of hardware components availability

Question 662

Before concluding that internal controls can be relied upon, the IS auditor should:

- ☐ discuss the internal control weaknesses with the auditee
- ☐ document application controls
- ☐ conduct tests of compliance
- ☐ document the system of internal control

Question 663

Which of the following characteristics pertaining to databases is not true?

- ☐ A data model should exist and all entities should have a significant name.
- ☐ Justifications must exist for normalized data.
- ☐ No NULLs should be allowed for primary keys.
- ☐ All relations must have a specific cardinality.

Question 664

What type of approach to the development of organizational policies is often driven by risk assessment?

- ☐ Bottom-up
- ☐ Top-down
- ☐ Comprehensive
- ☐ Integrated

Licensed to Berend Post berend.post@it-university.nl

Question 665

A review of Internet security disclosed that users have individual user accounts with the Internet service providers (ISPs) and use these accounts for downloading business data. The organization wants to ensure that only corporate network is used. The organization should FIRST:

- ☐ use a proxy server to filter out Internet sites that should not be accessed.
- ☐ keep a manual log of Internal access.
- ☐ monitor remote access activities.
- ☐ include a statement in its security policy about Internet use.

Question 666

Which of the following MUST be included in emergency change control procedures?

- ☐ Obtaining user management approval before implementing the changes
- ☐ Updating production source libraries to reflect the changes
- ☐ Using an emergency ID to move production programs into development
- ☐ Requesting that the help desk makes the changes

Question 667

Which of the following is the PRIMARY role of an IS auditor with regard to data privacy?

- ☐ Ensuring compliance with data privacy laws
- ☐ Communicating data privacy requirements to the organization
- ☐ Drafting the organization's data privacy policy
- ☐ Verifying that privacy practices match privacy statements

Question 668

For several years, a vendor has been providing offsite backup media and record storage for a bank. Due to familiarity with bank employees, the vendor does not consistently require authorization forms from them to retrieve media. Which of the following is the GREATEST risk from this situation?

- ☐ Bank employees can inappropriately obtain sensitive records
- ☐ Backup tapes may not be available
- ☐ Chain of custody could not be validated
- ☐ The vendor provides the incorrect media to employees

Licensed to Berend Post berend.post@it-university.nl

Question 669

While reviewing a hot site, the IS auditor discovers that one type of hardware platform is not installed. The IS auditor should FIRST:

- ☐ recommend the purchase and installation of hardware at the hot site.
- ☐ report the finding immediately to senior IS management.
- ☐ determine the business impact of the absence of the hardware.
- ☐ establish the lead time for delivery of a new machine.

Question 670

The PRIMARY purpose of reviewing the IT strategic plan is to identify risks that may:

- ☐ limit the ability to deliver customer requirements.
- ☐ limit the organization's ability to achieve its objectives.
- ☐ impact operational efficiency of the IT department.
- ☐ impact financial resourcing to implement the plan.

Question 671

Talking about application system audit, focus should always be placed on (Choose five.)

- ☐ performance and controls of the system
- ☐ the ability to limit unauthorized access and manipulation
- ☐ input of data are processed correctly
- ☐ output of data are processed correctly
- ☐ changes to the system are properly authorized
- ☐ None of the choices.

Question 672

Organization A has a Software as a Service Agreement (SaaS) with Organization B. The software is vital to Organization A. Which of the following would provide the GREATEST assurance that the application can be recovered in the event of a disaster?

- ☐ Organization B is responsible for disaster recovery and held accountable for interruption of service.
- ☐ Organization A has a source code escrow agreement and hardware procurement provisions for disaster recovery purposes.
- ☐ Organization B has a disaster recovery plan included in its contract and allows oversight by Organization A.
- ☐ Organization A buys disaster insurance to recuperate losses in the event of a disaster.

Licensed to Berend Post berend.post@it-university.nl

Question 673

Which of the following attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call?

- ☐ Eavesdropping
- ☐ Traffic analysis
- ☐ Masquerading
- ☐ Interrupt attack

Question 674

Which of the following is the MAIN purpose of data classification?

- ☐ Applying the appropriate protective measures
- ☐ Ensuring the segregation of duties
- ☐ Defining requirements of security labels
- ☐ Ensuring integrity of sensitive information

Question 675

During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:

- ☐ ask the auditee to sign a release form accepting full legal responsibility.
- ☐ elaborate on the significance of the finding and the risks of not correcting it.
- ☐ report the disagreement to the audit committee for resolution.
- ☐ accept the auditee's position since they are the process owners.

Question 676

During the audit of an acquired software package, an IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). The IS auditor should FIRST:

- ☐ test the software for compatibility with existing hardware.
- ☐ perform a gap analysis.
- ☐ review the licensing policy.
- ☐ ensure that the procedure had been approved.

Licensed to Berend Post berend.post@it-university.nl

Question 677

Which of the following would be the MOST significant audit finding when reviewing a point-of-sale (POS) system?

- ☐ invoices recorded on the POS system are manually entered into an accounting application
- ☐ An optical scanner is not used to read bar codes for the generation of sales invoices
- ☐ Frequent power outages occur, resulting in the manual preparation of invoices
- ☐ Customer credit card information is stored unencrypted on the local POS system

Question 678

The MOST appropriate person to chair the steering committee for an enterprise-wide system development should normally be the:

- ☐ project manager
- ☐ IS director
- ☐ executive level manager.
- ☐ business analyst

Question 679

An IS auditor finds multiple situations where the help desk resolved security incidents without notifying IT security as required by policy. Which of the following is the BEST audit recommendation?

- ☐ Display the incident response hotline in common areas.
- ☐ Have IT security review problem management policy.
- ☐ Reinforce the incident escalation process.
- ☐ Redesign the help desk reporting process.

Question 680

An IS auditor reviewing access controls for a client-server environment should FIRST:

- ☐ evaluate the encryption technique.
- ☐ identify the network access points.
- ☐ review the identity management system.
- ☐ review the application level access controls.

Licensed to Berend Post berend.post@it-university.nl

Question 681

Which of the following statement correctly describes the differences between tunnel mode and transport mode of the IPSec protocol?

- ☐ In transport mode the ESP is encrypted where as in tunnel mode the ESP and its header's are encrypted
- ☐ In tunnel mode the ESP is encrypted where as in transport mode the ESP and its header's are encrypted
- ☐ In both modes (tunnel and transport mode) the ESP and its header's are encrypted
- ☐ There is no encryption provided when using ESP or AH

Question 682

The PRIMARY benefit of using secure shell (SSH) to access a server on a network is that it:

- ☐ provides better session reliability.
- ☐ prevents man-in-the-middle attacks.
- ☐ provides confidentiality of transmitted data.
- ☐ facilitates communication across platforms.

Question 683

Which of the following is a function of an IS steering committee?

- ☐ Monitoring vendor-controlled change control and testing
- ☐ Ensuring a separation of duties within the information's processing environment
- ☐ Approving and monitoring major projects, the status of IS plans and budgets
- ☐ Liaising between the IS department and the end users

Question 684

What is the most common reason for information systems to fail to meet the needs of users?

- ☐ Lack of funding
- ☐ Inadequate user participation during system requirements definition
- ☐ Inadequate senior management participation during system requirements definition
- ☐ Poor IT strategic planning

Licensed to Berend Post berend.post@it-university.nl

Question 685

An organization is choosing key performance indicators (KPIs) for its information security management. Which of the following KPIs would provide stakeholders with the MOST useful information about whether information security risk is being managed?

- ☐ Time from initial reporting of an incident to appropriate escalation
- ☐ Time from identifying a security threat to implementing a solution
- ☐ The number of security controls implemented
- ☐ The number of security incidents during the past quarter

Question 686

Which of the following provides the GREATEST assurance that any confidential information on a disk is no longer accessible but the device is still usable by other internal users?

- ☐ Reformatting the disk
- ☐ Erasing the disk
- ☐ Degaussing the disk
- ☐ Password-protecting the disk

Question 687

Which of the following types of firewall treats each network frame or packet in isolation?

- ☐ statefull firewall
- ☐ hardware firewall
- ☐ combination firewall
- ☐ packet filtering firewall
- ☐ stateless firewall
- ☐ None of the choices.

Question 688

An IS auditor performing a telecommunication access control review should be concerned PRIMARILY with the:

- ☐ maintenance of access logs of usage of various system resources.
- ☐ authorization and authentication of the user prior to granting access to system resources.
- ☐ adequate protection of stored data on servers by encryption or other means.
- ☐ accountability system and the ability to identify any terminal accessing system resources.

Licensed to Berend Post berend.post@it-university.nl

Question 689

An internal control audit has revealed a control deficiency related to a legacy system where the compensating controls no longer appear to be effective. Which of the following would BEST help the information security manager determine the security requirements to resolve the control deficiency?

- ☐ Cost-benefit analysis
- ☐ Gap analysis
- ☐ Risk assessment
- ☐ Business case

Question 690

Which of the following is an appropriate test method to apply to a business continuity plan (BCP)?

- ☐ Pilot
- ☐ Paper
- ☐ Unit
- ☐ System

Question 691

Which of the following manages the digital certificate life cycle to ensure adequate security and controls exist in digital signature applications related to e-commerce?

- ☐ Registration authority
- ☐ Certificate authority (CA)
- ☐ Certification relocation list
- ☐ Certification practice statement

Question 692

A government organization uses standard Wi-Fi Protected Access 2 (WPA2) to protect confidential information transmitted to a file server. Which of the following is the IS auditor's BEST recommendation to further strengthen security?

- ☐ Certificate-based authentication
- ☐ Network address translation (NAT)
- ☐ Media access control (MAC) address filtering
- ☐ Service set identifier (SSID) masking

Licensed to Berend Post berend.post@it-university.nl

Question 693

The GREATEST advantage of using web services for the exchange of information between two systems is:

- ☐ secure communications.
- ☐ improved performance.
- ☐ efficient interfacing.
- ☐ enhanced documentation.

Question 694

Which of the following would be the BEST performance indicator for the effectiveness of an incident management program?

- ☐ Incident alert meantime
- ☐ Average time between incidents
- ☐ Number of incidents reported
- ☐ Incident resolution meantime

Question 695

Which of the following is the INCORRECT “layer - protocol" mapping within the TCP/IP model?

- ☐ Application layer – NFS
- ☐ Transport layer – TCP
- ☐ Network layer – UDP
- ☐ LAN or WAN interface layer – point-to-point protocol

Question 696

Which of the following would impair the independence of a quality assurance team?

- ☐ Ensuring compliance with development methods
- ☐ Checking the testing assumptions
- ☐ Correcting coding errors during the testing process
- ☐ Checking the code to ensure proper documentation

Question 697

Which of the following is MOST important when evaluating the retention period for a cloud provider’s client data backups?

- ☐ Cost of data storage
- ☐ Contractual commitments
- ☐ Previous audit recommendations
- ☐ Industry best practice

Licensed to Berend Post berend.post@it-university.nl

Question 698

Which of the following provides the MOST assurance that a newly developed web application does not have IT security issues?

- ☐ Server hardening
- ☐ Business impact analysis (BIA)
- ☐ Application whitelisting
- ☐ Penetration testing

Question 699

Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities BEST supports the concept of integrity?

- ☐ Ensuring encryption for data in transit
- ☐ Implementing a data classification schema
- ☐ Utilizing a formal change management process
- ☐ Enforcing service level agreements (SLAs)

Question 700

One advantage of managing an entire collection of projects as a portfolio is that it highlights the need to:

- ☐ identify dependencies between projects.
- ☐ inform users about all ongoing projects.
- ☐ manage the risk of each individual project.
- ☐ manage the quality of each project.

Question 701

Which of the following cloud deployment model is provisioned for open use by the general public?

- ☐ Private Cloud
- ☐ Community Cloud
- ☐ Public Cloud
- ☐ Hybrid Cloud

Question 702

Which of the following is the BEST time for an IS auditor to perform a post-implementation review?

- ☐ When the system has stabilized.
- ☐ After the completion of user testing.
- ☐ Before decommissioning the legacy system.
- ☐ Immediately after the new system goes into production.

Licensed to Berend Post berend.post@it-university.nl

Question 703

Which of the following is a tool you can use to simulate a big network structure on a single computer?

- ☐ honeymoon
- ☐ honeytrap
- ☐ honeytube
- ☐ honeyd
- ☐ None of the choices.

Question 704

An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:

- ☐ alignment of the BCP with industry best practices.
- ☐ results of business continuity tests performed by IS and end-user personnel.
- ☐ off-site facility, its contents, security and environmental controls.
- ☐ annual financial cost of the BCP activities versus the expected benefit of implementation of the plan.

Question 705

The lack of which of the following represents the GREATEST risk to the quality of developed software?

- ☐ Code reviews
- ☐ Periodic internal audits
- ☐ Load testing
- ☐ An enterprise architecture

Question 706

When an organization and its IT-hosting service provider are establishing a contract with each other, it is MOST important that the contract includes:

- ☐ each party’s security responsibilities
- ☐ details of expected security metrics
- ☐ penalties for noncompliance with security policy
- ☐ recovery time objectives (RTOs)

Licensed to Berend Post berend.post@it-university.nl

Question 707

Which of the following network configuration options contains a direct link between any two host machines?

- ☐ Bus
- ☐ Ring
- ☐ Star
- ☐ Completely connected (mesh)

Question 708

Which of the following features can be provided only by asymmetric encryption?

- ☐ 128-bit key length
- ☐ Information privacy
- ☐ Data confidentiality
- ☐ Nonrepudiation

Question 709

A technical lead who was working on a major project has left the organization. The project manager reports suspicious system activities on one of the servers that is accessible to the whole team. What would be of GREATEST concern if discovered during a forensic investigation?

- ☐ Audit logs are not enabled for the system
- ☐ A logon ID for the technical lead still exists
- ☐ Spyware is installed on the system
- ☐ A Trojan is installed on the system

Question 710

Depending on the complexity of an organization's business continuity plan (BCP), the plan may be developed as a set of more than one plan to address various aspects of business continuity and disaster recovery, in such an environment, it is essential that:

- ☐ each plan is consistent with one another.
- ☐ all plans are integrated into a single plan.
- ☐ each plan is dependent on one another.
- ☐ the sequence for implementation of all plans is defined.

Licensed to Berend Post berend.post@it-university.nl

Question 711

To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to:

- ☐ rely on senior management to enforce security
- ☐ promote the relevance and contribution of security
- ☐ reiterate the necessity of security
- ☐ focus on compliance

Question 712

What kind of protocols does the OSI Transport Layer of the TCP/IP protocol suite provide to ensure reliable communication?

- ☐ Nonconnection-oriented protocols
- ☐ Connection-oriented protocols
- ☐ Session-oriented protocols
- ☐ Nonsession-oriented protocols

Question 713

After threats to a data center are identified, an IS auditor would expect management to FIRST:

- ☐ recommend required actions to executive management.
- ☐ discuss risk management practices with neighboring firms.
- ☐ implement procedures to address all identified threats.
- ☐ establish and quantify the potential effects if each threat occurs.

Question 714

The PRIMARY focus of a training curriculum for members of an incident response team should be:

- ☐ technology training.
- ☐ security awareness.
- ☐ external corporate communication.
- ☐ specific role training.

Question 715

Which of the following audit risk is related to exposure of a process or entity to be audited without taking into account the control that management has implemented?

- ☐ Inherent Risk
- ☐ Control Risk
- ☐ Detection Risk
- ☐ Overall Audit Risk

Licensed to Berend Post berend.post@it-university.nl

Question 716

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses which stream cipher for confidentiality?

- ☐ CRC-32
- ☐ CRC-64
- ☐ DES
- ☐ 3DES
- ☐ RC4
- ☐ RC5
- ☐ None of the choices.

Question 717

An IS auditor is assigned to perform a post implementation review of an application system. Which pf the following situations may have impaired the independence of the IS auditor? The IS auditor:

- ☐ implemented a specific control during the development of the application system.
- ☐ designed an embedded audit module exclusively for auditing the application system.
- ☐ participated as a member of the application system project team, but did not have operational responsibilities.
- ☐ provided consulting advice concerning application system best practices.

Question 718

An IT management group has developed a standardized security control checklist and distributed it to the control self-assessors in each organizational unit. Which of the following is the GREATEST risk in this approach?

- ☐ Delayed feedback may increase exposures
- ☐ Over time the checklist may become outdated
- ☐ Assessors may manipulate the results
- ☐ Business-specific vulnerabilities may be overlooked

Question 719

An IS auditor identifies key controls that have been overridden by management. The NEXT step the IS auditor should take is to:

- ☐ perform procedures to quantify the irregularities.
- ☐ report the absence of key controls to regulators.
- ☐ recommend compensating controls.
- ☐ withdraw from the engagement.

Licensed to Berend Post berend.post@it-university.nl

Question 720

Which of the following statement is NOT true about smoke detector?

- ☐ The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised in the computer room floor
- ☐ The smoke detector should produce an audible alarm when activated and be linked to a monitored station
- ☐ The location of the smoke detector should be marked on the tiling for easy identification and access
- ☐ Smoke detector should replace fire suppression system

Question 721

When engaging services from external auditors, which of the following should be established FIRST?

- ☐ Termination conditions agreements
- ☐ Nondisclosure agreements
- ☐ Service level agreements
- ☐ Operational level agreements

Question 722

Which are the two primary types of scanner used for protecting against Malware?

- ☐ Malware mask/signatures and Heuristic Scanner
- ☐ Active and passive Scanner
- ☐ Behavioral Blockers and immunizer Scanner
- ☐ None of the above

Question 723

Disaster recovery planning (DRP) addresses the:

- ☐ technological aspect of business continuity planning.
- ☐ operational piece of business continuity planning.
- ☐ functional aspect of business continuity planning.
- ☐ overall coordination of business continuity planning.

Licensed to Berend Post berend.post@it-university.nl

Question 724

There is a concern that a salesperson may download an organization's full customer list from the Software as a Service (SaaS) when leaving to work for a competitor. Which of the following would BEST help to identify this type of incident?

- ☐ Monitor applications logs
- ☐ Disable remote access to the application
- ☐ Implement a web application firewall
- ☐ Implement an intrusion detection system (IDS)

Question 725

Which of the following activities should occur after a business impact analysis (BIA)?

- ☐ Identify threats to the IT environment
- ☐ Identify critical applications
- ☐ Analyze recovery options
- ☐ Review the computing and user environment

Question 726

What would be the MOST effective control for enforcing accountability among database users accessing sensitive information?

- ☐ implement a log management process
- ☐ implement a two-factor authentication
- ☐ Use table views to access sensitive data
- ☐ Separate database and application servers

Question 727

Which of the following kinds of function are particularly vulnerable to format string attacks?

- ☐ C functions that perform output formatting
- ☐ C functions that perform integer computation
- ☐ C functions that perform real number subtraction
- ☐ VB functions that perform integer conversion
- ☐ SQL functions that perform string conversion
- ☐ SQL functions that perform text conversion

Licensed to Berend Post berend.post@it-university.nl

Question 728

Which of the following BEST limits the impact of server failures in a distributed environment?

- ☐ Redundant pathways
- ☐ Clustering
- ☐ Dial backup lines
- ☐ Standby power

Question 729

What type of cryptosystem is characterized by data being encrypted by the sender using the recipient's public key, and the data then being decrypted using the recipient's private key?

- ☐ With public-key encryption, or symmetric encryption
- ☐ With public-key encryption, or asymmetric encryption
- ☐ With shared-key encryption, or symmetric encryption
- ☐ With shared-key encryption, or asymmetric encryption

Question 730

When is the BEST time to commence continuity planning for a new application system?

- ☐ Immediately after implementation
- ☐ Just prior to the handover to the system maintenance group
- ☐ During the design phase
- ☐ Following successful user testing

Question 731

Which of the following is the MOST important outcome of testing incident response plans?

- ☐ Internal procedures are improved.
- ☐ An action plan is available for senior management.
- ☐ Staff is educated about current threats.
- ☐ Areas requiring investment are identified.

Question 732

When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

- ☐ The point at which controls are exercised as data flow through the system
- ☐ Only preventive and detective controls are relevant
- ☐ Corrective controls can only be regarded as compensating
- ☐ Classification allows an IS auditor to determine which controls are missing

Licensed to Berend Post berend.post@it-university.nl

Question 733

Which of the following goals would you expect to find in an organization's strategic plan?

- ☐ Test a new accounting package.
- ☐ Perform an evaluation of information technology needs.
- ☐ Implement a new project planning system within the next 12 months.
- ☐ Become the supplier of choice for the product offered.

Question 734

An IS auditor discovered abnormalities in a monthly report generated from a system upgraded six months ago. Which of the following should be the auditor's FIRST course of action?

- ☐ Inspect source code for proof of abnormalities
- ☐ Perform a change management review of the system
- ☐ Schedule an access review of the system
- ☐ Determine the impact of abnormalities in the report

Question 735

When developing an escalation process for an incident response plan, the information security manager should PRIMARLY consider the:

- ☐ affected stakeholders
- ☐ availability of technical resources
- ☐ incident response team
- ☐ media coverage

Question 736

Which of the following is the MOSTlikely reason an organization would use Platform as a Service (PaaS)?

- ☐ To operate third-party hosted applications
- ☐ To install and manage operating systems
- ☐ To establish a network and security architecture
- ☐ To develop and integrate its applications

Question 737

Which of the following cloud deployment model can be shared by several organizations?

- ☐ Private Cloud\
- ☐ Community Cloud
- ☐ Public Cloud
- ☐ Hybrid Cloud

Licensed to Berend Post berend.post@it-university.nl

Question 738

The maturity level of an organization's problem management support function is optimized when the function:

- ☐ proactively provides solutions
- ☐ has formally documented the escalation process
- ☐ analyzes critical incidents to identify root cause
- ☐ resolves requests in a timely manner

Question 739

Which of the following is the BEST way to facilitate proper follow-up for audit findings?

- ☐ Schedule a follow-up audit for two weeks after the initial audit was completed.
- ☐ Conduct a surprise audit to determine whether remediation is in progress.
- ☐ Conduct a follow-up audit when findings escalate to incidents.
- ☐ Schedule a follow-up audit based on remediation due dates.

Question 740

Applying a retention date on a file will ensure that:

- ☐ data cannot be read until the date is set.
- ☐ data will not be deleted before that date.
- ☐ backup copies are not retained after that date.
- ☐ datasets having the same name are differentiated.

Question 741

Which of the following system and data conversion strategies provides the GREATEST redundancy?

- ☐ Direct cutover
- ☐ Pilot study
- ☐ Phased approach
- ☐ Parallel run

Question 742

Which of the following term related to network performance refers to the variation in the time of arrival of packets on the receiver of the information?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Jitter

Licensed to Berend Post berend.post@it-university.nl

Question 743

A new information security manager is charged with reviewing and revising the information security strategy. The information security manager's FIRST course of action should be to gain an understanding of the organization's:

- ☐ security architecture
- ☐ risk register
- ☐ internal control framework
- ☐ business strategy

Question 744

When preparing an audit report, the IS auditor should ensure that the results are supported by:

- ☐ statements from IS management.
- ☐ workpapers of other auditors.
- ☐ an organizational control self-assessment.
- ☐ sufficient and appropriate audit evidence.

Question 745

Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

- ☐ Power line conditioners
- ☐ Surge protective devices
- ☐ Alternative power supplies
- ☐ Interruptible power supplies

Question 746

Which of the following is of greatest concern when performing an IS audit?

- ☐ Users' ability to directly modify the database
- ☐ Users' ability to submit queries to the database
- ☐ Users' ability to indirectly modify the database
- ☐ Users' ability to directly view the database

Licensed to Berend Post berend.post@it-university.nl

Question 747

To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

- ☐ control self-assessments.
- ☐ a business impact analysis.
- ☐ an IT balanced scorecard.
- ☐ business process reengineering.

Question 748

Which of the following is the MOST robust method for disposing of magnetic media that contains confidential information?

- ☐ Degaussing
- ☐ Defragmenting
- ☐ Erasing
- ☐ Destroying

Question 749

A message is being sent with a hash. The risk of an attacker changing the message and generating an authentic hash value can be mitigated by:

- ☐ requiring the recipient to use a different hash algorithm.
- ☐ generating hash output that is the same size as the original message.
- ☐ using a secret key in conjunction with the hash algorithm.
- ☐ using the sender's public key to encrypt the message.

Question 750

Which of the following BEST supports the risk assessment process to determine criticality of an asset?

- ☐ Threat assessment
- ☐ Residual risk analysis
- ☐ Vulnerability assessment
- ☐ Business impact analysis (BIA)

Licensed to Berend Post berend.post@it-university.nl

Question 751

The sophistication and formality of IS audit programs may vary significantly depending on which of the following factors?

- ☐ the target's management hands-on involvement.
- ☐ the target's location.
- ☐ the target's size and complexity.
- ☐ the target's budget.
- ☐ the target's head count.
- ☐ None of the choices.

Question 752

An organization has a mix of access points that cannot be upgraded to stronger security and newer access points having advanced wireless security. An IS auditor recommends replacing the non-upgradeable access points. Which of the following would BEST justify the IS auditor's recommendation?

- ☐ The new access points with stronger security are affordable.
- ☐ The old access points are poorer in terms of performance.
- ☐ The organization's security would be as strong as its weakest points.
- ☐ The new access points are easier to manage.

Question 753

Which of the following refers to an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer?

- ☐ buffer overflow
- ☐ format string vulnerabilities
- ☐ integer misappropriation
- ☐ code injection
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 754

What is a callback system?

- ☐ It is a remote-access system whereby the remote-access server immediately calls the user back at a predetermined number if the dial-in connection fails.
- ☐ It is a remote-access system whereby the user's application automatically redials the remote access server if the initial connection attempt fails.
- ☐ It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration database.
- ☐ It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently allows the user to call back at an approved number for a limited period of time.

Question 755

Rather than decommission an entire legacy application, an organization's IT department has chosen to replace specific modules while maintaining those still relevant. Which of the following artifacts is MOST important for an IS auditor to review?

- ☐ IT service management catalog and service level requirements
- ☐ Security requirements for legacy data masking and data destruction
- ☐ Applicable licensing agreements for the application
- ☐ Future state architecture and requirements

Question 756

Integer overflow occurs primarily with:

- ☐ string formatting
- ☐ debug operations
- ☐ output formatting
- ☐ input verifications
- ☐ arithmetic operations
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 757

Which of the following function in traditional EDI process manipulates and routes data between the application system and the communication handler?

- ☐ Communication handler
- ☐ EDI Interface
- ☐ Application System
- ☐ EDI Translator

Question 758

Which of the following attack involves sending forged ICMP Echo Request packets to the broadcast address on multiple gateways in order to illicit responses from the computers behind the gateway where they all respond back with ICMP Echo Reply packets to the source IP address of the ICMP Echo Request packets?

- ☐ Reflected attack
- ☐ Brute force attack
- ☐ Buffer overflow
- ☐ Pulsing Zombie

Question 759

An information security manager has identified and implemented migrating controls according to industry best practices. Which of the following is the GREATEST risk associated with this approach?

- ☐ Important security controls may be missed without senior management input.
- ☐ The cost of control implementation may be too high.
- ☐ The migration measures may not be updated in a timely manner.
- ☐ The security program may not be aligned with organizational objectives.

Question 760

Privileged account access is required to start an ad hoc batch job. Which of the following would MOST effectively detect unauthorized job execution?

- ☐ Requiring manual approval by an authorized user
- ☐ Executing the job through two-factor authentication
- ☐ Introducing job execution request procedures
- ☐ Reconciling user activity logs against authorizations

Licensed to Berend Post berend.post@it-university.nl

Question 761

Why does an IS auditor review an organization chart?

- ☐ To optimize the responsibilities and authority of individuals
- ☐ To control the responsibilities and authority of individuals
- ☐ To better understand the responsibilities and authority of individuals
- ☐ To identify project sponsors

Question 762

During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be MOST concerned with the:

- ☐ allocation of resources during an emergency.
- ☐ maintenance of hardware and software compatibility.
- ☐ differences in IS policies and procedures.
- ☐ frequency of system testing.

Question 763

An IS auditor invited to a development project meeting notes that no project risks have been documented. When the IS auditor raises this issue, the project manager responds that it is too early to identify risks and that, if risks do start impacting the project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

- ☐ stress the importance of spending time at this point in the project to consider and document risks, and to develop contingency plans.
- ☐ accept the project manager's position as the project manager is accountable for the outcome of the project.
- ☐ offer to work with the risk manager when one is appointed.
- ☐ inform the project manager that the IS auditor will conduct a review of the risks at the completion of the requirements definition phase of the project.

Question 764

After completing the business impact analysis (BIA), what is the next step in the business continuity planning process?

- ☐ Test and maintain the plan.
- ☐ Develop a specific plan.
- ☐ Develop recovery strategies.
- ☐ implement the plan.

Licensed to Berend Post berend.post@it-university.nl

Question 765

Which of the following is the BEST indication of an effective incident management process?

- ☐ Percentage of incidents where root cause has been identified
- ☐ Percentage of incidents closed without escalation
- ☐ Number of calls to the help desk
- ☐ Number of incidents reviewed by the IT management

Question 766

The responsibility for authorizing access to application data should be with the:

- ☐ data custodian.
- ☐ database administrator (DBA).
- ☐ data owner.
- ☐ security administrator.

Question 767

A medium-sized organization, whose IT disaster recovery measures have been in place and regularly tested for years, has just developed a formal business continuity plan (BCP). A basic BCP tabletop exercise has been performed successfully. Which testing should an IS auditor recommend be performed NEXT to verify the adequacy of the new BCP?

- ☐ Full-scale test with relocation of all departments, including IT, to the contingency site
- ☐ Walk-through test of a series of predefined scenarios with all critical personnel involved
- ☐ IT disaster recovery test with business departments involved in testing the critical applications
- ☐ Functional test of a scenario with limited IT involvement

Question 768

The majority of software vulnerabilities result from a few known kinds of coding defects, such as (Choose five.):

- ☐ buffer overflows
- ☐ format string vulnerabilities
- ☐ integer overflow
- ☐ code injection
- ☐ command injection
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 769

If the recovery time objective (RTO) increases:

- ☐ the disaster tolerance increases.
- ☐ the cost of recovery increases.
- ☐ a cold site cannot be used.
- ☐ the data backup frequency increases.

Question 770

Which of the following is a feature of an intrusion detection system (IDS)?

- ☐ Gathering evidence on attack attempts
- ☐ Identifying weaknesses in the policy definition
- ☐ Blocking access to particular sites on the Internet
- ☐ Preventing certain users from accessing specific servers

Question 771

During business process reengineering (BPR) of a bank's teller activities, an IS auditor should evaluate:

- ☐ the impact of changed business processes.
- ☐ the cost of new controls.
- ☐ BPR project plans.
- ☐ continuous improvement and monitoring plans.

Question 772

While reviewing the IT infrastructure, an IS auditor notices that storage resources are continuously being added. The IS auditor should:

- ☐ recommend the use of disk mirroring.
- ☐ review the adequacy of offsite storage.
- ☐ review the capacity management process.
- ☐ recommend the use of a compression algorithm.

Licensed to Berend Post berend.post@it-university.nl

Question 773

A security company and service provider have merged, and the CEO has requested one comprehensive set of security policies be developed for the newly formed company. The IS auditor's BEST recommendation would be to:

- ☐ conduct a policy gap assessment.
- ☐ adopt an industry standard security policy.
- ☐ implement the service provider's policies.
- ☐ implement the security company's policies.

Question 774

What is the BEST method to determine if IT resource spending is aligned with planned project spending?

- ☐ Earned value analysis (EVA)
- ☐ Gantt chart
- ☐ Return on investment (ROI) analysis
- ☐ Critical path analysis

Question 775

Which of the following is MOST likely to be included in a post-implementation review?

- ☐ Results of live processing
- ☐ Current sets of test data
- ☐ Test results
- ☐ Development methodology

Question 776

What type of BCP test uses actual resources to simulate a system crash and validate the plan's effectiveness?

- ☐ Paper
- ☐ Preparedness
- ☐ Walk-through
- ☐ Parallel

Licensed to Berend Post berend.post@it-university.nl

Question 777

Which of the following is the BEST way to increase the effectiveness of security incident detection?

- ☐ Educating end users on identifying suspicious activity
- ☐ Establishing service level agreements (SLAs) with appropriate forensic service providers
- ☐ Determining containment activities based on the type of incident
- ☐ Documenting root cause analysis procedures

Question 778

Which of the following should be considered FIRST when implementing a risk management program?

- ☐ An understanding of the organization's threat, vulnerability and risk profile
- ☐ An understanding of the risk exposures and the potential consequences of compromise
- ☐ A determination of risk management priorities based on potential consequences
- ☐ A risk mitigation strategy sufficient to keep risk consequences at an acceptable level

Question 779

A senior auditor is reviewing work papers prepared by a junior auditor indicating that a finding was removed after the auditee said they corrected the problem. Which of the following would be the MOST appropriate course of action for the senior auditor?

- ☐ Approve the work papers as written
- ☐ Refer the issue to the audit director
- ☐ Have the finding reinstated
- ☐ Ask the auditee to retest

Question 780

Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance program?

- ☐ A system downtime log
- ☐ Vendors' reliability figures
- ☐ Regularly scheduled maintenance log
- ☐ A written preventive maintenance schedule

Licensed to Berend Post berend.post@it-university.nl

Question 781

An IS auditor is reviewing the results of a business process improvement project. Which of the following should be performed FIRST?

- ☐ Evaluate control gaps between the old and the new processes.
- ☐ Develop compensating controls.
- ☐ Document the impact of control weaknesses in the process.
- ☐ Ensure that lessons learned during the change process are documented.

Question 782

A retail outlet has introduced radio frequency identification (RFID) tags to create unique serial numbers for all products. Which of the following is the PRIMARY concern associated with this initiative?

- ☐ Issues of privacy
- ☐ Wavelength can be absorbed by the human body
- ☐ RFID tags may not be removable
- ☐ RFID eliminates line-of-sight reading

Question 783

When responding to an ongoing denial of service (DoS) attack, an organization's FIRST course of action should be to:

- ☐ restore service
- ☐ minimize impact
- ☐ analyze the attack path
- ☐ investigate damage

Question 784

For a discretionary access control to be effective, it must:

- ☐ operate within the context of mandatory access controls.
- ☐ operate independently of mandatory access controls.
- ☐ enable users to override mandatory access controls when necessary.
- ☐ be specifically permitted by the security policy.

Licensed to Berend Post berend.post@it-university.nl

Question 785

Which of the following would BEST assist senior management in evaluating IT performance as well as the alignment between corporate and IT strategic objectives?

- ☐ Enterprise architecture
- ☐ IT project value analysis
- ☐ Balanced scorecard
- ☐ Control self-assessment

Question 786

During an audit of a mission-critical system hosted in an outsourced data center, an IS auditor discovers that contracted routine maintenance for the alternate power generator was not performed. Which of the following should be the auditor's MAIN concern?

- ☐ Fraudulent behavior by the outsourcer charging for work not performed
- ☐ Failure of the alternate power generator during a power outage
- ☐ High repair costs if faulty generator parts are not detected in a timely manner
- ☐ Loss of warranty due to lack of system maintenance

Question 787

An IS auditor evaluating the resilience of a high-availability network should be MOST concerned if:

- ☐ the setup is geographically dispersed.
- ☐ the network servers are clustered in a site.
- ☐ a hot site is ready for activation.
- ☐ diverse routing is implemented for the network.

Question 788

The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

- ☐ comply with regulatory requirements.
- ☐ provide a basis for drawing reasonable conclusions.
- ☐ ensure complete audit coverage.
- ☐ perform the audit according to the defined scope.

Licensed to Berend Post berend.post@it-university.nl

Question 789

Which of the following types of firewalls provide the GREATEST degree and granularity of control?

- ☐ Screaming router
- ☐ Packet filter
- ☐ Application gateway
- ☐ Circuit gateway

Question 790

An IS auditor conducting an access control review in a client-server environment discovers that all printing options are accessible by all users. In this situation, the IS auditor is MOST likely to conclude that:

- ☐ exposure is greater, since information is available to unauthorized users.
- ☐ operating efficiency is enhanced, since anyone can print any report at any time.
- ☐ operating procedures are more effective, since information is easily available.
- ☐ user friendliness and flexibility is facilitated, since there is a smooth flow of information among users.

Question 791

Which of the following is the PRIMARY objective of a business impact analysis (BIA)?

- ☐ Define the recovery point objective (RPO).
- ☐ Analyze vulnerabilities.
- ☐ Confirm control effectiveness.
- ☐ Determine recovery priorities.

Question 792

As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up on tape. During the backup procedure, a drive malfunctions and the order entry files are lost. Which of the following is necessary to restore these files?

- ☐ The previous day's backup file and the current transaction tape
- ☐ The previous day's transaction file and the current transaction tape
- ☐ The current transaction tape and the current hard copy transaction log
- ☐ The current hard copy transaction log and the previous day's transaction file

Licensed to Berend Post berend.post@it-university.nl

Question 793

During an internal audit review of an HR recruitment system implementation, the IS auditor notes a number of defects were unresolved at the time the system went live. Which of the following is the auditor's MOST important task prior to formulating an audit opinion?

- ☐ Identify the root cause of the defects to confirm severity.
- ☐ Review the user acceptance test results.
- ☐ Verify risk acceptance by the project steering committee.
- ☐ Confirm the timeline for migration of the defects.

Question 794

Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

- ☐ Assimilation of the framework and intent of a written security policy by all appropriate parties
- ☐ Management support and approval for the implementation and maintenance of a security policy
- ☐ Enforcement of security rules by providing punitive actions for any violation of security rules
- ☐ Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Question 795

What process allows IS management to determine whether the activities of the organization differ from the planned or expected levels?

- ☐ Business impact assessment
- ☐ Risk assessment
- ☐ IS assessment methods
- ☐ Key performance indicators (KPIs)

Question 796

Which of the following is of greatest concern to the IS auditor?

- ☐ Failure to report a successful attack on the network
- ☐ Failure to prevent a successful attack on the network
- ☐ Failure to recover from a successful attack on the network
- ☐ Failure to detect a successful attack on the network

Licensed to Berend Post berend.post@it-university.nl

Question 797

What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

- ☐ Repeatable but Intuitive
- ☐ Defined
- ☐ Managed and Measurable
- ☐ Optimized

Question 798

Which of the following testing procedure is used by an auditor to check whether a firm is following the rules and regulations applicable to an activity or practice?

- ☐ Compliance testing
- ☐ Sanity testing
- ☐ Recovery testing
- ☐ Substantive testing

Question 799

An information security manager has observed multiple exceptions for a number of different security controls. Which of the following should be the information security manager's FIRST course of action?

- ☐ Design mitigating controls for the exceptions.
- ☐ Prioritize the risk and implement treatment options.
- ☐ Inform respective risk owners of the impact of exceptions.
- ☐ Report the noncompliance to the board of directors.

Question 800

IT governance is PRIMARILY the responsibility of the:

- ☐ chief executive officer.
- ☐ board of directors.
- ☐ IT steering committee.
- ☐ audit committee.

Licensed to Berend Post berend.post@it-university.nl

Question 801

While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:

- ☐ audit trail of the versioning of the work papers.
- ☐ approval of the audit phases.
- ☐ access rights to the work papers.
- ☐ confidentiality of the work papers.

Question 802

The MAIN benefit of using an integrated test facility (ITF) as an online auditing technique is that it enables:

- ☐ a cost-effective approach to application controls audit
- ☐ auditors to investigate fraudulent transactions
- ☐ auditors to test without impacting production data
- ☐ the integration of financial and audit tests

Question 803

To address an organization's disaster recovery requirements, backup intervals should not exceed the:

- ☐ service level objective (SLO).
- ☐ recovery time objective (RTO).
- ☐ recovery point objective (RPO).
- ☐ maximum acceptable outage (MAO).

Question 804

Which of the following is the MOST effective way to achieve the integration of information security governance into corporate governance?

- ☐ Ensure information security aligns with IT strategy.
- ☐ Provide periodic IT balanced scorecards to senior management.
- ☐ Align information security budget requests to organizational goals.
- ☐ Ensure information security efforts support business goals.

Licensed to Berend Post berend.post@it-university.nl

Question 805

Communicating which of the following would BEST encourage management to initiate appropriate actions following the receipt of report findings?

- ☐ Risk implications of the observations
- ☐ Strict deadlines to close all observations
- ☐ Statistical sampling used to derive observations
- ☐ Recommendations that align with the business strategy

Question 806

Effective IT governance requires organizational structures and processes to ensure that:

- ☐ the organization's strategies and objectives extend the IT strategy.
- ☐ the business strategy is derived from an IT strategy.
- ☐ IT governance is separate and distinct from the overall governance.
- ☐ the IT strategy extends the organization's strategies and objectives.

Question 807

Which of the following should be reviewed as part of a data integrity test?

- ☐ Completeness
- ☐ Confidentiality
- ☐ Data backup
- ☐ Redundancy

Question 808

A maturity model is useful in the assessment of IT service management because it:

- ☐ provides a benchmark for process improvement
- ☐ defines the level of control required to meet business needs
- ☐ indicates the service levels required for the business area
- ☐ specifies the mechanism needed to achieve defined service levels

Question 809

Which of the following should be of MOST influence to an information security manager when developing IT security policies?

- ☐ Past and current threats
- ☐ IT security framework
- ☐ Compliance with regulations
- ☐ Business strategy

Licensed to Berend Post berend.post@it-university.nl

Question 810

Which of the following layer of an enterprise data flow architecture represents subset of information from the core Data Warehouse selected and organized to meet the needs of a particular business unit or business line?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☐ Data Mart layer
- ☐ Data access layer

Question 811

Which of the following provides the MOST relevant information for proactively strengthening security settings?

- ☐ Bastion host
- ☐ Intrusion detection system
- ☐ Honeypot
- ☐ Intrusion prevention system

Question 812

During an ERP post-implementation review, it was noted that operating costs have been significantly higher than anticipated. Which of the following should the organization have done to detect this issue?

- ☐ Updated the project charter as major changes occurred
- ☐ Conducted periodic user satisfaction surveys
- ☐ Performed an analysis of system usage
- ☐ Monitored financial key performance indicators (KPIs)

Question 813

The MAIN purpose of documenting information security guidelines for use within a large, international organization is to:

- ☐ ensure that all business units have the same strategic security goals
- ☐ provide evidence for auditors that security practices are adequate
- ☐ explain the organization's preferred practices for security
- ☐ ensure that all business units implement identical security procedures

Licensed to Berend Post berend.post@it-university.nl

Question 814

Meeting which of the following security objectives BEST ensures that information is protected against unauthorized modification?

- ☐ Availability
- ☐ Authenticity
- ☐ Confidentiality
- ☐ Integrity

Question 815

Disaster recovery planning (DRP) for a company's computer system usually focuses on:

- ☐ operations turnover procedures.
- ☐ strategic long-range planning.
- ☐ the probability that a disaster will occur.
- ☐ alternative procedures to process transactions.

Question 816

In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

- ☐ there is an integration of IS and business staffs within projects.
- ☐ there is a clear definition of the IS mission and vision.
- ☐ a strategic information technology planning methodology is in place.
- ☐ the plan correlates business objectives to IS goals and objectives.

Question 817

When conducting a requirements analysis for a project the BEST approach would be to:

- ☐ conduct a control self-assessment.
- ☐ consult key stakeholders.
- ☐ test operational deliverables.
- ☐ prototype the requirements.

Question 818

A virus typically consists of what major parts (Choose three.):

- ☐ a mechanism that allows them to infect other files and reproduce" a trigger that activates delivery of a "payload""
- ☐ a payload
- ☐ a signature
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 819

Which of the following term in business continuity determines the maximum tolerable amount of time needed to bring all critical systems back online after disaster occurs?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 820

To develop a successful business continuity plan, end user involvement is critical during which of the following phases?

- ☐ Business recovery strategy
- ☐ Detailed plan development
- ☐ Business impact analysis (BIA)
- ☐ Testing and maintenance

Question 821

An auditor needs to be aware of technical controls which are used to protect computer from malware. Which of the following technical control interrupts DoS and ROM BIOS call and look for malware like action?

- ☐ Scanners
- ☐ Active Monitors
- ☐ Immunizer
- ☐ Behavior blocker

Question 822

An organization is within a jurisdiction where new regulations have recently been announced to restrict cross-border data transfer of personally identifiable information (PII). Which of the following IT decisions will MOST likely need to be assessed in the context of this change?

- ☐ Hosting the payroll system at an external cloud service provider
- ☐ Purchasing cyber insurance from an overseas insurance company
- ☐ Applying encryption to database hosting PII data
- ☐ Hiring IT consultants from overseas

Licensed to Berend Post berend.post@it-university.nl

Question 823

Which of the following is NOT a defined ISO basic task related to network management?

- ☐ Fault management
- ☐ Accounting resources
- ☐ Security management
- ☐ Communications management

Question 824

Which of the following is the protocol data unit (PDU) of application layer in TCP/IP model?

- ☐ Data
- ☐ Segment
- ☐ Packet
- ☐ Frame

Question 825

When performing an audit of a client relationship management (CRM) system migration project, which of the following should be of GREATEST concern to an IS auditor?

- ☐ The technical migration is planned for a Friday preceding a long weekend, and the time window is too short for completing all tasks.
- ☐ Employees pilot-testing the system are concerned that the data representation in the new system is completely different from the old system.
- ☐ A single implementation is planned, immediately decommissioning the legacy system.
- ☐ Five weeks prior to the target date, there are still numerous defects in the printing functionality of the new system's software.

Question 826

In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

- ☐ registration authority (RA).
- ☐ issuing certification authority (CA).
- ☐ subject CA.
- ☐ policy management authority.

Licensed to Berend Post berend.post@it-university.nl

Question 827

A stockbroker accepts orders over the Internet. Which of the following is the MOST appropriate control to ensure confidentiality of the orders?

- ☐ Virtual private network
- ☐ Public key encryption
- ☐ Data Encryption Standard (DES)
- ☐ Digital signature

Question 828

Which of the following is the MOST appropriate action to formalize IT governance in an organization?

- ☐ Evaluating the IT strategy
- ☐ Modifying IT goals and strategy
- ☐ Establishing an IT steering committee
- ☐ Implementing risk management

Question 829

Which of the following requirements in a document control standard would provide nonrepudiation to digitally signed legal documents?

- ☐ All digital signatures must include a hashing algorithm.
- ☐ All digitally signed documents must be stored in an encrypted database.
- ☐ All documents requiring digital signatures must be signed by both the customer and a witness.
- ☐ Only secure file transfer protocol (SFTP) may be used for digitally signed documentation.

Question 830

Integrating business continuity planning (BCP) into an IT project aids in:

- ☐ the retrofitting of the business continuity requirements.
- ☐ the development of a more comprehensive set of requirements.
- ☐ the development of a transaction flowchart.
- ☐ ensuring the application meets the user's needs.

Licensed to Berend Post berend.post@it-university.nl

Question 831

The application systems of an organization using open-source software have no single recognized developer producing patches. Which of the following would be the MOST secure way of updating open-source software?

- ☐ Rewrite the patches and apply them
- ☐ Code review and application of available patches
- ☐ Develop in-house patches
- ☐ identify and test suitable patches before applying them

Question 832

The PRIMARY objective of conducting a post-implementation review is to:

- ☐ determine if project management methodology was applied consistently
- ☐ verify that the information system meets the intended objectives
- ☐ determine if testing documentation was sufficient
- ☐ allow employees to provide feedback on the information system

Question 833

A sales representative is reviewing the organization's feedback blog and gets redirected to a site that sells illegal prescription drugs. The blog site is MOST likely susceptible to which of the following types of attacks?

- ☐ Directory harvesting
- ☐ SQL injection
- ☐ Cross-site scripting
- ☐ Phishing attack.

Question 834

Which of the following antispam filtering techniques would BEST prevent a valid, variable- length e-mail message containing a heavily weighted spam keyword from being labeled as spam?

- ☐ Heuristic (rule-based)
- ☐ Signature-based
- ☐ Pattern matching
- ☐ Bayesian (statistical)

Licensed to Berend Post berend.post@it-university.nl

Question 835

The use of statistical sampling procedures helps minimize:

- ☐ Detection risk
- ☐ Business risk
- ☐ Controls risk
- ☐ Compliance risk

Question 836

How does the process of systems auditing benefit from using a risk-based approach to audit planning?

- ☐ Controls testing starts earlier.
- ☐ Auditing resources are allocated to the areas of highest concern.
- ☐ Auditing risk is reduced.
- ☐ Controls testing is more thorough.

Question 837

William has been assigned a changeover task. He has to break the older system into deliverable modules. Initially, the first module of the older system is phased out using the first module of a new system. Then, the second module of the old system is phased out, using the second module of the newer system and so forth until reaching the last module. Which of the following changeover system William needs to implement?

- ☐ Parallel changeover
- ☐ Phased changeover
- ☐ Abrupt changeover
- ☐ Pilot changeover

Question 838

When conducting a penetration test of an organization's internal network, which of the following approaches would BEST enable the conductor of the test to remain undetected on the network?

- ☐ Use the IP address of an existing file server or domain controller.
- ☐ Pause the scanning every few minutes to allow thresholds to reset.
- ☐ Conduct the scans during evening hours when no one is logged-in.
- ☐ Use multiple scanning tools since each tool has different characteristics.

Licensed to Berend Post berend.post@it-university.nl

Question 839

Which of the following is MOST critical for the effective implementation of IT governance?

- ☐ Internal auditor commitment
- ☐ Supportive corporate culture
- ☐ Strong risk management practices
- ☐ Documented policies

Question 840

The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a(n):

- ☐ Implementor
- ☐ Facilitator
- ☐ Developer
- ☐ Sponsor

Question 841

Which of the following is the BEST defense against a brute force attack?

- ☐ Discretionary access control
- ☐ Intruder detection lockout
- ☐ Mandatory access control
- ☐ Time-of-day restrictions

Question 842

An IS auditor evaluating logical access controls should FIRST:

- ☐ document the controls applied to the potential access paths to the system.
- ☐ test controls over the access paths to determine if they are functional.
- ☐ evaluate the security environment in relation to written policies and practices
- ☐ obtain an understanding of the security risks to information processing.

Question 843

Which of the following is MOST critical to the successful implementation of information security within an organization?

- ☐ Strong risk management skills exist within the information security group.
- ☐ Budget is allocated for information security tools.
- ☐ The information security manager is responsible for setting information security policy.
- ☐ Security is effectively marketed to all managers and employees.

Licensed to Berend Post berend.post@it-university.nl

Question 844

Which of the following software development methods is based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams?

- ☐ Agile Development
- ☐ Software prototyping
- ☐ Rapid application development
- ☐ Component based development

Question 845

Off-site data storage should be kept synchronized when preparing for recovery of time- sensitive data such as that resulting from which of the following?

- ☐ Financial reporting
- ☐ Sales reporting
- ☐ Inventory reporting
- ☐ Transaction processing

Question 846

A bank is relocating its servers to a vendor that provides data center hosting services to multiple clients. Which of the following controls would restrict other clients from physical access to the bank's servers?

- ☐ Closed-circuit television cameras
- ☐ Locking server cages
- ☐ Biometric access at all data center entrances
- ☐ 24-hour security guards

Question 847

Which of the following service is a distributed database that translate host name to IP address to IP address to host name?

- ☐ DNS
- ☐ FTP
- ☐ SSH
- ☐ SMTP

Licensed to Berend Post berend.post@it-university.nl

Question 848

A digital signature contains a message digest to:

- ☐ show if the message has been altered after transmission.
- ☐ define the encryption algorithm.
- ☐ confirm the identity of the originator.
- ☐ enable message transmission in a digital format.

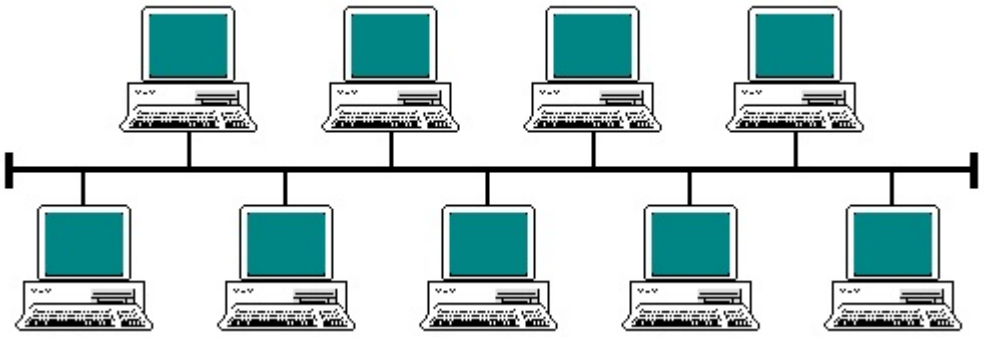
Question 849

An organization has outsourced its data leakage monitoring to an Internet service provider (ISP). Which of the following is the BEST way for an IS auditor to determine the effectiveness of this service?

- ☐ Verify the ISP has staff to deal with data leakage
- ☐ Review the ISP's external audit report
- ☐ Review the data leakage clause in the SLA
- ☐ Simulate a data leakage incident

Question 850

Identify the LAN topology from below diagram presented below:



bus topology

- ☐ Bus
- ☐ Star
- ☐ Ring
- ☐ Mesh

Licensed to Berend Post berend.post@it-university.nl

Question 851

An information security policy stating that 'the display of passwords must be masked or suppressed' addresses which of the following attack methods?

- ☐ Piggybacking
- ☐ Dumpster diving
- ☐ Shoulder surfing
- ☐ Impersonation

Question 852

Which of the following is MOST relevant for an information security manager to communicate to IT operations?

- ☐ The level of inherent risk
- ☐ Vulnerability assessments
- ☐ Threat assessments
- ☐ The level of exposure

Question 853

When reviewing a project where quality is a major concern, an IS auditor should use the project management triangle to explain that:

- ☐ increases in quality can be achieved, even if resource allocation is decreased.
- ☐ increases in quality are only achieved if resource allocation is increased.
- ☐ decreases in delivery time can be achieved, even if resource allocation is decreased.
- ☐ decreases in delivery time can only be achieved if quality is decreased.

Question 854

Which of the following is MOST important in determining a project's feasibility?

- ☐ The organization's main competitor has initiated a similar project.
- ☐ The IT steering committee endorses the project.
- ☐ A project management methodology is established.
- ☐ The project's value is established in an approved business case.

Question 855

In attribute sampling, what is the relationship between expected error rate and sample size?

- ☐ The expected error rate does not affect the sample size
- ☐ The greater the expected error rate, the smaller the sample size
- ☐ The greater the expected error rate, the grater the sample size
- ☐ The greater the sample size, the lower the expected error rate

Licensed to Berend Post berend.post@it-university.nl

Question 856

An intruder accesses an application server and makes changes to the system log. Which of the following would enable the identification of the changes?

- ☐ Mirroring the system log on another server
- ☐ Simultaneously duplicating the system log on a write-once disk
- ☐ Write-protecting the directory containing the system log
- ☐ Storing the backup of the system log offsite

Question 857

Which of the following cryptography demands less computational power and offers more security per bit?

- ☐ Quantum cryptography
- ☐ Elliptic Curve Cryptography (ECC)
- ☐ Symmetric Key Cryptography
- ☐ Asymmetric Key Cryptography

Question 858

Which of the following is MOST important for an IS auditor to consider during a review of the IT governance of an organization?

- ☐ Funding allocations
- ☐ Risk management methodology
- ☐ Defined service levels
- ☐ Decision making responsibilities

Question 859

Which of the following would be an auditor's GREATEST concern when reviewing data inputs from spreadsheets into the core finance system?

- ☐ Undocumented code formats data and transmits directly to the database.
- ☐ There is not a complete inventory of spreadsheets, and file naming is inconsistent.
- ☐ Spreadsheets are accessible by all members of the finance department.
- ☐ The department data protection policy has not been reviewed or updated for two years.

Licensed to Berend Post berend.post@it-university.nl

Question 860

Which of the following attacks targets the Secure Sockets Layer (SSL)?

- ☐ Man-in-the middle
- ☐ Dictionary
- ☐ Password sniffing
- ☐ Phishing

Question 861

Regarding a disaster recovery plan, the role of an IS auditor should include:

- ☐ identifying critical applications.
- ☐ determining the external service providers involved in a recovery test.
- ☐ observing the tests of the disaster recovery plan. determining the criteria for
- ☐ establishing a recovery time objective (RTO).

Question 862

An IS auditor has assessed a payroll service provider's security policy and finds significant topics are missing. Which of the following is the auditor's BEST course of action?

- ☐ Recommend the service provider update their policy.
- ☐ Notify the service provider of the discrepancies.
- ☐ Report the risk to internal management.
- ☐ Recommend replacement of the service provider.

Question 863

TEMPEST is a hardware for which of the following purposes?

- ☐ Eavedropping
- ☐ Social engineering
- ☐ Virus scanning
- ☐ Firewalling
- ☐ None of the choices.

Question 864

Which of the following should be of MOST concern to an IS auditor reviewing the public key infrastructure (PKI) for enterprise e-mail?

- ☐ The private key certificate has not been updated.
- ☐ The certificate revocation list has not been updated.
- ☐ The certificate practice statement has not been published.
- ☐ The PKI policy has not been updated within the last year.

Licensed to Berend Post berend.post@it-university.nl

Question 865

Which of the following is BEST suited for secure communications within a small group?

- ☐ Key distribution center
- ☐ Certification authority
- ☐ Web of trust
- ☐ Kerberos Authentication System

Question 866

A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:

- ☐ compute the amortization of the related assets.
- ☐ calculate a return on investment (ROI).
- ☐ apply a qualitative approach.
- ☐ spend the time needed to define exactly the loss amount.

Question 867

An IS auditor has been asked to assess the security of a recently migrated database system that contains personal and financial data for a bank's customers. Which of the following controls is MOST important for the auditor to confirm it in place?

- ☐ The default configurations have been changed.
- ☐ All tables in the database are normalized.
- ☐ The service port used by the database server has been changed.
- ☐ The default administration account is used after changing the account password.

Question 868

A payroll application system accepts individual user sign-on IDs and then connects to its database using a single application ID. The GREATEST weakness under this system architecture is that:

- ☐ an incident involving unauthorized access to data cannot be tied to a specific user.
- ☐ when multiple sessions with the same application ID collide, the database locks up.
- ☐ users can gain direct access to the application ID and circumvent data controls.
- ☐ the database becomes unavailable if the password of the application ID expires.

Licensed to Berend Post berend.post@it-university.nl

Question 869

Which of the following term in business continuity determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 870

An IS audit reveals that an organization is not proactively addressing known vulnerabilities. Which of the following should the IS auditor recommend the organization do FIRST?

- ☐ Verify the disaster recovery plan (DRP) has been tested.
- ☐ Ensure the intrusion prevention system (IPS) is effective.
- ☐ Confirm the incident response team understands the issue.
- ☐ Assess the security risks to the business.

Question 871

Which of the following is a substantive test?

- ☐ Checking a list of exception reports
- ☐ Ensuring approval for parameter changes
- ☐ Using a statistical sample to inventory the tape library
- ☐ Reviewing password history reports

Question 872

The BEST way to evaluate a shared control environment is to obtain an assurance report and review which of the following?

- ☐ Control self-assessment (CSA)
- ☐ Service level agreement (SLA)
- ☐ Master service agreement
- ☐ Complementary user entity controls

Question 873

Which of the following is the MOST important objective of data protection?

- ☐ identifying persons who need access to information
- ☐ Ensuring the integrity of information
- ☐ Denying or authorizing access to the IS system
- ☐ Monitoring logical accesses

Licensed to Berend Post berend.post@it-university.nl

Question 874

Which of the following is a benefit of using callback devices?

- ☐ Provide an audit trail
- ☐ Can be used in a switchboard environment
- ☐ Permit unlimited user mobility
- ☐ Allow call forwarding

Question 875

An IS auditor discovers that developers have operator access to the command line of a production environment operating system. Which of the following controls would BEST mitigate the risk of undetected and unauthorized program changes to the production environment?

- ☐ Commands typed on the command line are logged
- ☐ Hash keys are calculated periodically for programs and matched against hash keys calculated for the most recent authorized versions of the programs
- ☐ Access to the operating system command line is granted through an access restriction tool with preapproved rights
- ☐ Software development tools and compilers have been removed from the production environment

Question 876

The risk of communication failure in an e-commerce environment is BEST minimized through the use of:

- ☐ alternative or diverse routing
- ☐ compression software to minimize transmission duration
- ☐ a packet filtering firewall to reroute messages
- ☐ functional or message acknowledgments

Question 877

Which of the following will prevent dangling tuples in a database?

- ☐ Cyclic integrity
- ☐ Domain integrity
- ☐ Relational integrity
- ☐ Referential integrity

Licensed to Berend Post berend.post@it-university.nl

Question 878

Which of the following is MOST important to include in a business continuity plan (BCP)?

- ☐ Vendor contact information
- ☐ Documentation of critical systems
- ☐ Documentation of data center floor plans
- ☐ Backup site location information

Question 879

During which of the following phases in system development would user acceptance test plans normally be prepared?

- ☐ Feasibility study
- ☐ Requirements definition
- ☐ implementation planning
- ☐ Postimplementation review

Question 880

As an IS auditor it is very important to understand the importance of job scheduling. Which of the following statement is NOT true about job scheduler or job scheduling software?

- ☐ Job information is set up only once, which increase the probability of an error.
- ☐ Records are maintained of all job success and failures.
- ☐ Reliance on operator is reduced.
- ☐ Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.

Question 881

The FIRST step in establishing a firewall security policy is to determine the:

- ☐ necessary logical access rights.
- ☐ expected data throughput.
- ☐ business requirements.
- ☐ existing firewall configuration.

Licensed to Berend Post berend.post@it-university.nl

Question 882

Which of the following is the MOST important factor to consider when establishing a severity hierarchy for information security incidents?

- ☐ Management support
- ☐ Business impact
- ☐ Regulatory compliance
- ☐ Residual risk

Question 883

Which of the following is the PRIMARY advantage of single sign-on (SSO)?

- ☐ Improves system performance
- ☐ Ensures good password practices
- ☐ Improves security
- ☐ Reduces administrative workload.

Question 884

A critical function of a firewall is to act as a:

- ☐ special router that connects the Internet to a LAN.
- ☐ device for preventing authorized users from accessing the LAN.
- ☐ server used to connect authorized users to private trusted network resources.
- ☐ proxy server to increase the speed of access to authorized users.

Question 885

If a database is restored using before-image dumps, where should the process begin following an interruption?

- ☐ Before the last transaction
- ☐ After the last transaction
- ☐ As the first transaction after the latest checkpoint
- ☐ At the last transaction before the latest checkpoint

Question 886

Which of the following would be the MOST secure firewall system?

- ☐ Screened-host firewall
- ☐ Screened-subnet firewall
- ☐ Dual-homed firewall
- ☐ Stateful-inspection firewall

Licensed to Berend Post berend.post@it-university.nl

Question 887

Which of the following is the MOST critical and contributes the greatest to the quality of data in a data warehouse?

- ☐ Accuracy of the source data
- ☐ Credibility of the data source
- ☐ Accuracy of the extraction process
- ☐ Accuracy of the data transformation

Question 888

When reviewing an intrusion detection system (IDS), an IS auditor should be MOST concerned about which of the following?

- ☐ Number of nonthreatening events identified as threatening
- ☐ Attacks not being identified by the system
- ☐ Reports/logs being produced by an automated tool
- ☐ Legitimate traffic being blocked by the system

Question 889

A local area network (LAN) administrator normally would be restricted from:

- ☐ having end-user responsibilities.
- ☐ reporting to the end-user manager
- ☐ having programming responsibilities.
- ☐ being responsible for LAN security administration.

Question 890

Which of the following refers to the act of creating and using an invented scenario to persuade a target to perform an action?

- ☐ Pretexting
- ☐ Backgrounding
- ☐ Check making
- ☐ Bounce checking
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 891

Which of the following is a method to prevent disclosure of classified documents printed on a shared printer?

- ☐ Requiring a key code to be entered on the printer to produce hardcopy
- ☐ Producing a header page with classification level for printed documents
- ☐ Encrypting the data stream between the user's computer and the printer
- ☐ Using passwords to allow authorized users to send documents to the printer

Question 892

An IS auditor is a member of an application development team that is selecting software. Which of the following would impair the auditor's independence?

- ☐ Verifying the weighting of each selection criteria
- ☐ Approving the vendor selection methodology
- ☐ Reviewing the request for proposal (RFP)
- ☐ Witnessing the vendor selection process

Question 893

Transmitting redundant information with each character or frame to facilitate detection and correction of errors is called a:

- ☐ feedback error control.
- ☐ block sum check.
- ☐ forward error control.
- ☐ cyclic redundancy check.

Question 894

Which of the following type of network service stores information about the various resources in a central database on a network and help network devices locate services?

- ☐ DHCP
- ☐ DNS
- ☐ Directory Service
- ☐ Network Management

Licensed to Berend Post berend.post@it-university.nl

Question 895

An organization has installed blade server technology in its data center. To determine whether higher cooling demands are maintained, which of the following should the IS auditor review?

- ☐ Ventilation systems
- ☐ Uninterruptible power supply (UPS) systems
- ☐ Air conditioning capacity
- ☐ Duct maintenance

Question 896

In transport mode, the use of the Encapsulating Security Payload (ESP) protocol is advantageous over the Authentication Header (AH) protocol because it provides:

- ☐ connectionless integrity.
- ☐ data origin authentication.
- ☐ antireplay service.
- ☐ confidentiality.

Question 897

An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

- ☐ True
- ☐ False

Question 898

As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

- ☐ The same value.
- ☐ Greater value.
- ☐ Lesser value.
- ☐ Prior audit reports are not relevant.

Question 899

Electromagnetic emissions from a terminal represent an exposure because they:

- ☐ affect noise pollution.
- ☐ disrupt processor functions.
- ☐ produce dangerous levels of electric current.
- ☐ can be detected and displayed.

Licensed to Berend Post berend.post@it-university.nl

Question 900

Which of the following is one most common way that spyware is distributed?

- ☐ as a trojan horse.
- ☐ as a virus.
- ☐ as an Adware.
- ☐ as a device driver.
- ☐ as a macro.
- ☐ None of the choices.

Question 901

The technique of rummaging through commercial trash to collect useful business information is known as:

- ☐ Information diving
- ☐ Intelligence diving
- ☐ Identity diving
- ☐ System diving
- ☐ Program diving
- ☐ None of the choices.

Question 902

An organization is considering connecting a critical PC-based system to the Internet. Which of the following would provide the BEST protection against hacking?

- ☐ An application-level gateway
- ☐ A remote access server
- ☐ A proxy server
- ☐ Port scanning

Question 903

The MOST important function of a business continuity plan is to:

- ☐ ensure that the critical business functions can be recovered
- ☐ provide procedures for evaluating tests of the business continuity plan
- ☐ provide a schedule of events that has to occur if there is a disaster
- ☐ ensure that all business functions are restored

Licensed to Berend Post berend.post@it-university.nl

Question 904

Using the OSI reference model, what layer(s) is/are used to encrypt data?

- ☐ transport layer
- ☐ Session layer
- ☐ Session and transport layers
- ☐ Data link layer

Question 905

In a decentralized organization, the selection and purchase of IS products is acceptable as long as which of the following conditions exists?

- ☐ The same operating system is used throughout the organization.
- ☐ Various offices are independent and exchange data on an occasional basis.
- ☐ Acquired items are consistent with the organization's short- and long-term IS strategy plans.
- ☐ Managers undertake a full cost-benefit analysis before deciding what to purchase.

Question 906

To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

- ☐ during data preparation.
- ☐ in transit to the computer.
- ☐ between related computer runs.
- ☐ during the return of the data to the user department.

Question 907

Which of the following provides the GREATEST assurance of message authenticity?

- ☐ The prehash code is derived mathematically from the message being sent.
- ☐ The prehash code is encrypted using the sender's private key.
- ☐ The prehash code and the message are encrypted using the secret key.
- ☐ The sender attains the recipient's public key and verifies the authenticity of its digital certificate with a certificate authority.

Licensed to Berend Post berend.post@it-university.nl

Question 908

An IS auditor conducting a review of disaster recovery planning (DRP) at a financial processing organization has discovered the following:

-The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.

-The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting his/her attention.

-The plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.

The basis of an organization's disaster recovery plan is to reestablish live processing at an alternative site where a similar, but not identical, hardware configuration is already established. An IS auditor should:

- ☐ take no action as the lack of a current plan is the only significant finding.
- ☐ recommend that the hardware configuration at each site is identical.
- ☐ perform a review to verify that the second configuration can support live processing.
- ☐ report that the financial expenditure on the alternative site is wasted without an effective plan.

Question 909

In an annual audit cycle, the audit of an organization’s IT department resulted in many findings. Which of the following would be the MOST important consideration when planning the next audit?

- ☐ Limiting the review to the deficient areas
- ☐ Verifying that all recommendations have been implemented
- ☐ Postponing the review until all of the findings have been rectified
- ☐ Following up on the status of all recommendations

Question 910

Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?

- ☐ Restricting evidence access to professionally certified forensic investigators
- ☐ Engaging an independent third party to perform the forensic investigation
- ☐ Performing investigative procedures on the original hard drives rather than images of the hard drives
- ☐ Documenting evidence handling by personnel throughout the forensic investigation

Licensed to Berend Post berend.post@it-university.nl

Question 911

After a full operational contingency test, an IS auditor performs a review of the recovery steps. The auditor concludes that the time it took for the technological environment and systems to return to full-functioning exceeded the required critical recovery time. Which of the following should the auditor recommend?

- ☐ Perform an integral review of the recovery tasks.
- ☐ Broaden the processing capacity to gain recovery time.
- ☐ Make improvements in the facility's circulation structure.
- ☐ increase the amount of human resources involved in the recovery.

Question 912

Which of the following is the MOST reliable network connection medium in an environment where there is strong electromagnetic interference?

- ☐ Coaxial cable
- ☐ Fiber optic cable
- ☐ Shielded twisted-pair cable
- ☐ Wireless link

Question 913

Pretexting is an act of:

- ☐ DoS
- ☐ social engineering
- ☐ eavedropping
- ☐ soft coding
- ☐ hard coding
- ☐ None of the choices.

Question 914

What should be the information security manager’s MOST important consideration when planning a disaster recovery test?

- ☐ Stakeholder notification procedures
- ☐ Organization-wide involvement
- ☐ Impact to production systems
- ☐ Documented escalation processes

Licensed to Berend Post berend.post@it-university.nl

Question 915

Which of the following is a ITU-T standard protocol suite for packet switched wide area network communication?

- ☐ Point-to-point protocol
- ☐ X.25
- ☐ Frame Relay
- ☐ ISDN

Question 916

A hot site should be implemented as a recovery strategy when the:

- ☐ disaster tolerance is low.
- ☐ recovery point objective (RPO) is high.
- ☐ recovery time objective (RTO) is high.
- ☐ disaster tolerance is high.

Question 917

For which of the following applications would rapid recovery be MOST crucial?

- ☐ Point-of-sale system
- ☐ Corporate planning
- ☐ Regulatory reporting
- ☐ Departmental chargeback

Question 918

Which of the following would BEST provide executive management with current information on IT-related costs and IT performance indicators?

- ☐ IT dashboard
- ☐ Risk register
- ☐ IT service-management plan
- ☐ Continuous audit reports

Question 919

An organization allows its employees to use personal mobile devices for work. Which of the following would BEST maintain information security without compromising employee privacy?

- ☐ Partitioning the work environment from personal space on devices
- ☐ Preventing users from adding applications
- ☐ Restricting the use of devices for personal purposes during working hours
- ☐ Installing security software on the devices

Licensed to Berend Post berend.post@it-university.nl

Question 920

Which of the following reduces the potential impact of social engineering attacks?

- ☐ Compliance with regulatory requirements
- ☐ Promoting ethical understanding
- ☐ Security awareness programs
- ☐ Effective performance incentives

Question 921

When determining the specifications for a server supporting an online application using more than a hundred endpoints, which of the following is the MOST important factor to be considered?

- ☐ High availability of different systems
- ☐ Cost-benefit comparison between the available systems
- ☐ Reputation of the vendors and their customer base
- ☐ Transaction volume estimate during peak periods

Question 922

Which of the following should be of GREATEST concern to an IS auditor conducting an audit of incident response procedures?

- ☐ End users have not completed security awareness training.
- ☐ Senior management is not involved in the incident response process.
- ☐ There is no procedure in place to learn from previous security incidents.
- ☐ Critical incident response events are not recorded in a centralized repository.

Question 923

What must an IS auditor understand before performing an application audit?

- ☐ The potential business impact of application risks.
- ☐ Application risks must first be identified.
- ☐ Relative business processes.
- ☐ Relevant application risks.

Question 924

Which of the following should concern an IS auditor when reviewing security in a client- server environment?

- ☐ Protecting data using an encryption technique
- ☐ Preventing unauthorized access using a diskless workstation
- ☐ The ability of users to access and modify the database directly
- ☐ Disabling floppy drives on the users' machines

Licensed to Berend Post berend.post@it-university.nl

Question 925

Which of the following should be the PRIMARY consideration for IT management when selecting a new information security tool that monitors suspicious file access patterns?

- ☐ Integration with existing architecture
- ☐ Ease of support and troubleshooting
- ☐ Data correlation and visualization capabilities
- ☐ Ability to contribute to key performance indicator data

Question 926

Which of the following is the MOST important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings?

- ☐ Peak activity periods for the business
- ☐ Remediation dates included in management responses
- ☐ Availability of IS audit resources
- ☐ Complexity of business processes identified in the audit

Question 927

Applying a digital signature to data traveling in a network provides:

- ☐ confidentiality and integrity.
- ☐ security and nonrepudiation.
- ☐ integrity and nonrepudiation.
- ☐ confidentiality and nonrepudiation.

Question 928

Which of the following human resources management practices BEST leads to the detection of fraudulent activity?

- ☐ Background checks
- ☐ Time reporting
- ☐ Employee code of ethics
- ☐ Mandatory time off

Licensed to Berend Post berend.post@it-university.nl

Question 929

Which of the following is the MOST important driver when developing an effective information security strategy?

- ☐ Security audit reports
- ☐ Benchmarking reports
- ☐ Information security standards
- ☐ Compliance requirements

Question 930

An advantage of using sanitized live transactions in test data is that:

- ☐ all transaction types will be included.
- ☐ every error condition is likely to be tested.
- ☐ no special routines are required to assess the results.
- ☐ test transactions are representative of live processing.

Question 931

Which of the following is the BEST information source for management to use as an aid in the identification of assets that are subject to laws and regulations?

- ☐ Security incident summaries
- ☐ Vendor best practices
- ☐ CERT coordination center
- ☐ Significant contracts

Question 932

Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

- ☐ Gateway
- ☐ Protocol converter
- ☐ Front-end communication processor
- ☐ Concentrator/multiplexor

Question 933

Which of the following methods would BEST ensure that IT strategy is in line with business strategy?

- ☐ Break-even-point analysis
- ☐ IT value analysis
- ☐ Critical path analysis
- ☐ Business impact analysis (BIA)

Licensed to Berend Post berend.post@it-university.nl

Question 934

Which of the following would be the BEST overall control for an Internet business looking for confidentiality, reliability and integrity of data?

- ☐ Secure Sockets Layer (SSL)
- ☐ Intrusion detection system (IDS)
- ☐ Public key infrastructure (PKI)
- ☐ Virtual private network (VPN)

Question 935

An organization can ensure that the recipients of e-mails from its employees can authenticate the identity of the sender by:

- ☐ digitally signing all e-mail messages.
- ☐ encrypting all e-mail messages.
- ☐ compressing all e-mail messages.
- ☐ password protecting all e-mail messages.

Question 936

An employee of an organization has reported losing a smartphone that contains sensitive information. The BEST step to address this situation should be to:

- ☐ terminate the device connectivity
- ☐ escalated to the user's management
- ☐ disable the user's access to corporate resources
- ☐ remotely wipe the device

Question 937

Which of the following is the MOST important aspect relating to employee termination?

- ☐ The details of employee have been removed from active payroll files.
- ☐ Company property provided to the employee has been returned.
- ☐ User ID and passwords of the employee have been deleted.
- ☐ The appropriate company staff are notified about the termination.

Licensed to Berend Post berend.post@it-university.nl

Question 938

Which of the following is the BEST source for describing the objectives of an organization's information systems?

- ☐ Business process owners
- ☐ End users
- ☐ IT management
- ☐ Information security management

Question 939

Both statistical and nonstatistical sampling techniques:

- ☐ permit the auditor to quantify the probability of error.
- ☐ permit the auditor to quantify and fix the level of risk.
- ☐ require judgment when defining population characteristics.
- ☐ provide each item an equal opportunity of being selected.

Question 940

An IS auditor should carefully review the functional requirements in a system-development project to ensure that the project is designed to:

- ☐ Meet business objectives
- ☐ Enforce data security
- ☐ Be culturally feasible
- ☐ Be financially feasible

Question 941

Which of the following would BEST help to support an auditor's conclusion about the effectiveness of an implemented data classification program?

- ☐ Detailed data classification scheme
- ☐ Access rights provisioned according to scheme
- ☐ Business use cases and scenarios
- ☐ Purchase of information management tools

Question 942

Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

- ☐ True
- ☐ False

Licensed to Berend Post berend.post@it-university.nl

Question 943

Which of the following term in business continuity determines the maximum acceptable amount of data loss measured in time?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 944

When an employee is terminated from service, the MOST important action is to:

- ☐ hand over all of the employee's files to another designated employee.
- ☐ complete a backup of the employee's work.
- ☐ notify other employees of the termination.
- ☐ disable the employee's logical access.

Question 945

A structured walk-through test of a disaster recovery plan involves:

- ☐ representatives from each of the functional areas coming together to go over the plan.
- ☐ all employees who participate in the day-to-day operations coming together to practice executing the plan.
- ☐ moving the systems to the alternate processing site and performing processing operations.
- ☐ distributing copies of the plan to the various functional areas for review.

Question 946

What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off?

- ☐ Employee security awareness training
- ☐ Administrator alerts
- ☐ Screensaver passwords
- ☐ Close supervision

Licensed to Berend Post berend.post@it-university.nl

Question 947

What is essential for the IS auditor to obtain a clear understanding of network management?

- ☐ Security administrator access to systems
- ☐ Systems logs of all hosts providing application services
- ☐ A graphical map of the network topology
- ☐ Administrator access to systems

Question 948

Which procedure provides the GREATEST assurance that corrective action to an audit report has been taken?

- ☐ Performing subsequent audit tests to verify resolution of the deficiencies
- ☐ Inquiring about the current status of the recommendation
- ☐ Reporting to the audit committee or the board of directors concerning specific action taken or lack thereof
- ☐ Requesting a written management reply to the audit report, identifying corrective action for each deficiency

Question 949

Which of the following would be MOST useful to an information security manager when conducting a post-incident review of an attack?

- ☐ Details from intrusion detection system logs
- ☐ Method of operation used by the attacker
- ☐ Cost of the attack to the organization
- ☐ Location of the attacker

Question 950

A penetration test performed as part of evaluating network security:

- ☐ provides assurance that all vulnerabilities are discovered.
- ☐ should be performed without warning the organization's management.
- ☐ exploits the existing vulnerabilities to gain unauthorized access.
- ☐ would not damage the information assets when performed at network perimeters.

Licensed to Berend Post berend.post@it-university.nl

Question 951

Multiple invoices are usually received for individual purchase orders, since purchase orders require staggered delivery dates. Which of the following is the BEST audit technique to test for duplicate payments?

- ☐ Run the data on the software programs used to process supplier payments.
- ☐ Use generalized audit software on the invoice transaction file.
- ☐ Run the data on the software programs used to process purchase orders.
- ☐ Use generalized audit software on the purchase order transaction file.

Question 952

Which of the following is a software application that pretend to be a server on the Internet and is not set up purposely to actively protect against break-ins?

- ☐ Bastion host
- ☐ Honey pot
- ☐ Dual Homed
- ☐ Demilitarize Zone (DMZ)

Question 953

Which of the following types of attack works by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs?

- ☐ format string vulnerabilities
- ☐ integer overflow
- ☐ code injection
- ☐ command injection
- ☐ None of the choices.

Question 954

Which of the following measures can effectively minimize the possibility of buffer overflows?

- ☐ Sufficient bounds checking
- ☐ Sufficient memory
- ☐ Sufficient processing capability
- ☐ Sufficient code injection
- ☐ None of the choices

Licensed to Berend Post berend.post@it-university.nl

Question 955

The use of symmetric key encryption controls to protect sensitive data transmitted over a communications network requires that:

- ☐ primary keys for encrypting the data be stored in encrypted form.
- ☐ encryption keys be changed only when a compromise is detected at both ends.
- ☐ encryption keys at one end be changed on a regular basis.
- ☐ public keys be stored in encrypted form.

Question 956

Which of the following controls would provide the GREATEST assurance of database integrity?

- ☐ Audit log procedures
- ☐ Table link/reference checks
- ☐ Query/table access time checks
- ☐ Rollback and roll forward database features

Question 957

An IS auditor performing a review of an application's controls would evaluate the:

- ☐ efficiency of the application in meeting the business processes.
- ☐ impact of any exposures discovered.
- ☐ business processes served by the application.
- ☐ application's optimization.

Question 958

Which of the following would be the BEST population to take a sample from when testing program changes?

- ☐ Test library listings
- ☐ Source program listings
- ☐ Program change requests
- ☐ Production library listings

Question 959

After the release of an application system, an IS auditor wants to verify that the system is providing value to the organization. The auditor's BEST course of action would be to:

- ☐ review the results of compliance testing.
- ☐ quantify improvements in client satisfaction.
- ☐ confirm that risk has declined since the application system release.
- ☐ perform a gap analysis against the benefits defined in the business case.

Licensed to Berend Post berend.post@it-university.nl

Question 960

A grants management system is used to calculate grant payments. Once per day, a batch interface extracts grant amounts and payee details from this system for import into the finance system so payments can be made overnight. Which of the following controls provides the GREATEST assurance and completeness of the imported payments?

- ☐ Performing monthly bank reconciliations in a timely manner
- ☐ Restricting access to the grants and finance systems
- ☐ Reviewing transaction logs for anomalies
- ☐ Reconciling data from both systems

Question 961

The PRIMARY objective of an audit of IT security policies is to ensure that:

- ☐ they are distributed and available to all staff.
- ☐ security and control policies support business and IT objectives.
- ☐ there is a published organizational chart with functional descriptions.
- ☐ duties are appropriately segregated.

Question 962

What is the MOST prevalent security risk when an organization implements remote virtual private network (VPN) access to its network?

- ☐ Malicious code could be spread across the network
- ☐ VPN logon could be spoofed
- ☐ Traffic could be sniffed and decrypted
- ☐ VPN gateway could be compromised

Question 963

A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

- ☐ reasonableness check.
- ☐ parity check.
- ☐ redundancy check.
- ☐ check digits.

Licensed to Berend Post berend.post@it-university.nl

Question 964

Which of the following is the BEST type of program for an organization to implement to aggregate, correlate and store different log and event files, and then produce weekly and monthly reports for IS auditors?

- ☐ A security information event management (SIEM) product
- ☐ An open-source correlation engine
- ☐ A log management tool
- ☐ An extract, transform, load (ETL) system

Question 965

Which of the following is the MOST important reason for performing vulnerability assessments periodically?

- ☐ Technology risks must be mitigated.
- ☐ Management requires regular reports.
- ☐ The environment changes constantly.
- ☐ The current threat levels are being assessed.

Question 966

Which of the following scenarios would enable a forensic investigation?

- ☐ The suspected computer was rebooted, and the evidence log file was converted to a readable format for further analysis.
- ☐ The incident response team prepared a final report for the forensic investigator and deleted the original file securely to avoid further damage.
- ☐ The media in question was preserved using imaging, and chain of custody was documented according to the organization's incident response plan.
- ☐ Incident response team members extracted the logs showing the suspicious activity and added their notes before submitting for investigation.

Question 967

During a human resources (HR) audit, an IS auditor is informed that there is a verbal agreement between the IT and HR departments as to the level of IT services expected. In this situation, what should the IS auditor do FIRST?

- ☐ Postpone the audit until the agreement is documented
- ☐ Report the existence of the undocumented agreement to senior management
- ☐ Confirm the content of the agreement with both departments
- ☐ Draft a service level agreement (SLA) for the two departments

Licensed to Berend Post berend.post@it-university.nl

Question 968

In reviewing the IT strategic plan, the IS auditor should consider whether it identifies the:

- ☐ major IT initiatives.
- ☐ links to operational tactical plans.
- ☐ allocation of IT staff
- ☐ project management methodologies used.

Question 969

Implementing a strong password policy is part of an organization's information security strategy for the year. A business unit believes the strategy may adversely affect a client's adoption of a recently developed mobile application and has decided not to implement the policy. Which of the following would be the information security manager's BEST course of action?

- ☐ Analyze the risk and impact of not implementing the policy
- ☐ Develop and implement a password policy for the mobile application
- ☐ Escalate non-implementation of the policy to senior management
- ☐ Benchmark with similar mobile applications to identify gaps

Question 970

As part of the business continuity planning process, which of the following should be identified FIRST in the business impact analysis?

- ☐ Organizational risks, such as single point-of-failure and infrastructure risk
- ☐ Threats to critical business processes
- ☐ Critical business processes for ascertaining the priority for recovery
- ☐ Resources required for resumption of business

Question 971

A risk analysis for a new system is being performed. For which of the following is business knowledge MORE important than IT knowledge?

- ☐ Vulnerability analysis
- ☐ Cost-benefit analysis
- ☐ Impact analysis
- ☐ Balanced scorecard

Licensed to Berend Post berend.post@it-university.nl

Question 972

Which of the following external entities would provide the BEST guidance to an organization facing advanced attacks?

- ☐ Recognized threat intelligence communities
- ☐ Open-source reconnaissance
- ☐ Disaster recovery consultants widely endorsed in industry forums
- ☐ Incident response experts from highly regarded peer organizations

Question 973

Which of the following data validation control validates input data against predefined range values?

- ☐ Range Check
- ☐ Table lookups
- ☐ Existence check
- ☐ Reasonableness check

Question 974

The optimum business continuity strategy for an entity is determined by the:

- ☐ lowest downtime cost and highest recovery cost.
- ☐ lowest sum of downtime cost and recovery cost.
- ☐ lowest recovery cost and highest downtime cost.
- ☐ average of the combined downtime and recovery cost.

Question 975

Due to the increasing size of a database, user access times and daily backups continue to increase. Which of the following would be the BEST way to address this situation?

- ☐ Data modeling
- ☐ Data visualization
- ☐ Data mining
- ☐ Data purging

Question 976

Reverse proxy technology for web servers should be deployed if:

- ☐ http servers' addresses must be hidden.
- ☐ accelerated access to all published pages is required.
- ☐ caching is needed for fault tolerance.
- ☐ bandwidth to the user is limited.

Licensed to Berend Post berend.post@it-university.nl

Question 977

A comprehensive IS audit policy should include guidelines detailing what involvement the internal audit team should have?

- ☐ in the development and coding of major OS applications.
- ☐ in the acquisition and maintenance of major WEB applications.
- ☐ in the human resource management cycle of the application development project.
- ☐ in the development, acquisition, conversion, and testing of major applications.
- ☐ None of the choices.

Question 978

When following up on a data breach, an IS auditor finds a system administrator may have compromised the chain of custody. Which of the following should the system administrator have done FIRST to preserve the evidence?

- ☐ Perform forensic discovery
- ☐ Notify key stakeholders
- ☐ Quarantine the system
- ☐ Notify the incident response team

Question 979

Which of the following should be an IS auditor's FIRST action when assessing the risk associated with unstructured data?

- ☐ Implement strong encryption for unstructured data.
- ☐ Implement user access controls to unstructured data.
- ☐ Identify repositories of unstructured data.
- ☐ Identify appropriate tools for data classification.

Question 980

An IS auditor is reviewing IT policies and found that most policies have not been reviewed in over 3 years. The MOST significant risk is that the policies do not reflect:

- ☐ current legal requirements.
- ☐ the vision of the CEO.
- ☐ the mission of the organization.
- ☐ current industry best practices.

Licensed to Berend Post berend.post@it-university.nl

Question 981

Which of the following database model allow many-to-many relationships in a tree-like structure that allows multiple parents?

- ☐ Hierarchical database model
- ☐ Network database model
- ☐ Relational database model
- ☐ Object-relational database model

Question 982

During an IS audit, one of your auditor has observed that some of the critical servers in your organization can be accessed ONLY by using shared/common user name and password. What should be the auditor's PRIMARY concern be with this approach?

- ☐ Password sharing
- ☐ Accountability
- ☐ Shared account management
- ☐ Difficulty in auditing shared account

Question 983

An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

- ☐ cold site.
- ☐ warm site.
- ☐ dial-up site.
- ☐ duplicate processing facility.

Question 984

An information security manager has developed a strategy to address new information security risks resulting from recent changes in the business. Which of the following would be MOST important to include when presenting the strategy to senior management?

- ☐ The impact of organizational changes on the security risk profile
- ☐ The costs associated with business process changes
- ☐ Results of benchmarking against industry peers
- ☐ Security controls needed for risk mitigation

Licensed to Berend Post berend.post@it-university.nl

Question 985

Which of the following layer of an enterprise data flow architecture is concerned with basic data communication?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☐ Internet/Intranet layer
- ☐ Data access layer

Question 986

Which of the following should be an IS auditor's BEST recommendation to prevent installation of unlicensed software on employees' company-provided devices?

- ☐ Enforce audit logging of software installation activities.
- ☐ Restrict software installation authority to administrative users only.
- ☐ Implement software blacklisting.
- ☐ Remove unlicensed software from end-user devices.

Question 987

Software is considered malware based on:

- ☐ the intent of the creator.
- ☐ its particular features.
- ☐ its location.
- ☐ its compatibility.
- ☐ None of the choices.

Question 988

While planning a review of IT governance, the IS auditor is MOST likely to:

- ☐ examine audit committee minutes for IS-related matters and their control.
- ☐ obtain information about the framework of control adopted by management.
- ☐ assess whether business process owner responsibilities are consistent across the organization.
- ☐ review compliance with policies and procedures issued by the board of directors.

Licensed to Berend Post berend.post@it-university.nl

Question 989

When conducting a review of security incident management, an IS auditor found there are no defined escalation processes. All incidents are managed by the service desk. Which of the following should be the auditor's PRIMARY concern?

- ☐ Inefficient use of service desk resources
- ☐ Management's lack of high impact incidents
- ☐ Delays in resolving low priority trouble tickets
- ☐ Management's inability to follow up on incident resolution

Question 990

Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

- ☐ Ensuring that invoices are paid to the provider
- ☐ Participating in systems design with the provider
- ☐ Renegotiating the provider's fees
- ☐ Monitoring the outsourcing provider's performance

Question 991

What control detects transmission errors by appending calculated bits onto the end of each segment of data?

- ☐ Reasonableness check
- ☐ Parity check
- ☐ Redundancy check
- ☐ Check digits

Question 992

Which of the following is the BEST data integrity check?

- ☐ Counting the transactions processed per day
- ☐ Performing a sequence check
- ☐ Tracing data back to the point of origin
- ☐ Preparing and running test data

Licensed to Berend Post berend.post@it-university.nl

Question 993

Which of the following could be used to evaluate the effectiveness of IT operations?

- ☐ Total cost of ownership
- ☐ Net present value
- ☐ Balanced scorecard
- ☐ Internal rate of return

Question 994

Allowing application programmers to directly patch or change code in production programs increases risk of fraud. True or false?

- ☐ True
- ☐ False

Question 995

Which of the following ACID property ensures that transaction will bring the database from one valid state to another?

- ☐ Atomicity
- ☐ Consistency
- ☐ Isolation
- ☐ Durability

Question 996

During an audit of the logical access control of an ERP financial system an IS auditor found some user accounts shared by multiple individuals. The user IDs were based on roles rather than individual identities. These accounts allow access to financial transactions on the ERP. What should the IS auditor do next?

- ☐ Look for compensating controls.
- ☐ Review financial transactions logs.
- ☐ Review the scope of the audit.
- ☐ Ask the administrator to disable these accounts.

Licensed to Berend Post berend.post@it-university.nl

Question 997

When reviewing an organization's strategic IT plan an IS auditor should expect to find:

- ☐ an assessment of the fit of the organization's application portfolio with business objectives.
- ☐ actions to reduce hardware procurement cost.
- ☐ a listing of approved suppliers of IT contract resources.
- ☐ a description of the technical architecture for the organization's network perimeter security.

Question 998

The MOST effective control for addressing the risk of piggybacking is:

- ☐ a single entry point with a receptionist.
- ☐ the use of smart cards.
- ☐ a biometric door lock.
- ☐ a deadman door.

Question 999

Before implementing controls, management should FIRST ensure that the controls:

- ☐ satisfy a requirement in addressing a risk issue.
- ☐ do not reduce productivity.
- ☐ are based on a cost-benefit analysis.
- ☐ are detective or corrective.

Question 1000

The MOST important reason why an IT risk assessment should be updated on a regular basis is to:

- ☐ utilize IT resources in a cost-effective manner
- ☐ comply with data classification changes
- ☐ comply with risk management policies
- ☐ react to changes in the IT environment

Question 1001

Planning for the implementation of an information security program is MOST effective when it:

- ☐ uses risk-based analysis for security projects.
- ☐ applies technology-driven solutions to identified needs.
- ☐ uses decision trees to prioritize security projects.
- ☐ applies gap analysis to current and future business plans.

Licensed to Berend Post berend.post@it-university.nl

Question 1002

Which of the following should be of concern to an IS auditor performing a software audit on virtual machines?

- ☐ Software licensing does not support virtual machines.
- ☐ Software has been installed on virtual machines by privileged users.
- ☐ Multiple users can access critical applications.
- ☐ Applications have not been approved by the CFO.

Question 1003

The purpose of a mainframe audit is to provide assurance that processes are being implemented as required, the mainframe is operating as it should, security is strong, and that procedures in place are working and are updated as needed. The auditor may accordingly make recommendations for improvement. Which of the following types of audit always takes high priority over the others? (Choose five.)

- ☐ System audit
- ☐ Application audit
- ☐ Software audit
- ☐ License audit
- ☐ Security server audit
- ☐ None of the choices.

Question 1004

Which of the following is the MOST important action in recovering from a cyberattack?

- ☐ Creation of an incident response team
- ☐ Use of cyber forensic investigators
- ☐ Execution of a business continuity plan
- ☐ Filling an insurance claim

Question 1005

The use of residual biometric information to gain unauthorized access is an example of which of the following attacks?

- ☐ Replay
- ☐ Brute force
- ☐ Cryptographic
- ☐ Mimic

Licensed to Berend Post berend.post@it-university.nl

Question 1006

What is the PRIMARY objective of performing a vulnerability assessment following a business system update?

- ☐ Update the threat landscape
- ☐ Review the effectiveness of controls
- ☐ Determine operational losses
- ☐ Improve the change control process

Question 1007

A review of an organization's IT portfolio revealed several applications that are not in use. The BEST way to prevent this situation from recurring would be to implement:

- ☐ a formal request for proposal (RFP) process
- ☐ an information asset acquisition policy
- ☐ asset life cycle management
- ☐ business case development procedures

Question 1008

Which of the following is an advantage of prototyping?

- ☐ The finished system normally has strong internal controls.
- ☐ Prototype systems can provide significant time and cost savings.
- ☐ Change control is often less complicated with prototype systems.
- ☐ it ensures that functions or extras are not added to the intended system.

Question 1009

What is a data validation edit control that matches input data to an occurrence rate? Choose the BEST answer.

- ☐ Accuracy check
- ☐ Completeness check
- ☐ Reasonableness check
- ☐ Redundancy check

Licensed to Berend Post berend.post@it-university.nl

Question 1010

Assessments of critical information systems are based on a cyclical audit plan that has not been updated for several years. Which of the following should the IS auditor recommend to BEST address this situation?

- ☐ Use a revolving set of audit plans to cover all systems
- ☐ Update the audit plan quarterly to account for delays and deferrals of periodic reviews
- ☐ Regularly validate the audit plan against business risks
- ☐ Do not include periodic reviews in detail as part of the audit plan

Question 1011

Management has agreed to perform multiple remediation actions in response to an audit issue, including the implementation of a new control. Which of the following is the BEST time for an IS auditor to perform an audit follow-up of this issue?

- ☐ After management has completed the required actions
- ☐ When audit resources are available
- ☐ When management resources are available
- ☐ After the new control has been in place for one year

Question 1012

An IS auditor reviewing a proposed application software acquisition should ensure that the:

- ☐ operating system (OS) being used is compatible with the existing hardware platform.
- ☐ planned OS updates have been scheduled to minimize negative impacts on company needs.
- ☐ OS has the latest versions and updates.
- ☐ products are compatible with the current or planned OS.

Question 1013

Which of the following step of PDCA implement the plan, execute the process and make product?

- ☐ Plan
- ☐ Do
- ☐ Check
- ☐ Act

Licensed to Berend Post berend.post@it-university.nl

Question 1014

Which of the following is not a common method of multiplexing data?

- ☐ Analytical multiplexing
- ☐ Time-division multiplexing
- ☐ Asynchronous time-division multiplexing
- ☐ Frequency division multiplexing

Question 1015

Which of the following is the BEST detective control for a job scheduling process involving data transmission?

- ☐ Metrics denoting the volume of monthly job failures are reported and reviewed by senior management.
- ☐ Job failure alerts are automatically generated and routed to support personnel.
- ☐ Jobs are scheduled and a log of this activity is retained for subsequent review.
- ☐ Jobs are scheduled to be completed daily and data is transmitted using a secure File Transfer Protocol (FTP).

Question 1016

The PRIMARY reason for an IS auditor to use data analytics techniques is to reduce which type of audit risk?

- ☐ Technology risk
- ☐ Inherent risk
- ☐ Detection risk
- ☐ Control risk

Question 1017

Which of the following could be determined by an entity-relationship diagram?

- ☐ Links between data objects
- ☐ How the system behaves as a consequence of external events
- ☐ How data are transformed as they move through the system
- ☐ Modes of behavior of data objects

Licensed to Berend Post berend.post@it-university.nl

Question 1018

In the event of a disruption or disaster, which of the following technologies provides for continuous operations?

- ☐ Load balancing
- ☐ Fault-tolerant hardware
- ☐ Distributed backups
- ☐ High-availability computing

Question 1019

In computer forensics, which of the following is the process that allows bit-for-bit copy of a data to avoid damage of original data or information when multiple analysis may be performed?

- ☐ Imaging
- ☐ Extraction
- ☐ Data Protection
- ☐ Data Acquisition

Question 1020

Which of the following is MOST important to include in forensic data collection and preservation procedures?

- ☐ Maintaining chain of custody
- ☐ Preserving data integrity
- ☐ Determining tools to be used
- ☐ Assuring the physical security of devices

Question 1021

Following a breach, what is the BEST source to determine the maximum amount of time before customers must be notified that their personal information may have been compromised?

- ☐ Industry standards
- ☐ Information security policy
- ☐ Incident response plan
- ☐ Industry regulations

Licensed to Berend Post berend.post@it-university.nl

Question 1022

Which of the following should an IS auditor review to gain an understanding of the effectiveness of controls over the management of multiple projects?

- ☐ Project database
- ☐ Policy documents
- ☐ Project portfolio database
- ☐ Program organization

Question 1023

Which of the following responsibilities of an organization's quality assurance function should raise concern for an IS auditor?

- ☐ Ensuring the test work supports observations
- ☐ Ensuring standards are adhered to within the development process
- ☐ Implementing solutions to correct defects
- ☐ Updating development methodology

Question 1024

Which of the following is the MOST effective way to reduce risk to an organization from widespread use of web-based communication technologies?

- ☐ Publish an enterprise-wide policy outlining acceptance use of web-based communication technologies.
- ☐ Incorporate risk awareness training for web-based communications into the IT security program.
- ☐ Monitor staff usage of web-based communication and notify the IT security department of violations.
- ☐ Block access from user devices to unauthorized pages that allow web-based communication.

Question 1025

Which of the following is a practice that should be incorporated into the plan for testing disaster recovery procedures?

- ☐ Invite client participation.
- ☐ involve all technical staff.
- ☐ Rotate recovery managers.
- ☐ install locally-stored backup.

Licensed to Berend Post berend.post@it-university.nl

Question 1026

Which of the following INCORRECTLY describes the layer function of the Application Layer within the TCP/IP model?

- ☐ Provides user interface
- ☐ Perform data processing such as encryption, encoding, etc
- ☐ Provides reliable delivery
- ☐ Keeps separate the data of different applications

Question 1027

An example of a direct benefit to be derived from a proposed IT-related business investment is:

- ☐ enhanced reputation.
- ☐ enhanced staff morale.
- ☐ the use of new technology.
- ☐ increased market penetration.

Question 1028

Which of the following correctly describe the potential problem of deploying Wi-Fi Protected Access to secure your wireless network?

- ☐ potential compatibility problems with wireless network interface cards.
- ☐ potential compatibility problems with wireless access points.
- ☐ potential performance problems with wireless network interface cards.
- ☐ potential performance problems with wireless access points.
- ☐ None of the choices.

Question 1029

Which of the following is the GREATEST risk when relying on reports generated by end-user computing?

- ☐ Data may be inaccurate
- ☐ Reports may not work efficiently
- ☐ Reports may not be timely
- ☐ Historical data may not be available

Licensed to Berend Post berend.post@it-university.nl

Question 1030

An appropriate control for ensuring the authenticity of orders received in an EDI application is to:

- ☐ acknowledge receipt of electronic orders with a confirmation message.
- ☐ perform reasonableness checks on quantities ordered before filling orders.
- ☐ verify the identity of senders and determine if orders correspond to contract terms.
- ☐ encrypt electronic orders.

Question 1031

During Involuntary termination of an employee, which of the following is the MOST important step to be considered?

- ☐ Get a written NDA agreement from an employee
- ☐ Terminate all physical and logical access
- ☐ Provide compensation in lieu of notice period
- ☐ Do not communicate to the respective employee about the termination

Question 1032

An IS auditor is unable to directly test privacy controls for a client's cloud-based application. The MOST effective alternative to direct testing is to review:

- ☐ the provider's internal audit reports.
- ☐ the provider's statement of assurance.
- ☐ formal privacy certification.
- ☐ independent audit reports.

Question 1033

Which of the following attack is MOSTLY performed by an attacker to steal the identity information of a user such as credit card number, passwords, etc?

- ☐ Smurf attack
- ☐ Traffic analysis
- ☐ Harming
- ☐ Interrupt attack

Licensed to Berend Post berend.post@it-university.nl

Question 1034

Which of the following is the MOST effective way to ensure security policies are relevant to organizational business practices?

- ☐ Leverage security steering committee contribution.
- ☐ Obtain senior management sign-off.
- ☐ Integrate industry best practices.
- ☐ Conduct an organization-wide security audit.

Question 1035

Email required for business purposes is being stored on employees' personal devices. Which of the following is an IS auditor's BEST recommendation?

- ☐ Implement an email containerization solution on personal devices
- ☐ Prohibit employees from storing company email on personal devices.
- ☐ Ensure antivirus to utilize passwords on personal devices.
- ☐ Require employees to utilize passwords on personal devices.

Question 1036

Which of the following results in a denial-of-service attack?

- ☐ Brute force attack
- ☐ Ping of death
- ☐ Leapfrog attack
- ☐ Negative acknowledgement (NAK) attack

Question 1037

To ensure message integrity, confidentiality and non-repudiation between two parties, the MOST effective method would be to create a message digest by applying a cryptographic hashing algorithm against:

- ☐ the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key by using the receiver's public key.
- ☐ any part of the message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key using the receiver's public key.
- ☐ the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering both the encrypted message and digest using the receiver's public key.
- ☐ the entire message, enciphering the message digest using the sender's private key and enciphering the message using the receiver's public key.

Licensed to Berend Post berend.post@it-university.nl

Question 1038

Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?

- ☐ increase the time allocated for system testing
- ☐ implement formal software inspections
- ☐ increase the development staff
- ☐ Require the sign-off of all project deliverables

Question 1039

Which of the following is a concern when data are transmitted through Secure Sockets Layer (SSL) encryption, implemented on a trading partner's server?

- ☐ The organization does not have control over encryption.
- ☐ Messages are subjected to wiretapping.
- ☐ Data might not reach the intended recipient.
- ☐ The communication may not be secure.

Question 1040

Which of the following step of PDCA study the actual result and compares it against the expected result?

- ☐ Plan
- ☐ Do
- ☐ Check
- ☐ Act

Question 1041

An internal audit department recently established a quality assurance (QA) program. Which of the following activities is MOST important to include as part of the QA program requirements?

- ☐ Ongoing monitoring of the audit activities
- ☐ Analysis of user satisfaction reports from business lines.
- ☐ Feedback from internal audit staff
- ☐ Long-term internal audit resource planning

Licensed to Berend Post berend.post@it-university.nl

Question 1042

What type(s) of firewalls provide(s) the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic?

- ☐ A first-generation packet-filtering firewall
- ☐ A circuit-level gateway
- ☐ An application-layer gateway, or proxy firewall, and stateful-inspection firewalls
- ☐ An application-layer gateway, or proxy firewall, but not stateful-inspection firewalls

Question 1043

Which of the following cloud deployment model is formed by the composition of two or more cloud deployment mode?

- ☐ Private Cloud
- ☐ Community Cloud
- ☐ Public Cloud
- ☐ Hybrid Cloud

Question 1044

You should keep all computer rooms at reasonable temperatures, which is in between (choose all that apply):

- ☐ 60 - 75 degrees Fahrenheit
- ☐ 10 - 25 degrees Celsius
- ☐ 30 - 45 degrees Fahrenheit
- ☐ 1 - 15 degrees Celsius
- ☐ 20 - 35 degrees Fahrenheit
- ☐ 0 - 5 degrees Celsius

Question 1045

Which of the following encryption methods uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message?

- ☐ Blowfish
- ☐ Tripwire
- ☐ certificate
- ☐ DES
- ☐ one-time pad
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 1046

A vulnerability in which of the following virtual systems would be of GREATEST concern to the IS auditor?

- ☐ The virtual machine management server
- ☐ The virtual file server
- ☐ The virtual application server
- ☐ The virtual antivirus server

Question 1047

A core tenant of an IS strategy is that it must:

- ☐ Be inexpensive
- ☐ Be protected as sensitive confidential information
- ☐ Protect information confidentiality, integrity, and availability
- ☐ Support the business objectives of the organization

Question 1048

Which of the following level in CMMI model focuses on process innovation and continuous optimization?

- ☐ Level 4
- ☐ Level 5
- ☐ Level 3
- ☐ Level 2

Question 1049

An IS auditor is involved in the user testing phase of a development project. The developers wish to use a copy of a peak volume transaction file from the production process to show that the development can cope with the required volume. What is the auditor's PRIMARY concern?

- ☐ Sensitive production data may be read by unauthorized persons.
- ☐ The error-handling and credibility checks may not be fully proven.
- ☐ Users may not wish for production data to be made available for testing.
- ☐ All functionality of the new process may not be tested.

Licensed to Berend Post berend.post@it-university.nl

Question 1050

Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the recipient's private key.
True or false?

- ☐ False
- ☐ True

Question 1051

After reviewing its business processes, a large organization is deploying a new web application based on a VoIP technology. Which of the following is the MOST appropriate approach for implementing access control that will facilitate security management of the VoIP web application?

- ☐ Fine-grained access control
- ☐ Role-based access control (RBAC)
- ☐ Access control lists
- ☐ Network/service access control

Question 1052

Which of the following is the BEST reason to certify an organization to an international security standard?

- ☐ The certification covers enterprise security end-to-end.
- ☐ The certification reduces information security risk.
- ☐ The certification ensures that optimal controls are in place.
- ☐ The certification delivers value to stakeholders.

Question 1053

Which of the following should be the FIRST step when drafting an incident response plan for a new cyber-attack scenario?

- ☐ Schedule response testing
- ☐ Create a new incident response team
- ☐ Create a reporting template
- ☐ Identify relevant stakeholders

Licensed to Berend Post berend.post@it-university.nl

Question 1054

Talking about biometric measurement, which of the following measures the percent of invalid users who are incorrectly accepted in?

- ☐ failure to reject rate
- ☐ false accept rate
- ☐ false reject rate
- ☐ failure to enroll rate
- ☐ None of the choices.

Question 1055

During a help desk review, an IS auditor determines the call abandonment rate exceeds agreed-upon service levels. What conclusions can be drawn from this finding?

- ☐ There are insufficient telephone lines available to the help desk.
- ☐ There is insufficient staff to handle the help desk call volume.
- ☐ Help desk staff are unable to resolve a sufficient number of problems on the first call.
- ☐ Users are finding solutions from alternative sources.

Question 1056

Which of the following is the MOST important factor when determining the frequency of information security risk reassessment?

- ☐ Audit findings
- ☐ Risk priority
- ☐ Mitigating controls
- ☐ Risk metrics

Question 1057

Which of the following occurs during the issues management process for a system development project?

- ☐ Contingency planning
- ☐ Impact assessment
- ☐ Configuration management
- ☐ Help desk management

Licensed to Berend Post berend.post@it-university.nl

Question 1058

An IS auditor has completed a service level management audit related to order management services provided by a third party. Which of the following is the MOST significant finding?

- ☐ The third party has offshore support arrangements.
- ☐ Penalties for missing service levels are limited.
- ☐ The service level agreement does not define how availability is measured.
- ☐ Service desk support is not available outside the company's business hours.

Question 1059

To minimize the cost of a software project, quality management techniques should be applied:

- ☐ as close to their writing (i.e., point of origination) as possible.
- ☐ primarily at project start-up to ensure that the project is established in accordance with organizational governance standards.
- ☐ continuously throughout the project with an emphasis on finding and fixing defects primarily during testing to maximize the defect detection rate.
- ☐ mainly at project close-down to capture lessons learned that can be applied to future projects.

Question 1060

An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

- ☐ True
- ☐ False

Question 1061

Which of the following help(s) prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack?

- ☐ Inbound traffic filtering
- ☐ Using access control lists (ACLs) to restrict inbound connection attempts
- ☐ Outbound traffic filtering
- ☐ Recentralizing distributed systems

Licensed to Berend Post berend.post@it-university.nl

Question 1062

To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following?

- ☐ The business objectives of the organization
- ☐ The effect of segregation of duties on internal controls
- ☐ The point at which controls are exercised as data flows through the system
- ☐ Organizational control policies

Question 1063

An organization has implemented a disaster recovery plan. Which of the following steps should be carried out next?

- ☐ Obtain senior management sponsorship.
- ☐ Identify business needs.
- ☐ Conduct a paper test.
- ☐ Perform a system restore test.

Question 1064

Which of the following is the BEST method for uncovering shadow IT within an organization?

- ☐ Analyze help desk tickets.
- ☐ Review secondary approval thresholds.
- ☐ Use a cloud access security broker (CASB).
- ☐ Review business processes.

Question 1065

Which of the following layer of an OSI model transmits and receives the bit stream as electrical, optical or radio signals over an appropriate medium or carrier?

- ☐ Transport Layer
- ☐ Network Layer
- ☐ Data Link Layer
- ☐ Physical Layer

Licensed to Berend Post berend.post@it-university.nl

Question 1066

The ability of the internal IS audit function to achieve desired objectives depends largely on:

- ☐ the training of audit personnel
- ☐ the background of audit personnel
- ☐ the independence of audit personnel
- ☐ the performance of audit personnel
- ☐ None of the choices.

Question 1067

Which of the following would be of GREATEST concern to an IS auditor receiving an organization's security incident handling procedures?

- ☐ Annual tabletop exercises are performed instead of functional incident response exercises.
- ☐ Roles for computer emergency response team (CERT) members have not been formally documented.
- ☐ Guidelines for prioritizing incidents have not been identified.
- ☐ Workstation antivirus software alerts are not regularly reviewed.

Question 1068

In the absence of technical controls, what would be the BEST way to reduce unauthorized text messaging on company-supplied mobile devices?

- ☐ Update the corporate mobile usage policy to prohibit texting.
- ☐ Conduct a business impact analysis (BIA) and provide the report to management.
- ☐ Stop providing mobile devices until the organization is able to implement controls.
- ☐ Include the topic of prohibited texting in security awareness training.

Question 1069

Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?

- ☐ Session keys are dynamic
- ☐ Private symmetric keys are used
- ☐ Keys are static and shared
- ☐ Source addresses are not encrypted or authenticated

Licensed to Berend Post berend.post@it-university.nl

Question 1070

In a relational database with referential integrity, the use of which of the following keys would prevent deletion of a row from a customer table as long as the customer number of that row is stored with live orders on the orders table?

- ☐ Foreign key
- ☐ Primary key
- ☐ Secondary key
- ☐ Public key

Question 1071

Distributed denial-of-service (DDOS) attacks on Internet sites are typically evoked by hackers using which of the following?

- ☐ Logic bombs
- ☐ Phishing
- ☐ Spyware
- ☐ Trojan horses

Question 1072

A perpetrator looking to gain access to and gather information about encrypted data being transmitted over the network would use:

- ☐ eavesdropping
- ☐ spoofing.
- ☐ traffic analysis.
- ☐ masquerading.

Question 1073

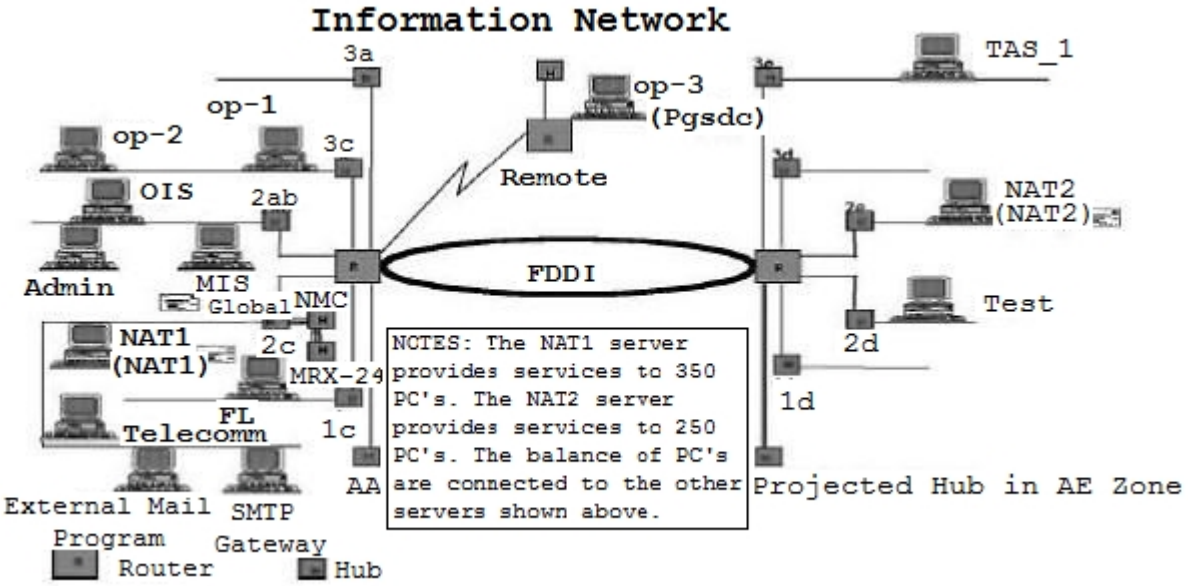
Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

- ☐ Check digit
- ☐ Existence check
- ☐ Completeness check
- ☐ Reasonableness check

Licensed to Berend Post berend.post@it-university.nl

Question 1074

In the 2c area of the diagram, there are three hubs connected to each other. What potential risk might this indicate?



- ☐ Virus attack
- ☐ Performance degradation
- ☐ Poor management controls
- ☐ Vulnerability to external hackers

Question 1075

Which of the following will replace system binaries and/or hook into the function calls of the operating system to hide the presence of other programs (choose the most precise answer)?

- ☐ rootkits
- ☐ virus
- ☐ trojan
- ☐ tripwire
- ☐ None of the choices.

Question 1076

What is wrong with a Black Box type of intrusion detection system?

- ☐ you cannot patch it
- ☐ you cannot test it
- ☐ you cannot examine its internal workings from outside.
- ☐ you cannot tune it
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 1077

Two-factor authentication can be circumvented through which of the following attacks?

- ☐ Denial-of-service
- ☐ Man-in-the-middle
- ☐ Key logging
- ☐ Brute force

Question 1078

Which of the following internet security threats could compromise integrity?

- ☐ Theft of data from the client
- ☐ Exposure of network configuration information
- ☐ A Trojan horse browser
- ☐ Eavesdropping on the net

Question 1079

Which of the following statement INCORRECTLY describes network device such as a Router?

- ☐ Router creates a new header for each packet
- ☐ Router builds a routing table based on MAC address
- ☐ Router does not forward broadcast packet
- ☐ Router assigns a different network address per port

Question 1080

With the help of a security officer, granting access to data is the responsibility of:

- ☐ data owners.
- ☐ programmers.
- ☐ system analysts.
- ☐ librarians.

Question 1081

Which of the following is widely accepted as one of the critical components in networking management?

- ☐ Configuration management
- ☐ Topological mappings
- ☐ Application of monitoring tools
- ☐ Proxy server troubleshooting

Licensed to Berend Post berend.post@it-university.nl

Question 1082

During a review of an organization's IT incident management practices, the IS auditor finds the quality of incident resolution documentation is poor. Which of the following is the BEST recommendation to help address this issue?

- ☐ Have service desk staff create documentation be choosing from pre-selected answers in the service management tool.
- ☐ Require service desk staff to open incident tickets only when they have sufficient information.
- ☐ Revise incident resolution procedures and provide training for service desk staff on the applicable updates.
- ☐ Require peer review of resolution documentation followed by service desk management sign off.

Question 1083

An IS auditor reviewing an organization's IT strategic plan should FIRST review:

- ☐ the existing IT environment.
- ☐ the business plan.
- ☐ the present IT budget.
- ☐ current technology trends.

Question 1084

An organization uses electronic funds transfer (EFT) to pay its vendors. Which of the following should be an IS auditor's MAIN focus while reviewing controls in the accounts payable application?

- ☐ Changes to the vendor master file
- ☐ Volume of transactions
- ☐ Amount of disbursements
- ☐ Frequency of transactions

Question 1085

In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

- ☐ The data should be deleted and overwritten with binary 0s.
- ☐ The data should be demagnetized.
- ☐ The data should be low-level formatted.
- ☐ The data should be deleted.

Licensed to Berend Post berend.post@it-university.nl

Question 1086

Which of the following is protocol data unit (PDU) of transport layer in TCP/IP model?

- ☐ Data
- ☐ Segment
- ☐ Packet
- ☐ Frame

Question 1087

An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST cost-effective test of the DRP?

- ☐ Full operational test
- ☐ Preparedness test
- ☐ Paper test
- ☐ Regression test

Question 1088

An IS auditor's PRIMARY concern when application developers wish to use a copy of yesterday's production transaction file for volume tests is that:

- ☐ users may prefer to use contrived data for testing.
- ☐ unauthorized access to sensitive data may result.
- ☐ error handling and credibility checks may not be fully proven.
- ☐ the full functionality of the new process may not necessarily be tested.

Question 1089

Which of the following is the MOST reasonable option for recovering a noncritical system?

- ☐ Warm site
- ☐ Mobile site
- ☐ Hot site
- ☐ Cold site

Licensed to Berend Post berend.post@it-university.nl

Question 1090

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the CRC- 32 checksum for:

- ☐ integrity.
- ☐ validity.
- ☐ accuracy.
- ☐ confidentiality.
- ☐ None of the choices.

Question 1091

Sending a message and a message hash encrypted by the sender's private key will ensure:

- ☐ authenticity and integrity.
- ☐ authenticity and privacy.
- ☐ integrity and privacy.
- ☐ privacy and nonrepudiation.

Question 1092

Talking about the different approaches to security in computing, the principle of regarding the computer system itself as largely an untrusted system emphasizes:

- ☐ most privilege
- ☐ full privilege
- ☐ least privilege
- ☐ null privilege
- ☐ None of the choices.

Question 1093

An IS auditor is using a statistical sample to inventory the tape library. What type of test would this be considered?

- ☐ Substantive
- ☐ Compliance
- ☐ Integrated
- ☐ Continuous audit

Licensed to Berend Post berend.post@it-university.nl

Question 1094

When introducing a maturity model to the IT management process, it is BEST to align the maturity level to a point that reflects which of the following?

- ☐ Ideal business production level
- ☐ Minimum cost expenditure level
- ☐ Maximum risk tolerance level
- ☐ Industry-standard practice level

Question 1095

A manufacturing company is implementing application software for its sales and distribution system. Which of the following is the MOST important reason for the company choose a centralized online database?

- ☐ Enhanced data redundancy
- ☐ Elimination of multiple points of failure
- ☐ Elimination of the need for data normalization
- ☐ Enhanced integrity controls

Question 1096

Following significant organizational changes, which of the following is the MOST important consideration when updating the IT policy?

- ☐ The policy is integrated into job descriptions.
- ☐ The policy is endorsed by senior executives.
- ☐ The policy is compliant with relevant laws and regulations.
- ☐ The policy is aligned with industry standards and best practice.

Question 1097

When considering whether to adopt bring your own device (BYOD), it is MOST important for the information security manager to ensure that:

- ☐ security controls are applied to each device when joining the network
- ☐ business leaders have an understanding of security risks
- ☐ users have read and signed acceptable use agreements
- ☐ the applications are tested prior to implementation

Licensed to Berend Post berend.post@it-university.nl

Question 1098

In planning a major system development project, function point analysis would assist in:

- ☐ estimating the elapsed time of the project.
- ☐ estimating the size of a system development task.
- ☐ analyzing the functions undertaken by system users as an aid to job redesign.
- ☐ determining the business functions undertaken by a system or program.

Question 1099

Why is one-time pad not always preferable for encryption (choose all that apply):

- ☐ it is difficult to use securely.
- ☐ it is highly inconvenient to use.
- ☐ it requires licensing fee.
- ☐ it requires internet connectivity.
- ☐ it is Microsoft only.
- ☐ None of the choices.

Question 1100

Due to a recent business divesture, an organization has limited IT resources to deliver critical projects. Reviewing the IT staffing plan against which of the following would BEST guide IT management when estimating resource requirements for future projects?

- ☐ Peer organizational staffing benchmarks
- ☐ Budgeted forecast for the next financial year
- ☐ Human resources sourcing strategy
- ☐ Records of actual time spent on projects

Question 1101

Which of the following protects against the impact of temporary and rapid decreases or increases in electricity?

- ☐ Redundant power supply
- ☐ Emergency power-off switch
- ☐ Stand-by generator
- ☐ Uninterruptible power supply (UPS)

Licensed to Berend Post berend.post@it-university.nl

Question 1102

The most likely error to occur when implementing a firewall is:

- ☐ incorrectly configuring the access lists.
- ☐ compromising the passwords due to social engineering.
- ☐ connecting a modem to the computers in the network.
- ☐ inadequately protecting the network and server from virus attacks.

Question 1103

E-mail message authenticity and confidentiality is BEST achieved by signing the message using the:

- ☐ sender's private key and encrypting the message using the receiver's public key.
- ☐ sender's public key and encrypting the message using the receiver's private key.
- ☐ receiver's private key and encrypting the message using the sender's public key.
- ☐ receiver's public key and encrypting the message using the sender's private key.

Question 1104

The BEST access strategy while configuring a firewall would be to:

- ☐ permit access to all and log the activity
- ☐ deny access to all but permit selected
- ☐ permit access to all but deny selected
- ☐ deny access to all except authorized programs

Question 1105

Which of the following is a data validation edit and control?

- ☐ Hash totals
- ☐ Reasonableness checks
- ☐ Online access controls
- ☐ Before and after image reporting

Question 1106

An efficient use of public key infrastructure (PKI) should encrypt the:

- ☐ entire message.
- ☐ private key.
- ☐ public key.
- ☐ symmetric session key.

Licensed to Berend Post berend.post@it-university.nl

Question 1107

Am advantage of the use of hot sites as a backup alternative is that:

- ☐ the costs associated with hot sites are low.
- ☐ hot sites can be used for an extended amount of time.
- ☐ hot sites can be made ready for operation within a short period of time.
- ☐ they do not require that equipment and systems software be compatible with the primary site.

Question 1108

What is the BEST population to select from when testing that programs are migrated to production with proper approval?

- ☐ List of changes provided by application programming managers
- ☐ List of production programs
- ☐ Completed change request forms
- ☐ Change advisory board meeting minutes

Question 1109

After assessing risk, the decision to treat the risk should be based PRIMARILY on:

- ☐ whether the level of risk exceeds risk appetite
- ☐ availability of financial resources
- ☐ whether the level of risk exceeds inherent risk
- ☐ the criticality of the risk

Question 1110

The BEST filter rule for protecting a network from being used as an amplifier in a denial of service (DoS) attack is to deny all:

- ☐ outgoing traffic with IP source addresses externa! to the network.
- ☐ incoming traffic with discernible spoofed IP source addresses.
- ☐ incoming traffic with IP options set.
- ☐ incoming traffic to critical hosts.

Licensed to Berend Post berend.post@it-university.nl

Question 1111

Which of the following activities would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA)?

- ☐ Developing the CSA questionnaire
- ☐ Developing the remediation plan
- ☐ Implementing the remediation plan
- ☐ Partially completing the CSA

Question 1112

An IS auditor examining the configuration of an operating system to verify the controls should review the:

- ☐ transaction logs.
- ☐ authorization tables.
- ☐ parameter settings.
- ☐ routing tables.

Question 1113

An IS auditor conducting audit follow-up activities learns that some previously agreed-upon corrective actions have not been taken and that the associated risk has been accepted by senior management. If the auditor disagrees with management's decision, what is the BEST way to address the situation?

- ☐ Repeat the audit with audit scope only covering areas with accepted risks
- ☐ Report the issue to the chief audit executive for resolution
- ☐ Recommend new corrective actions to mitigate the accepted risk
- ☐ Take no action since management's decision has been made

Question 1114

Which of the following uses a prototype that can be updated continually to meet changing user or business requirements?

- ☐ PERT
- ☐ Rapid application development (RAD)
- ☐ Function point analysis (FPA)
- ☐ GANTT

Licensed to Berend Post berend.post@it-university.nl

Question 1115

An IS auditor observes an organization is performing data backup and restoration testing on an ad hoc basis without a defined process. What is the MOST likely result of a data disruption event?

- ☐ Increased loss impact
- ☐ Decreased data confidentiality
- ☐ Increased likelihood of future risk events
- ☐ Decreased data integrity

Question 1116

An organization's disaster recovery plan should address early recovery of:

- ☐ all information systems processes.
- ☐ all financial processing applications.
- ☐ only those applications designated by the IS manager.
- ☐ processing in priority order, as defined by business management.

Question 1117

Digital signatures require the:

- ☐ signer to have a public key and the receiver to have a private key.
- ☐ signer to have a private key and the receiver to have a public key.
- ☐ signer and receiver to have a public key.
- ☐ signer and receiver to have a private key.

Question 1118

Which of the following would BEST detect logic bombs in the new programs?

- ☐ Final acceptance testing by users
- ☐ Parallel/pilot testing
- ☐ Regression testing
- ☐ Independent program review

Question 1119

Which of the following is an analytical review procedure for a payroll system?

- ☐ Performing penetration attempts on the payroll system
- ☐ Evaluating the performance of the payroll system, using benchmarking software
- ☐ Performing reasonableness tests by multiplying the number of employees by the average wage rate
- ☐ Testing hours reported on time sheets

Licensed to Berend Post berend.post@it-university.nl

Question 1120

Which of the following should be the MOST important consideration when prioritizing the funding for competing IT projects?

- ☐ Criteria used to determine the benefits of projects
- ☐ Skills and capabilities within the project management team
- ☐ Quality and accuracy of the IT project inventory
- ☐ Senior management preferences

Question 1121

An organization was recently notified by its regulatory body of significant discrepancies in its reporting data. A preliminary investigation revealed that the discrepancies were caused by problems with the organization's data quality. Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be advisors to the process. After the data quality team identifies the system data at fault, which of the following should internal audit recommend as the NEXT step in the process?

- ☐ Create business rules that validate data quality.
- ☐ Develop an improvement plan.
- ☐ Identify the root cause of data quality problems.
- ☐ Identify the source data owners.

Question 1122

An organization has decided to migrate payroll processing to a new platform hosted by a third party in a different country. Which of the following is MOST important for the IS auditor to consider?

- ☐ The service provider's compliance with privacy regulations
- ☐ Whether the contract contains a right-to-terminate clause
- ☐ The service provider's compliance with financial regulations
- ☐ Storage costs charged by the service provider

Question 1123

Which of the following controls can BEST detect accidental corruption during transmission of data across a network?

- ☐ Sequence checking
- ☐ Parity checking
- ☐ Symmetric encryption
- ☐ Check digit verification

Licensed to Berend Post berend.post@it-university.nl

Question 1124

An organization has outsourced some of its subprocesses to a service provider. When scoping the audit of the provider, the organization's internal auditor should FIRST:

- ☐ evaluate operational controls of the provider
- ☐ discuss audit objectives with the provider
- ☐ review internal audit reports of the provider
- ☐ review the contract with the provider

Question 1125

Which of the following is the MOST important requirement for the successful implementation of security governance?

- ☐ Aligning to an international security framework
- ☐ Mapping to organizational strategies
- ☐ Implementing a security balanced scorecard
- ☐ Performing an enterprise-wide risk assessment

Question 1126

Fault-tolerance is a feature particularly sought-after in which of the following kinds of computer systems:

- ☐ desktop systems
- ☐ laptop systems
- ☐ handheld PDAs
- ☐ business-critical systems
- ☐ None of the choices.

Question 1127

An IS auditor is reviewing the remote access methods of a company used to access system remotely. Which of the following is LEAST preferred remote access method from a security and control point of view?

- ☐ RADIUS
- ☐ TACACS
- ☐ DIAL-UP
- ☐ DIAMETER

Licensed to Berend Post berend.post@it-university.nl

Question 1128

When designing an incident response plan to be agreed upon with a cloud computing vendor, including which of the following will BEST help to ensure the effectiveness of the plan?

- ☐ A training program for the vendor staff
- ☐ An audit and compliance program
- ☐ Responsibility and accountability assignments
- ☐ Requirements for onsite recovery testing

Question 1129

Which of the following sampling techniques is commonly used in fraud detection when the expected occurrence rate is small and the specific controls are critical?

- ☐ Discovery sampling
- ☐ Monetary unit sampling
- ☐ Stop-or-go sampling
- ☐ Random sampling

Question 1130

An information security manager is concerned that executive management does not support information security initiatives. Which of the following is the BEST way to address this situation?

- ☐ Demonstrate alignment of the information security function with business needs.
- ☐ Escalate noncompliance concerns to the internal audit manager.
- ☐ Report the risk and status of the information security program to the board.
- ☐ Revise the information security strategy to meet executive management's expectations.

Question 1131

Which of the following would an IS auditor use to determine if unauthorized modifications were made to production programs?

- ☐ System log analysis
- ☐ Compliance testing
- ☐ Forensic analysis
- ☐ Analytical review

Licensed to Berend Post berend.post@it-university.nl

Question 1132

An organization performs nightly backups but does not have a formal policy. An IS auditor should FIRST:

- ☐ evaluate current backup procedures
- ☐ escalate to senior management
- ☐ document a policy for the organization
- ☐ recommend automated backup

Question 1133

Which of the following is the PRIMARY reason for an IS auditor to use computer-assisted audit techniques (CAATs)?

- ☐ To efficiently test an entire population
- ☐ To perform direct testing of production data
- ☐ To conduct automated sampling for testing
- ☐ To enable quicker access to information

Question 1134

Which of the following is MOST likely to reduce the effectiveness of a signature-based intrusion detection system (IDS)?

- ☐ The activities being monitored deviate from what is considered normal.
- ☐ The environment is complex.
- ☐ The pattern of normal behavior changes quickly and dramatically.
- ☐ The information regarding monitored activities becomes state.

Question 1135

Which of the following should be the PRIMARY basis for planning and prioritizing IT infrastructure security audits?

- ☐ Asset value to the organization
- ☐ Management requests
- ☐ The organization's risk appetite
- ☐ Security best practice

Licensed to Berend Post berend.post@it-university.nl

Question 1136

An IS auditor is reviewing a bank's service level agreement (SLA) with a third-party provider that hosts the bank's secondary data center. Which of the following findings should be of GREATEST concern to the auditor?

- ☐ The recovery point objective (RPO) has a shorter duration than documented in the disaster recovery plan
- ☐ The recovery time objective (RTO) has a longer duration than documented in the disaster recovery plan
- ☐ Backup data is hosted online only
- ☐ The SLA has not been reviewed in more than a year

Question 1137

Which of the following would BEST facilitate the detection of internal fraud perpetrated by an individual?

- ☐ Corporate fraud hotline
- ☐ Segregation of duties
- ☐ Mandatory leave
- ☐ Flexible time

Question 1138

The PRIMARY advantage of a continuous audit approach is that it:

- ☐ does not require an IS auditor to collect evidence on system reliability while processing is taking place.
- ☐ requires the IS auditor to review and follow up immediately on all information collected.
- ☐ can improve system security when used in time-sharing environments that process a large number of transactions.
- ☐ does not depend on the complexity of an organization's computer systems.

Question 1139

Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

- ☐ Function point analysis
- ☐ Earned value analysis
- ☐ Cost budget
- ☐ Program Evaluation and Review Technique

Licensed to Berend Post berend.post@it-university.nl

Question 1140

Which of the following tasks should be performed FIRST when preparing a disaster recovery plan?

- ☐ Develop a recovery strategy.
- ☐ Perform a business impact analysis.
- ☐ Map software systems, hardware and network components.
- ☐ Appoint recovery teams with defined personnel, roles and hierarchy.

Question 1141

Which of the following controls would be MOST effective in ensuring that production source code and object code are synchronized?

- ☐ Release-to-release source and object comparison reports
- ☐ Library control software restricting changes to source code
- ☐ Restricted access to source code and object code
- ☐ Date and time-stamp reviews of source and object code

Question 1142

Labeling information according to its security classification:

- ☐ reduces the need to identify baseline controls for each classification.
- ☐ reduces the number and type of countermeasures required.
- ☐ enhances the likelihood of people handling information securely.
- ☐ affects the consequences if information is handled insecurely.

Question 1143

When conducting a penetration test of an IT system, an organization should be MOST concerned with:

- ☐ the confidentiality of the report.
- ☐ finding all possible weaknesses on the system.
- ☐ restoring all systems to the original state.
- ☐ logging all changes made to the production system.

Question 1144

Which of the following should an IS auditor be MOST concerned with during a post-implementation review?

- ☐ The system does not have a maintenance plan
- ☐ The system contains several minor defects
- ☐ The system was over budget by 15%
- ☐ The system deployment was delayed by three weeks

Licensed to Berend Post berend.post@it-university.nl

Question 1145

Which of the following is MOST likely to enable a hacker to successfully penetrate a system?

- ☐ Lack of virus protection
- ☐ Unpatched software
- ☐ Decentralized dialup access
- ☐ Lack of DoS protection

Question 1146

A LAN administrator normally would be restricted from:

- ☐ having end-user responsibilities.
- ☐ reporting to the end-user manager.
- ☐ having programming responsibilities.
- ☐ being responsible for LAN security administration.

Question 1147

Which of the following is the MAIN purpose of implementing an incident response process?

- ☐ Provide substantial audit-trail evidence.
- ☐ Assign roles and responsibilities.
- ☐ Comply with policies and procedures.
- ☐ Manage impact due to breaches.

Question 1148

Which of the following method should be recommended by security professional to erase the data on the magnetic media that would be reused by another employee?

- ☐ Degaussing
- ☐ Overwrite every sector of magnetic media with pattern of 1's and 0's
- ☐ Format magnetic media
- ☐ Delete File allocation table

Licensed to Berend Post berend.post@it-university.nl

Question 1149

Audit management has just completed the annual audit plan for the upcoming year, which consists entirely of high-risk processes. However, it is determined that there are insufficient resources to execute the plan. What should be done NEXT?

- ☐ Remove audits from the annual plan to better match the number of resources available
- ☐ Reduce the scope of the audits to better match the number of resources available
- ☐ Present the annual plan to the audit committee and ask for more resources
- ☐ Review the audit plan and defer some audits to the subsequent year

Question 1150

A major portion of what is required to address nonrepudiation is accomplished through the use of:

- ☐ strong methods for authentication and ensuring data validity
- ☐ strong methods for authentication and ensuring data integrity.
- ☐ strong methods for authorization and ensuring data integrity.
- ☐ strong methods for authentication and ensuring data reliability.
- ☐ None of the choices.

Question 1151

Which of the following privacy principles ensures data controllers do not use personal data unintended ways that breach protection of data subjects?

- ☐ Data retention
- ☐ Adequacy
- ☐ Accuracy
- ☐ Purpose limitation

Question 1152

Which of the following is the MOST critical step in planning an audit?

- ☐ Implementing a prescribed auditing framework such as COBIT
- ☐ Identifying current controls
- ☐ Identifying high-risk audit targets
- ☐ Testing controls

Licensed to Berend Post berend.post@it-university.nl

Question 1153

Talking about biometric authentication, physical characteristics typically include (Choose five.):

- ☐ fingerprints
- ☐ eye retinas
- ☐ irises
- ☐ facial patterns
- ☐ hand measurements
- ☐ None of the choices.

Question 1154

Which of the following is a detective control that can be used to uncover unauthorized access to information systems?

- ☐ Requiring long and complex passwords for system access
- ☐ Implementing a security information and event management (SIEM) system
- ☐ Requiring internal audit to perform periodic reviews of system access logs
- ☐ Protecting access to the data center with multifactor authentication

Question 1155

While implementing an invoice system, Lily has implemented a database control which checks that new transactions are matched to those previously input to ensure that they have not already been entered. Which of the following control is implemented by Lily?

- ☐ Range Check
- ☐ Duplicate Check
- ☐ Existence check
- ☐ Reasonableness check

Question 1156

Which of the following should be reviewed FIRSTwhen assessing the effectiveness of an organization's network security procedures and controls?

- ☐ Data recovery capability
- ☐ Inventory of authorized devices
- ☐ Vulnerability remediation
- ☐ Malware defenses

Licensed to Berend Post berend.post@it-university.nl

Question 1157

Which of the following is the BEST way to satisfy a two-factor user authentication?

- ☐ A smart card requiring the user's PIN
- ☐ User ID along with password
- ☐ Iris scanning plus fingerprint scanning
- ☐ A magnetic card requiring the user's PIN

Question 1158

When information security management is receiving an increased number of false positive incident reports, which of the following is MOST important to review?

- ☐ The security awareness programs
- ☐ Post-incident analysis results
- ☐ The risk management processes
- ☐ Firewall logs

Question 1159

A security regulation requires the disabling of direct administrator access. Such access must occur through an intermediate server that holds administrator passwords for all systems and records all actions. An IS auditor's PRIMARY concern with this solution would be that:

- ☐ it is not feasible to implement.
- ☐ it represents a single point of failure.
- ☐ segregation of duties is not observed.
- ☐ access logs may not be maintained.

Question 1160

What uses questionnaires to lead the user through a series of choices to reach a conclusion?

- ☐ Logic trees
- ☐ Decision trees
- ☐ Decision algorithms
- ☐ Logic algorithms

Question 1161

Which of the following BEST describes an audit risk?

- ☐ The financial report may contain undetected material errors.
- ☐ The company is being sued for false accusations.
- ☐ Key employees have not taken vacation for 2 years.
- ☐ Employees have been misappropriating funds.

Licensed to Berend Post berend.post@it-university.nl

Question 1162

A recent audit concluded that an organization's information security system was weak and that monitoring would likely fail to detect penetration. Which of the following would be the MOST appropriate recommendation?

- ☐ Look continually for new criminal behavior and attacks on sensitive data
- ☐ Establish a clear policy related to security and the handling of sensitive data
- ☐ Encrypt sensitive data while strengthening the system
- ☐ Identify and periodically remove sensitive data that is no longer needed

Question 1163

Why does the IS auditor often review the system logs?

- ☐ To get evidence of password spoofing
- ☐ To get evidence of data copy activities
- ☐ To determine the existence of unauthorized access to data by a user or program
- ☐ To get evidence of password sharing

Question 1164

Which of the following is MOST directly affected by network performance monitoring tools?

- ☐ Integrity
- ☐ Availability
- ☐ Completeness
- ☐ Confidentiality

Question 1165

Which of the following entities is BEST suited to define the data classification levels within an organization?

- ☐ Database administrator based on the data schema
- ☐ Legal compliance team based on the application regulations
- ☐ Business owner responsible for the respective data
- ☐ System administrator responsible for data security controls

Licensed to Berend Post berend.post@it-university.nl

Question 1166

Which of the following should be the PRIMARY basis for how digital evidence is handled during a forensics investigation?

- ☐ Industry best practices
- ☐ Regulatory requirements
- ☐ Organizational risk culture
- ☐ Established business practices

Question 1167

Which of the following testing method examines the functionality of an application without peering into its internal structure or knowing the details of it's internals?

- ☐ Black-box testing
- ☐ Parallel Test
- ☐ Regression Testing
- ☐ Pilot Testing

Question 1168

Which of the following statement correctly describes the difference between IPSec and SSH protocols?

- ☐ IPSec works at the transport layer where as SSH works at the network layer of an OSI Model
- ☐ IPSec works at the network layer where as SSH works at the application layer of an OSI Model
- ☐ IPSec works at the network layer and SSH works at the transport layer of an OSI Model
- ☐ IPSec works at the transport layer and SSH works at the network layer of an OSI Model

Question 1169

What determines the strength of a secret key within a symmetric key cryptosystem?

- ☐ A combination of key length, degree of permutation, and the complexity of the data-encryption algorithm that uses the key
- ☐ A combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key
- ☐ A combination of key length and the complexity of the data-encryption algorithm that uses the key
- ☐ Initial input vectors and the complexity of the data-encryption algorithm that uses the key

Licensed to Berend Post berend.post@it-university.nl

Question 1170

Receiving an EDI transaction and passing it through the communication's interface stage usually requires:

- ☐ translating and unbundling transactions.
- ☐ routing verification procedures.
- ☐ passing data to the appropriate application system.
- ☐ creating a point of receipt audit log.

Question 1171

An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted as defect fixes are implemented by developers. Which of the following would be the BEST recommendation for an IS auditor to make?

- ☐ Consider feasibility of a separate user acceptance environment
- ☐ Schedule user testing to occur at a given time each day
- ☐ implement a source code version control tool
- ☐ Only retest high priority defects

Question 1172

Which of the following would be MOST important to update once a decision has been made to outsource a critical application to a cloud service provider?

- ☐ Project portfolio
- ☐ IT resource plan
- ☐ IT budget
- ☐ Business impact analysis (BIA)

Question 1173

An IS auditor conducts a review of a third-party vendor’s reporting of key performance indicators (KPIs). Which of the following findings should be of MOST concern to the auditor?

- ☐ Some KPIs are not documented.
- ☐ KPIs have never been updated.
- ☐ KPIs data is not being analyzed.
- ☐ KPIs are not clearly defined.

Licensed to Berend Post berend.post@it-university.nl

Question 1174

In which of the following transmission media it is MOST difficult to modify the information traveling across the network?

- ☐ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Coaxial cable

Question 1175

The activation of an enterprise's business continuity plan should be based on predetermined criteria that address the:

- ☐ duration of the outage.
- ☐ type of outage.
- ☐ probability of the outage.
- ☐ cause of the outage.

Question 1176

During an audit of an organization's incident management process, an IS auditor learns that the security operations team includes detailed reports of recent attacks in its communications to employees. Which of the following is the GREATEST concern with this situation?

- ☐ Employees may fail to understand the severity of the threats.
- ☐ The reports may be too complex for a nontechnical audience.
- ☐ Employees may misuse the information in the reports.
- ☐ There is not a documented procedure to communicate the reports.

Question 1177

When is regression testing used to determine whether new application changes have introduced any errors in the remaining unchanged code?

- ☐ In program development and change management
- ☐ In program feasibility studies
- ☐ In program development
- ☐ In change management

Licensed to Berend Post berend.post@it-university.nl

Question 1178

An organization wants to reuse company-provided smartphones collected from staff leaving the organization. Which of the following would be the BEST recommendation?

- ☐ The memory cards of the smartphones should be replaced.
- ☐ Smartphones should not be reused, but physically destroyed.
- ☐ Data should be securely deleted from the smartphones.
- ☐ The SIM card and telephone number should be changed.

Question 1179

An IS auditor is evaluating the completeness of privacy procedures involving personally identifiable information (PII). Which of the following is MOST important for the auditor to verify is included in the procedures?

- ☐ Regulatory requirements for protecting PII
- ☐ The organization's definition of PII
- ☐ Encryption requirements for transmitting PII externally
- ☐ A description of how PII is masked within key systems

Question 1180

An advantage in using a bottom-up vs. a top-down approach to software testing is that:

- ☐ interface errors are detected earlier.
- ☐ confidence in the system is achieved earlier.
- ☐ errors in critical modules are detected earlier.
- ☐ major functions and processing are tested earlier.

Question 1181

With respect to the outsourcing of IT services, which of the following conditions should be of GREATEST concern to an IS auditor?

- ☐ Outsourced activities are core and provide a differentiated advantage to the organization.
- ☐ Periodic renegotiation is specified in the outsourcing contract.
- ☐ The outsourcing contract fails to cover every action required by the arrangement.
- ☐ Similar activities are outsourced to more than one vendor.

Licensed to Berend Post berend.post@it-university.nl

Question 1182

Which of the following term describes a failure of an electric utility company to supply power within acceptable range?

- ☐ Sag
- ☐ Blackout
- ☐ Brownout
- ☐ EMI

Question 1183

Which of the following are designed to detect network attacks in progress and assist in post- attack forensics?

- ☐ Intrusion Detection Systems
- ☐ Audit trails
- ☐ System logs
- ☐ Tripwire
- ☐ None of the choices.

Question 1184

Which of the following data would be used when performing a business impact analysis (BIA)?

- ☐ Projected impact of current business on future business
- ☐ Cost of regulatory compliance
- ☐ Cost benefit analysis of running the current business
- ☐ Expected costs for recovering the business.

Question 1185

Which of the following is penetration test where the penetration tester is provided with limited or no knowledge of the target's information systems?

- ☐ External Testing
- ☐ Internal Testing
- ☐ Blind Testing
- ☐ Targeted Testing

Licensed to Berend Post berend.post@it-university.nl

Question 1186

Which of the following is MOST important to the successful implementation of an information security governance framework across the organization?

- ☐ The existing organizational security culture
- ☐ Security management processes aligned with security objectives
- ☐ Organizational security controls deployed in line with regulations
- ☐ Security policies that adhere to industry best practices

Question 1187

An organization has a recovery time objective (RTO) equal to zero and a recovery point objective (RPO) close to 1 minute for a critical system. This implies that the system can tolerate:

- ☐ a data loss of up to 1 minute, but the processing must be continuous.
- ☐ a 1-minute processing interruption but cannot tolerate any data loss.
- ☐ a processing interruption of 1 minute or more.
- ☐ both a data less and processing interruption longer than 1 minute.

Question 1188

The MOST efficient way to confirm that an ERP system being implemented satisfies business expectations is to utilize which of the following types of testing?

- ☐ Parallel
- ☐ Pilot
- ☐ Sociability
- ☐ Alpha

Question 1189

Which of the following would be considered an essential feature of a network management system?

- ☐ A graphical interface to map the network topology
- ☐ Capacity to interact with the Internet to solve the problems
- ☐ Connectivity to a help desk for advice on difficult issues
- ☐ An export facility for piping data to spreadsheets

Licensed to Berend Post berend.post@it-university.nl

Question 1190

The business owner's approval of software changes being moved into production is PRIMARILY necessary to:

- ☐ ensure that an application functionality requirement is satisfied.
- ☐ prevent unauthorized access to data.
- ☐ inform management of deployments of new functionality.
- ☐ confirm there is a process to control system changes.

Question 1191

Which of the following is a reason for implementing a decentralized IT governance model?

- ☐ Standardized controls and economies of scale
- ☐ IT synergy among business units
- ☐ Greater consistency among business units
- ☐ Greater responsiveness to business needs

Question 1192

Which of the following would BEST provide assurance of the integrity of new staff?

- ☐ background screening
- ☐ References
- ☐ Bonding
- ☐ Qualifications listed on a resume

Question 1193

Which of the following would be of GREATEST concern to an IS auditor evaluating governance over open source development components?

- ☐ The development project has gone over budget and time
- ☐ The open source development components do not meet industry best practices
- ☐ The software is not analyzed for compliance with organizational requirements
- ☐ Existing open source policies have not been approved in over a year

Question 1194

An employee has accidentally posted confidential data to the company's social media page. Which of the following is the BEST control to prevent this from recurring?

- ☐ Require all updates to be made by the marketing director
- ☐ Implement a moderator approval process
- ☐ Perform periodic audits of social media updates
- ☐ Establish two-factor access control for social media accounts

Licensed to Berend Post berend.post@it-university.nl

Question 1195

During a review of a production schedule, an IS auditor observes that a staff member is not complying with mandatory operational procedures. The auditor's NEXT step should be to:

- ☐ determine why the procedures were not followed.
- ☐ include the noncompliance in the audit report.
- ☐ note the noncompliance in the audit working papers.
- ☐ issue an audit memorandum identifying the noncompliance.

Question 1196

Everything not explicitly permitted is forbidden has which of the following kinds of tradeoff?

- ☐ it improves security at a cost in functionality.
- ☐ it improves functionality at a cost in security.
- ☐ it improves security at a cost in system performance.
- ☐ it improves performance at a cost in functionality.
- ☐ None of the choices.

Question 1197

At a project steering committee meeting, it is stated that adding controls to business processes undergoing re-engineering is an unnecessary cost. The IS auditor's BEST response is that the actual control overhead for a business process is:

- ☐ usually considerable, but the benefits of good controls always exceed the cost.
- ☐ the responsibility of the project manager, and the cost should have been included in the budget.
- ☐ usually difficult to ascertain but is justifiable, because controls are essential to doing business
- ☐ usually less than the potential cost of failure caused by lack of controls.

Question 1198

An advantage of installing a thin client architecture in a local area network (LAN) is that this would:

- ☐ stabilize network bandwidth requirements
- ☐ facilitate the updating of software versions
- ☐ ensure application availability when the server is down
- ☐ reduce the risk of a single point of failure

Licensed to Berend Post berend.post@it-university.nl

Question 1199

An internal audit has found that critical patches were not implemented within the timeline established by policy without a valid reason. Which of the following is the BEST course of action to address the audit findings?

- ☐ Monitor and notify IT staff of critical patches.
- ☐ Evaluate patch management training.
- ☐ Perform regular audits on the implementation of critical patches.
- ☐ Assess the patch management process.

Question 1200

Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?

- ☐ Intrusion detection systems
- ☐ Data mining techniques
- ☐ Firewalls
- ☐ Packet filtering routers

Question 1201

The GREATEST benefit of choosing a private cloud over a public cloud would be:

- ☐ server protection.
- ☐ online service availability.
- ☐ containment of customer data.
- ☐ collection of data forensics.

Question 1202

During a change control audit of a production system, an IS auditor finds that the change management process is not formally documented and that some migration procedures failed. What should the IS auditor do next?

- ☐ Recommend redesigning the change management process.
- ☐ Gain more assurance on the findings through root cause analysis.
- ☐ Recommend that program migration be stopped until the change process is documented.
- ☐ Document the finding and present it to management.

Licensed to Berend Post berend.post@it-university.nl

Question 1203

Which of the following type of network service maps Domain Names to network IP addresses or network IP addresses to Domain Names?

- ☐ DHCP
- ☐ DNS
- ☐ Directory Service
- ☐ Network Management

Question 1204

Which of the following is an implementation risk within the process of decision support systems?

- ☐ Management control
- ☐ Semistructured dimensions
- ☐ inability to specify purpose and usage patterns
- ☐ Changes in decision processes

Question 1205

Identify the correct sequence of Business Process Reengineering (BPR) application steps from the given choices below?

- ☐ Envision, Initiate, Diagnose, Redesign, Reconstruct and Evaluate
- ☐ Initiate, Envision, Diagnose, Redesign, Reconstruct and Evaluate
- ☐ Envision, Diagnose, Initiate, Redesign, Reconstruct and Evaluate
- ☐ Evaluate, Envision, Initiate, Diagnose, Redesign, Reconstruct

Question 1206

Machines that operate as a closed system can NEVER be eavesdropped.

- ☐ True
- ☐ False

Question 1207

During a vulnerability assessment, an IS auditor finds a high-risk vulnerability in a public-facing web server used to process online customer orders via credit card. The IS auditor should FIRST:

- ☐ notify management.
- ☐ redesign the customer order process.
- ☐ document the finding in the report.
- ☐ suspend credit card processing.

Licensed to Berend Post berend.post@it-university.nl

Question 1208

An information security manager is developing evidence preservation procedures for an incident response plan. Which of the following would be the BEST source of guidance for requirements associated with the procedures?

- ☐ IT management
- ☐ Executive management
- ☐ Legal counsel
- ☐ Data owners

Question 1209

Which of the following findings would be of MOST concern to an IS auditor performing a review of an end-user developed application that generates financial statements?

- ☐ The application is not sufficiently supported by the IT department
- ☐ There is not adequate training in the use of the application
- ☐ There is no adequate user license for the application
- ☐ There is no control to ensure accuracy of the processed data

Question 1210

When reviewing the effectiveness of data center operations, the IS auditor would FIRST establish that system performance:

- ☐ is monitored and reported against agreed service levels.
- ☐ reflects the expected usage levels established at implementation.
- ☐ meets the expected targets specified by the manufacturer.
- ☐ is within generally accepted reliability levels for that system.

Question 1211

Naming conventions for system resources are important for access control because they:

- ☐ ensure that resource names are not ambiguous.
- ☐ reduce the number of rules required to adequately protect resources.
- ☐ ensure that user access to resources is clearly and uniquely identified.
- ☐ ensure that internationally recognized names are used to protect resources.

Licensed to Berend Post berend.post@it-university.nl

Question 1212

The FIRSTstep in establishing an information security program is to:

- ☐ secure organizational commitment and support
- ☐ assess the organization's compliance with regulatory requirements
- ☐ determine the level of risk that is acceptable to senior management
- ☐ define policies and standards that mitigate the organization's risks

Question 1213

When providing a vendor with data containing personally identifiable information (PII) for offsite testing, the data should be:

- ☐ current
- ☐ encrypted.
- ☐ sanitized.
- ☐ backed up.

Question 1214

Which of the following is MOST important for an IS auditor to consider when evaluating a Software as a Service (SaaS) arrangement?

- ☐ Total cost of ownership
- ☐ Frequency of software updates
- ☐ Physical security
- ☐ Software availability

Question 1215

Which of the following would have the HIGHEST priority in a business continuity plan (BCP)?

- ☐ Resuming critical processes
- ☐ Recovering sensitive processes
- ☐ Restoring the site
- ☐ Relocating operations to an alternative site

Licensed to Berend Post berend.post@it-university.nl

Question 1216

The IS management of a multinational company is considering upgrading its existing virtual private network (VPN) to support voice-over IP (VoIP) communications via tunneling. Which of the following considerations should be PRIMARILY addressed?

- ☐ Reliability and quality of service (QoS)
- ☐ Means of authentication
- ☐ Privacy of voice transmissions
- ☐ Confidentiality of data transmissions

Question 1217

What is the best defense against Local DoS attacks?

- ☐ patch your systems.
- ☐ run a virus checker.
- ☐ run an anti-spy software.
- ☐ find this program and kill it.
- ☐ None of the choices.

Question 1218

Which of the following cryptographic systems is MOST appropriate for bulk data encryption and small devices such as smart cards?

- ☐ DES
- ☐ AES
- ☐ Triple DES
- ☐ RSA

Question 1219

Which of the following would BEST maintain the integrity of a firewall log?

- ☐ Granting access to log information only to administrators
- ☐ Capturing log events in the operating system layer
- ☐ Writing dual logs onto separate storage media
- ☐ Sending log information to a dedicated third-party log server

Licensed to Berend Post berend.post@it-university.nl

Question 1220

An IS auditor has obtained a large data set containing multiple fields and non-numeric data for analysis. Which of the following activities will MOST improve the quality of conclusions derived from the use of a data analytics tool for this audit?

- ☐ Data anonymization
- ☐ Data classification
- ☐ Data stratification
- ☐ Data preparation

Question 1221

In an environment where most IT services have been outsourced, continuity planning is BEST controlled by:

- ☐ outsourced service provider management.
- ☐ business management.
- ☐ continuity planning specialists.
- ☐ IT management.

Question 1222

In an organization that has a staff-rotation policy, the MOST appropriate access control model is:

- ☐ role based.
- ☐ discretionary.
- ☐ mandatory.
- ☐ lattice based.

Question 1223

To ensure the integrity of a recovered database, which of the following would be MOST useful?

- ☐ Before-and-after transaction images
- ☐ Database defragmentation tools
- ☐ A copy of the data dictionary
- ☐ Application transaction logs

Licensed to Berend Post berend.post@it-university.nl

Question 1224

Which of the following is the MOST important security consideration when using infrastructure as a Service (IaaS)?

- ☐ User access management
- ☐ Compliance with internal standards
- ☐ Segmentation among guests
- ☐ Backup and recovery strategy

Question 1225

Which of the following functions is MOST critical when initiating the removal of system access for terminated employees?

- ☐ Legal
- ☐ Help desk
- ☐ Human resources
- ☐ Information security

Question 1226

What is the PRIMARY advantage of prototyping as part of systems development?

- ☐ Maximizes user satisfaction
- ☐ Eliminates the need for internal controls
- ☐ Increases accuracy in reporting
- ☐ Reduces the need for compliance testing

Question 1227

An IS auditor reviewed the business case for a proposed investment to virtualize an organization's server infrastructure. Which of the following is MOST likely to be included among the benefits in the project proposal?

- ☐ Fewer operating system licenses
- ☐ Better efficiency of logical resources
- ☐ Reduced hardware footprint
- ☐ Less memory and storage space

Licensed to Berend Post berend.post@it-university.nl

Question 1228

An organization establishes an internal document collaboration site. To ensure data confidentiality of each project group, it is MOST important to:

- ☐ conduct a vulnerability assessment.
- ☐ enforce document life cycle management.
- ☐ prohibit remote access to the site.
- ☐ periodically recertify access rights.

Question 1229

Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

- ☐ Traffic analysis
- ☐ SYN flood
- ☐ Denial of service (DoS)
- ☐ Distributed denial of service (DoS)

Question 1230

Spreadsheets are used to calculate project cost estimates. Totals for each cost category are then keyed into the job-costing system. What is the BEST control to ensure that data are accurately entered into the system?

- ☐ Reasonableness checks for each cost type
- ☐ Validity checks, preventing entry of character data
- ☐ Display back of project detail after entry
- ☐ Reconciliation of total amounts by project

Question 1231

Which of the following would be MOST time and cost efficient when performing a control self-assessment (CSA) for an organization with a large number of widely dispersed employees?

- ☐ Top-down and bottom-up analysis
- ☐ Face-to-face interviews
- ☐ Survey questionnaire
- ☐ Facilitated workshops

Licensed to Berend Post berend.post@it-university.nl

Question 1232

The selection of security controls is PRIMARILY linked to:

- ☐ risk appetite of the organization.
- ☐ regulatory requirements.
- ☐ business impact assessment.
- ☐ best practices of similar organizations.

Question 1233

Of the following procedures for testing a disaster recovery plan (DRP), which should be used MOST frequently?

- ☐ Unannounced shutdown of the primary computing facility.
- ☐ Review of documented backup and recovery procedures
- ☐ Testing at a secondary site using offsite data backups
- ☐ Preplanned shutdown of the computing facility during an off-peak period

Question 1234

Which of the following is MOST critical to the success of an information security program?

- ☐ Integration of business and information security
- ☐ Alignment of information security with IT objectives
- ☐ Management's commitment to information security
- ☐ User accountability for information security

Question 1235

How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

- ☐ By implementing redundant systems and applications onsite
- ☐ By geographically dispersing resources
- ☐ By retaining onsite data backup in fireproof vaults
- ☐ By preparing BCP and DRP documents for commonly identified disasters

Licensed to Berend Post berend.post@it-university.nl

Question 1236

The human resources (HR) department has developed a system to allow employees to enroll in benefits via a web site on the corporate Intranet. Which of the following would protect the confidentiality of the data?

- ☐ SSL encryption
- ☐ Two-factor authentication
- ☐ Encrypted session cookies
- ☐ IP address verification

Question 1237

An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

- ☐ There are a number of external modems connected to the network.
- ☐ Users can install software on their desktops.
- ☐ Network monitoring is very limited.
- ☐ Many user IDs have identical passwords.

Question 1238

An IS auditor is told by IS management that the organization has recently reached the highest level of the software capability maturity model (CMM). The software quality process MOST recently added by the organization is:

- ☐ continuous improvement.
- ☐ quantitative quality goals.
- ☐ a documented process.
- ☐ a process tailored to specific projects.

Question 1239

On a daily basis, an in-house development team moves duplicate copies of production data containing personally identifiable information (PII) to the test environment. Which of the following is the BEST way to mitigate the privacy risk involved?

- ☐ Require data owners to sign off on production data.
- ☐ Encrypt the data file.
- ☐ Obtain customer opt-in acceptances.
- ☐ Sanitize the data in the test environment.

Licensed to Berend Post berend.post@it-university.nl

Question 1240

As an auditor it is very important to ensure confidentiality, integrity, authenticity and availability are implemented appropriately in an information system. Which of the following definitions incorrectly describes these parameters?

1. Authenticity – A third party must be able to verify that the content of a message has been sent by a specific entity and nobody else.

2. Non-repudiation – The origin or the receipt of a specific message must be verifiable by a third party. A person cannot deny having sent a message if the message is signed by the originator.

3. Accountability – The action of an entity must be uniquely traceable to different entities
4. Availability – The IT resource must be available on a timely basis to meet mission requirements or to avoid substantial losses.

- ☐ All of the options presented
- ☐ None of the options presented
- ☐ Options number 1 and 2
- ☐ Option number 3

Question 1241

You should know the difference between an exploit and a vulnerability. Which of the following refers to a weakness in the system?

- ☐ exploit
- ☐ vulnerability
- ☐ both

Question 1242

The waterfall life cycle model of software development is most appropriately used when:

- ☐ requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate.
- ☐ requirements are well understood and the project is subject to time pressures.
- ☐ the project intends to apply an object-oriented design and programming approach.
- ☐ the project will involve the use of new technology.

Licensed to Berend Post berend.post@it-university.nl

Question 1243

Which of the following refers to any program that invites the user to run it but conceals a harmful or malicious payload?

- ☐ virus
- ☐ worm
- ☐ trojan horse
- ☐ spyware
- ☐ rootkits
- ☐ None of the choices.

Question 1244

An IS auditor is performing a business continuity plan (BCP) audit and identifies that the plan has not been tested for five years. However, the plan was successfully activated during a recent extended power outage. Which of the following is the IS auditor's BEST course of action?

- ☐ Determine if lessons learned from the activation were incorporated into the plan.
- ☐ Determine if the business impact analysis (BIA) is still accurate.
- ☐ Determine if a follow-up BCP audit is required to identify future gaps.
- ☐ Determine if the annual BCP training program is in need of a review.

Question 1245

Which of the following is MOST important for the improvement of an organization's incident response processes?

- ☐ Post-event reviews by the incident response team
- ☐ Regular upgrades to incident management software
- ☐ Ongoing incident response training for users
- ☐ Periodic walk-through of incident response procedures

Question 1246

An IS auditor reviewing an organization's data file control procedures finds that transactions are applied to the most current files, while restart procedures use earlier versions. The IS auditor should recommend the implementation of:

- ☐ source documentation retention.
- ☐ data file security.
- ☐ version usage control.
- ☐ one-for-one checking.

Licensed to Berend Post berend.post@it-university.nl

Question 1247

Relatively speaking, firewalls operated at the physical level of the seven-layer OSI model are:

- ☐ almost always less efficient.
- ☐ almost always less effective.
- ☐ almost always less secure.
- ☐ almost always less costly to setup.
- ☐ None of the choices.

Question 1248

Which of the following is used to evaluate biometric access controls?

- ☐ FAR
- ☐ EER
- ☐ ERR
- ☐ FRR

Question 1249

An IS auditor has completed a review of an outsourcing agreement and has identified IT governance issues. Which of the following is the MOST effective and efficient way of communicating the issues at a meeting with senior management?

- ☐ Present a completed report and discuss the details.
- ☐ Provide a detailed report in advance and open the floor to questions.
- ☐ Present an overview highlighting the key findings.
- ☐ Provide a plan of action and milestones.

Question 1250

Which of the following would be an indicator of the effectiveness of a computer security incident response team?

- ☐ Financial impact per security incident
- ☐ Number of security vulnerabilities that were patched
- ☐ Percentage of business applications that are being protected
- ☐ Number of successful penetration tests

Licensed to Berend Post berend.post@it-university.nl

Question 1251

When reviewing the procedures for the disposal of computers, which of the following should be the GREATEST concern for the IS auditor?

- ☐ Hard disks are overwritten several times at the sector level, but are not reformatted before leaving the organization.
- ☐ All files and folders on hard disks are separately deleted, and the hard disks are formatted before leaving the organization.
- ☐ Hard disks are rendered unreadable by hole-punching through the platters at specific positions before leaving the organization.
- ☐ The transport of hard disks is escorted by internal security staff to a nearby metal recycling company, where the hard disks are registered and then shredded.

Question 1252

When consolidating several applications from two outdated servers onto one new server, which of the following is the GREATEST concern?

- ☐ Increased software licensing cost
- ☐ Maintenance requires more coordination
- ☐ Decreased utilization of capacity
- ☐ Increased network traffic

Question 1253

Which of the following is the PRIMARY reason social media has become a popular target for attack?

- ☐ The accessibility of social media from multiple locations
- ☐ The prevalence of strong perimeter protection
- ☐ The reduced effectiveness of access controls
- ☐ The element of trust created by social media

Question 1254

Which of the following is an example of a preventive control in an accounts payable system?

- ☐ The system only allows payments to vendors who are included in the system's master vendor list.
- ☐ Policies and procedures are clearly communicated to all members of the accounts payable department.
- ☐ The system produces daily payment summary reports that staff use to compare against invoice totals.
- ☐ Backups of the system and its data are performed on a nightly basis and tested periodically.

Licensed to Berend Post berend.post@it-university.nl

Question 1255

Which of the following is the BEST audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

- ☐ Review the parameter settings.
- ☐ Interview the firewall administrator.
- ☐ Review the actual procedures.
- ☐ Review the device's log file for recent attacks.

Question 1256

Which of the following is the PRIMARY benefit to an organization using an automated event monitoring solution?

- ☐ Enhanced forensic analysis
- ☐ Improved response time to incidents
- ☐ Improved network protection
- ☐ Reduced need for manual analysis

Question 1257

Which of the following procedures should an IS auditor complete FISRT when evaluating the adequacy of IT key performance indicators (KPIs)?

- ☐ Independently calculate the accuracy of the KPIs.
- ☐ Review KPIs that indicate poor IT performance.
- ☐ Validate the KPI thresholds.
- ☐ Determine whether the KPIs support IT objectives.

Question 1258

Two servers are deployed in a cluster to run a mission-critical application. To determine whether the system has been designed for optimal efficiency, the IS auditor should verify that:

- ☐ the security features in the operating system are all enabled
- ☐ the number of disks in the cluster meets minimum requirements
- ☐ the two servers are of exactly the same configuration
- ☐ load balancing between the servers has been implemented

Licensed to Berend Post berend.post@it-university.nl

Question 1259

An IS auditor is reviewing the performance outcomes of controls in an agile development project. Which of the following would provide the MOST relevant evidence for the auditor to consider?

- ☐ Progress report of outstanding work
- ☐ Product backlog
- ☐ Number of failed builds
- ☐ Composition of the scrum team

Question 1260

A legacy application is running on an operating system that is no longer supported by the vendor. If the organization continues to use the current application, which of the following should be the IS auditor's GREATEST concern?

- ☐ Potential exploitation of zero-day vulnerabilities in the system
- ☐ Inability to update the legacy application database
- ☐ Increased cost of maintaining the system
- ☐ Inability to use the operating system due to potential license issues

Question 1261

Sign-on procedures include the creation of a unique user ID and password. However, an IS auditor discovers that in many cases the username and password are the same. The BEST control to mitigate this risk is to:

- ☐ change the company's security policy.
- ☐ educate users about the risk of weak passwords.
- ☐ build in validations to prevent this during user creation and password change.
- ☐ require a periodic review of matching user ID and passwords for detection and correction.

Question 1262

During the planning stage of a compliance audit, an IS auditor discovers that a bank's inventory of compliance requirements does not include recent regulatory changes related to managing data risk. What should the auditor do FIRST?

- ☐ Discuss potential regulatory issues with the legal department.
- ☐ Ask management why the regulatory changes have not been included.
- ☐ Exclude recent regulatory changes from the audit scope.
- ☐ Report the missing regulatory updates to the chief information officer (CIO).

Licensed to Berend Post berend.post@it-university.nl

Question 1263

Which of the following is the MOST important for an IS auditor to do during an exit meeting with an auditee?

- ☐ Ensure that the facts presented in the report are correct.
- ☐ Specify implementation dates for the recommendations.
- ☐ Request input in determining corrective action.
- ☐ Communicate the recommendations to senior management.

Question 1264

The PRIMARY purpose of aligning information security with corporate governance objectives is to:

- ☐ identify an organization's tolerance for risk.
- ☐ re-align roles and responsibilities.
- ☐ build capabilities to improve security processes.
- ☐ consistently manage significant areas of risk.

Question 1265

Structured programming is BEST described as a technique that:

- ☐ provides knowledge of program functions to other programmers via peer reviews.
- ☐ reduces the maintenance time of programs by the use of small-scale program modules.
- ☐ makes the readable coding reflect as closely as possible the dynamic execution of the program.
- ☐ controls the coding and testing of the high-level functions of the program in the development process.

Question 1266

In a typical network architecture used for e-commerce, a load balancer is normally found between the:

- ☐ routers and the web servers.
- ☐ mail servers and the mail repositories.
- ☐ users and the external gateways.
- ☐ databases and the external gateways.

Licensed to Berend Post berend.post@it-university.nl

Question 1267

When transmitting a payment instruction, which of the following will help verify that the instruction was not duplicated?

- ☐ Use of a cryptographic hashing algorithm
- ☐ Enciphering the message digest
- ☐ Deciphering the message digest
- ☐ A sequence number and time stamp

Question 1268

During an IS audit of a data center, it was found that programmers are allowed to make emergency fixes to operational programs. Which of the following should be the IS auditor's PRIMARY recommendation?

- ☐ Bypass use ID procedures should be put in place to ensure that the changes are subject to after-the-event approval and testing
- ☐ The ability to undertake emergency fixes should be restricted to selected key personnel
- ☐ Programmers should be allowed to implement emergency fixes only after obtaining verbal agreement from the application owner
- ☐ Emergency program changes should be subject to program migration and testing procedures before they are applied to operational systems

Question 1269

Which of the following is the MOST important reason to document information security incidents that are reported across the organization?

- ☐ Prevent incident recurrence.
- ☐ Support business investments in security.
- ☐ Identify unmitigated risk.
- ☐ Evaluate the security posture of the organization.

Question 1270

An employee transfers from an organization's risk management department to become the lead IS auditor. While in the risk management department, the employee helped develop the key performance indicators (KPIs) now used by the organization. Which of the following would pose the GREATEST threat to the independence of this auditor?

- ☐ Evaluating the effectiveness of IT risk management processes
- ☐ Recommending controls to address the IT risks identified by KPIs
- ☐ Developing KPIs to measure the internal audit team
- ☐ Training the IT audit team on IT risk management processes

Licensed to Berend Post berend.post@it-university.nl

Question 1271

Which of the following is the BEST way to determine if IT is delivering value to the business?

- ☐ Distribute surveys to various end users of IT services.
- ☐ Interview key IT managers and service providers.
- ☐ Review IT service level agreement (SLA) metrics.
- ☐ Analyze downtime frequency and duration.

Question 1272

Following a recent acquisition, an information security manager has been requested the outstanding risk reported early in the acquisition process. Which of the following would be the manager's BESTcourse of action?

- ☐ Perform a vulnerability assessment of the acquired company's infrastructure.
- ☐ Re-evaluate the risk treatment plan for the outstanding risk.
- ☐ Re-assess the outstanding risk of the acquired company.
- ☐ Add the outstanding risk to the acquiring organization's risk registry

Question 1273

Active radio frequency ID (RFID) tags are subject to which of the following exposures?

- ☐ Session hijacking
- ☐ Eavesdropping
- ☐ Malicious code
- ☐ Phishing

Question 1274

When building a corporate-wide business continuity plan, it is discovered there are two separate lines of business systems that could be impacted by the same threat. Which of the following is the BEST method to determine the priority of systems recovery in the event of a disaster?

- ☐ Reviewing the business plans of each department
- ☐ Evaluating the cost associated with each system's outage
- ☐ Reviewing each system's key performance indicators (KPIs)
- ☐ Comparing the recovery point objectives (RPOs)

Licensed to Berend Post berend.post@it-university.nl

Question 1275

Which of the following is an environmental issue caused by electric storms or noisy electric equipment and may also cause computer system to hang or crash?

- ☐ Sag
- ☐ Blackout
- ☐ Brownout
- ☐ EMI

Question 1276

The BEST way to validate whether a malicious act has actually occurred in an application is to review:

- ☐ segregation of duties
- ☐ access controls
- ☐ activity logs
- ☐ change management logs

Question 1277

Business applications should be selected for disaster recovery testing on the basis of:

- ☐ the results of contingency desktop checks
- ☐ the number of failure points that are being tested
- ☐ recovery time objectives (RTOs)
- ☐ criticality to the enterprise

Question 1278

An IS auditor finds that an organization's data loss prevention (DLP) system is configured to use vendor default settings to identify violations. The auditor's MAIN concern should be that:

- ☐ violations may not be categorized according to the organization's risk profile.
- ☐ violation reports may not be retained according to the organization's risk profile.
- ☐ violation reports may not be reviewed in a timely manner.
- ☐ a significant number of false positive violations may be reported.

Question 1279

Which of the following should be the PRIMARY objective of the information security incident response process?

- ☐ Minimizing negative impact to critical operations
- ☐ Communicating with internal and external parties
- ☐ Classifying incidents
- ☐ Conducting incident triage

Licensed to Berend Post berend.post@it-university.nl

Question 1280

To provide protection for media backup stored at an offsite location, the storage site should be:

- ☐ located on a different floor of the building.
- ☐ easily accessible by everyone.
- ☐ clearly labeled for emergency access.
- ☐ protected from unauthorized access.

Question 1281

An offsite information processing facility with electrical wiring, air conditioning and flooring, but no computer or communications equipment, is a:

- ☐ cold site.
- ☐ warm site.
- ☐ dial-up site.
- ☐ duplicate processing facility.

Question 1282

A recent audit has identified that security controls required by the organization's policies have not been implemented for a particular application. What should the information security manager do NEXT to address this issue?

- ☐ Deny access to the application until the issue is resolved.
- ☐ Discuss the issue with data custodians to determine the reason for the exception.
- ☐ Report the issue to senior management and request funding to fix the issue.
- ☐ Discuss the issue with data owners to determine the reason for the exception.

Question 1283

Which of the following requires a consensus by key stakeholders on IT strategic goals and objectives?

- ☐ Balanced scorecards
- ☐ Benchmarking
- ☐ Maturity models
- ☐ Peer reviews

Question 1284

Which of the following concerns is BEST addressed by securing production source libraries?

- ☐ Production source and object libraries may not be synchronized.
- ☐ Unauthorized changes can be moved into production.
- ☐ Programs are not approved before production source libraries are updated.
- ☐ Changes are applied to the wrong version of production source libraries.

Licensed to Berend Post berend.post@it-university.nl

Question 1285

What is the first step in a business process re-engineering project?

- ☐ Identifying current business processes
- ☐ Forming a BPR steering committee
- ☐ Defining the scope of areas to be reviewed
- ☐ Reviewing the organizational strategic plan

Question 1286

Which of the following is not a good tactic to use against hackers?

- ☐ Enticement
- ☐ Entrapment

Question 1287

When are benchmarking partners identified within the benchmarking process?

- ☐ In the design stage
- ☐ In the testing stage
- ☐ In the research stage
- ☐ In the development stage

Question 1288

The IS auditor's PRIMARY role in control self-assessment (CSA) is to:

- ☐ evaluate the controls.
- ☐ facilitate the process.
- ☐ identify weaknesses.
- ☐ draw up an action plan.

Question 1289

The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

- ☐ Test data
- ☐ Generalized audit software
- ☐ Integrated test facility
- ☐ Embedded audit module

Licensed to Berend Post berend.post@it-university.nl

Question 1290

Outsourcing the development of business systems is MOST likely to result in the loss of:

- ☐ control over strategic direction.
- ☐ accountability for end products.
- ☐ in-house competencies.
- ☐ responsibility for IT security.

Question 1291

A poor choice of passwords and transmission over unprotected communications lines are examples of:

- ☐ vulnerabilities.
- ☐ threats.
- ☐ probabilities.
- ☐ impacts.

Question 1292

An audit of the quality management system (QMS) begins with an evaluation of the:

- ☐ organization's QMS policy
- ☐ sequence and interaction of QMS processes
- ☐ QMS processes and their application
- ☐ QMS document control procedures

Question 1293

A warehouse employee of a retail company has been able to conceal the theft of inventory items by entering adjustments of either damaged or lost stock items to the inventory system. Which control would have BEST prevented this type of fraud in a retail environment?

- ☐ An edit check for the validity of the inventory transaction
- ☐ Separate authorization for input of transactions
- ☐ Unscheduled audits of lost stock lines
- ☐ Statistical sampling of adjustment transactions

Licensed to Berend Post berend.post@it-university.nl

Question 1294

An IS auditor begins an assignment and identifies audit components for which the auditor is not qualified to assess. Which of the following is the BEST course of action?

- ☐ Notify audit management for a decision on how to proceed.
- ☐ Complete the audit and give full disclosure in the final audit report.
- ☐ Complete the work assignment to the best of the auditor's ability.
- ☐ Exclude the related tests from the audit plan and continue the assignment.

Question 1295

Which of the following statement correctly describes difference between packet filtering firewall and stateful inspection firewall?

- ☐ Packet filtering firewall do not maintain client session whereas Stateful firewall maintains client session.
- ☐ Packet filtering firewall and Stateful firewall both maintain session of client.
- ☐ Packet filtering firewall is a second generation firewall whereas Stateful is a first generation of firewall.
- ☐ Packet filtering firewall and Stateful firewall do not maintain any session of client.

Question 1296

What is used as a control to detect loss, corruption, or duplication of data?

- ☐ Redundancy check
- ☐ Reasonableness check
- ☐ Hash totals
- ☐ Accuracy check

Question 1297

Why is a clause for requiring source code escrow in an application vendor agreement important?

- ☐ To segregate systems development and live environments
- ☐ To protect the organization from copyright disputes
- ☐ To ensure that sufficient code is available when needed
- ☐ To ensure that the source code remains available even if the application vendor goes out of business

Licensed to Berend Post berend.post@it-university.nl

Question 1298

During the development of an application, the quality assurance testing and user acceptance testing were combined. The MAJOR concern for an IS auditor reviewing the project is that there will be:

- ☐ increased maintenance.
- ☐ improper documentation of testing.
- ☐ inadequate functional testing.
- ☐ delays in problem resolution.

Question 1299

The goal of an information system is to achieve integrity, authenticity and non-repudiation of information's sent across the network. Which of the following statement correctly describe the steps to address all three?

- ☐ Encrypt the message digest using symmetric key and then send the encrypted digest to receiver along with original message.
- ☐ Encrypt the message digest using receiver's public key and then send the encrypted digest to receiver along with original message. The receiver can decrypt the message digest using his own private key.
- ☐ Encrypt the message digest using sender's public key and then send the encrypted digest to the receiver along with original message. The receiver can decrypt using his own private key.
- ☐ Encrypt message digest using sender's private key and then send the encrypted digest to the receiver along with original message. Receiver can decrypt the same using sender's public key.

Question 1300

Which of the following measures can protect systems files and data, respectively?

- ☐ User account access controls and cryptography
- ☐ User account access controls and firewall
- ☐ User account access controls and IPS
- ☐ IDS and cryptography
- ☐ Firewall and cryptography
- ☐ None of the choices.

Question 1301

Which of the following is the GREATEST risk posed by denial-of-service attacks?

- ☐ Confidential information leakage
- ☐ Loss of integrity and corruption of databases
- ☐ Loss of reputation and business
- ☐ Unauthorized access to the systems

Licensed to Berend Post berend.post@it-university.nl

Question 1302

An IS auditor who was involved in designing an organization's business continuity plan(BCP) has been assigned to audit the plan. The IS auditor should:

- ☐ decline the assignment.
- ☐ inform management of the possible conflict of interest after completing the audit assignment.
- ☐ inform the business continuity planning (BCP) team of the possible conflict of interest prior to beginning the assignment.
- ☐ communicate the possibility of conflict of interest to management prior to starting the assignment.

Question 1303

An organization's IS audit charter should specify the:

- ☐ short- and long-term plans for IS audit engagements
- ☐ objectives and scope of IS audit engagements.
- ☐ detailed training plan for the IS audit staff.
- ☐ role of the IS audit function.

Question 1304

Which of the following control make sure that input data comply with predefined criteria maintained in computerized table of possible values?

- ☐ Range Check
- ☐ Table lookups
- ☐ Existence check
- ☐ Reasonableness check

Question 1305

For application acquisitions with significant impacts, participation of your IS audit team should be encouraged:

- ☐ early in the due diligence stage.
- ☐ at the testing stage.
- ☐ at the final approval stage.
- ☐ at the budget preparation stage.
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 1306

Information security awareness programs are MOST effective when they are:

- ☐ customized for each target audience
- ☐ conducted at employee orientation
- ☐ reinforced by computer-based training
- ☐ sponsored by senior management

Question 1307

To verify that the correct version of a data file was used for a production run, an IS auditor should review:

- ☐ operator problem reports.
- ☐ operator work schedules.
- ☐ system logs.
- ☐ output distribution reports.

Question 1308

Which of the following BEST enables timely detection of changes in the IT environment to support informed decision making by management?

- ☐ Continuous monitoring
- ☐ Sampling checks on high-risk areas
- ☐ Change management reports
- ☐ Established key risk indicators (KRIs)

Question 1309

When reviewing an organization's logical access security, which of the following should be of MOST concern to an IS auditor?

- ☐ Passwords are not shared.
- ☐ Password files are not encrypted.
- ☐ Redundant logon IDs are deleted.
- ☐ The allocation of logon IDs is controlled.

Licensed to Berend Post berend.post@it-university.nl

Question 1310

Which of the following cryptography is based on practical application of the characteristics of the smallest “grains” of light, the photon, the physical laws governing their generation and propagation and detection?

- ☐ Quantum Cryptography
- ☐ Elliptical Curve Cryptography (ECC)
- ☐ Symmetric Key Cryptography
- ☐ Asymmetric Key Cryptography

Question 1311

The MAIN purpose for periodically testing offsite facilities is to:

- ☐ protect the integrity of the data in the database.
- ☐ eliminate the need to develop detailed contingency plans.
- ☐ ensure the continued compatibility of the contingency facilities.
- ☐ ensure that program and system documentation remains current.

Question 1312

The information security policy that states 'each individual must have their badge read at every controlled door' addresses which of the following attack methods?

- ☐ Piggybacking
- ☐ Shoulder surfing
- ☐ Dumpster diving
- ☐ Impersonation

Question 1313

Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

- ☐ meets or exceeds industry security standards.
- ☐ agrees to be subject to external security reviews.
- ☐ has a good market reputation for service and experience.
- ☐ complies with security policies of the organization.

Licensed to Berend Post berend.post@it-university.nl

Question 1314

A live test of a mutual agreement for IT system recovery has been carried out, including a four- hour test of intensive usage by the business units. The test has been successful, but gives only partial assurance that the:

- ☐ system and the IT operations team can sustain operations in the emergency environment.
- ☐ resources and the environment could sustain the transaction load.
- ☐ connectivity to the applications at the remote site meets response time requirements.
- ☐ workflow of actual business operations can use the emergency system in case of a disaster.

Question 1315

Which of the following BEST ensures that effective change management is in place in an IS environment?

- ☐ User authorization procedures for application access are well established.
- ☐ User-prepared detailed test criteria for acceptance testing of the software.
- ☐ Adequate testing was carried out by the development team.
- ☐ Access to production source and object programs is well controlled.

Question 1316

An IS auditor concludes that a local area network's (LAN's) access security is satisfactory. In reviewing the work, the audit manager should:

- ☐ re-perform some steps of the audit to verify the quality of the work.
- ☐ verify that the elements of an agreed-upon audit plan have been addressed.
- ☐ verify user management's agreement with the findings.
- ☐ assess whether the auditor had the appropriate skills to perform the work.

Question 1317

The PRIMARY objective of value delivery in reference to IT governance is to:

- ☐ increase efficiency
- ☐ promote best practices
- ☐ optimize investments
- ☐ ensure compliance

Licensed to Berend Post berend.post@it-university.nl

Question 1318

A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:

- ☐ payroll reports should be compared to input forms.
- ☐ gross payroll should be recalculated manually.
- ☐ checks (cheques) should be compared to input forms.
- ☐ checks (cheques) should be reconciled with output reports.

Question 1319

Before a failover test of a critical business application is performed, it is MOST important for the information security manager to:

- ☐ obtain a signed risk acceptation from the recovery team
- ☐ obtain senior management's approval
- ☐ inform the users that the test is taking place
- ☐ verify that the information assets have been classified properly

Question 1320

Hamid needs to shift users from using the application from the existing (Old) system to the replacing (new) system. His manager Lily has suggested he uses an approach in which the newer system is changed over from the older system on a cutoff date and time and the older system is discontinued once the changeover to the new system takes place. Which of the following changeover approach is suggested by Lily?

- ☐ Parallel changeover
- ☐ Phased changeover
- ☐ Abrupt changeover
- ☐ Pilot changeover

Question 1321

Which of the following should be of MOST concern to an IS auditor reviewing the BCP?

- ☐ The disaster levels are based on scopes of damaged functions, but not on duration.
- ☐ The difference between low-level disaster and software incidents is not clear.
- ☐ The overall BCP is documented, but detailed recovery steps are not specified.
- ☐ The responsibility for declaring a disaster is not identified.

Licensed to Berend Post berend.post@it-university.nl

Question 1322

Which of the following BEST indicates a need to review an organization's information security policy?

- ☐ Completion of annual IT risk assessment
- ☐ Increasing complexity of business transactions
- ☐ Increasing exceptions approved by management
- ☐ High number of low-risk findings in the audit report

Question 1323

Business units are concerned about the performance of a newly implemented system. Which of the following should an IS auditor recommend?

- ☐ Develop a baseline and monitor system usage.
- ☐ Define alternate processing procedures.
- ☐ Prepare the maintenance manual.
- ☐ implement the changes users have suggested.

Question 1324

During a review of a business continuity plan, an IS auditor noticed that the point at which a situation is declared to be a crisis has not been defined. The MAJOR risk associated with this is that:

- ☐ assessment of the situation may be delayed.
- ☐ execution of the disaster recovery plan could be impacted.
- ☐ notification of the teams might not occur.
- ☐ potential crisis recognition might be ineffective.

Question 1325

Which of the following will identify a deviation in the information security management process from generally accepted standards of good practices?

- ☐ Gap analysis
- ☐ Risk assessment
- ☐ Business impact analysis (BIA)
- ☐ Penetration testing

Question 1326

Inadequate programming and coding practices introduce the risk of:

- ☐ phishing.
- ☐ buffer overflow exploitation.
- ☐ SYN flood.
- ☐ brute force attacks.

Licensed to Berend Post berend.post@it-university.nl

Question 1327

Which of the following would be MOST effective when justifying the cost of adding security controls to an existing web application?

- ☐ Vulnerability assessment results
- ☐ Application security policy
- ☐ A business case
- ☐ Internal audit reports

Question 1328

Which of the following network components is PRIMARILY set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

- ☐ Firewalls
- ☐ Routers
- ☐ Layer 2 switches
- ☐ VLANs

Question 1329

An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:

- ☐ a backup server be available to run ETCS operations with up-to-date data.
- ☐ a backup server be loaded with all the relevant software and data.
- ☐ the systems staff of the organization be trained to handle any event.
- ☐ source code of the ETCS application be placed in escrow.

Question 1330

Which of the following sampling methods is MOST useful when testing for compliance?

- ☐ Attribute sampling
- ☐ Variable sampling
- ☐ Stratified mean per unit
- ☐ Difference estimation

Licensed to Berend Post berend.post@it-university.nl

Question 1331

Which of the following BEST facilitates compliance with requirements mandating the security of confidential data?

- ☐ Classification of data
- ☐ Security awareness training
- ☐ Encryption of external data transmissions
- ☐ Standardized escalation protocols for breaches

Question 1332

An IS auditor is conducting a review of a healthcare organization's IT policies for handling medical records. Which of the following is MOST important to verify?

- ☐ A documented policy approval process is in place
- ☐ Policy writing standards are consistent
- ☐ The policies comply with regulatory requirements
- ☐ IT personnel receive ongoing policy training

Question 1333

The difference between a vulnerability assessment and a penetration test is that a vulnerability assessment:

- ☐ searches and checks the infrastructure to detect vulnerabilities, whereas penetration testing intends to exploit the vulnerabilities to probe the damage that could result from the vulnerabilities.
- ☐ and penetration tests are different names for the same activity.
- ☐ is executed by automated tools, whereas penetration testing is a totally manual process.
- ☐ is executed by commercial tools, whereas penetration testing is executed by public processes.

Question 1334

"Nowadays, computer security comprises mainly "preventive"" measures."

- ☐ True
- ☐ True only for trusted networks
- ☐ True only for untrusted networks
- ☐ False
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 1335

Invoking a business continuity plan (BCP) is demonstrating which type of control?

- ☐ Corrective
- ☐ Preventive
- ☐ Detective
- ☐ Directive

Question 1336

From a control perspective, the PRIMARY objective of classifying information assets is to:

- ☐ establish guidelines for the level of access controls that should be assigned.
- ☐ ensure access controls are assigned to all information assets.
- ☐ assist management and auditors in risk assessment.
- ☐ identify which assets need to be insured against losses.

Question 1337

Which of the following should be the MOST important consideration when establishing data classification standards?

- ☐ An education campaign is established upon rollout.
- ☐ Reporting metrics are established.
- ☐ Management supports the newly developed standards.
- ☐ The standards comply with relevant regulations.

Question 1338

The ultimate purpose of IT governance is to:

- ☐ encourage optimal use of IT.
- ☐ reduce IT costs.
- ☐ decentralize IT resources across the organization.
- ☐ centralize control of IT.

Question 1339

At the completion of a system development project, a post project review should include which of the following?

- ☐ Assessing risks that may lead to downtime after the production release
- ☐ Identifying lessons learned that may be applicable to future projects
- ☐ Verifying the controls in the delivered system are working
- ☐ Ensuring that test data are deleted

Licensed to Berend Post berend.post@it-university.nl

Question 1340

Which of the following could lead to an unintentional loss of confidentiality?

- ☐ Lack of employee awareness of a company's information security policy
- ☐ Failure to comply with a company's information security policy
- ☐ A momentary lapse of reason
- ☐ Lack of security policy enforcement procedures

Question 1341

During a review of the IT strategic plan, an IS auditor finds several IT initiatives focused on delivering new systems and technology are not aligned with the organization's strategy. Witch of the following would be the IS auditor's BEST recommendation?

- ☐ Reassess the return on investment for the IT initiatives
- ☐ Modify IT initiatives that do not map to business strategies
- ☐ Utilize a balanced scorecard to align IT initiatives to business strategies
- ☐ Reassess IT initiatives that do not map business strategies

Question 1342

What is the MOST effective way to ensure information security incidents will be managed effectively and in a timely manner?

- ☐ Obtain senior management commitment.
- ☐ Test incident response procedures regularly.
- ☐ Communicate incident response procedures to staff.
- ☐ Establish and measure key performance indicators (KPIs).

Question 1343

An organization has an integrated development environment (IDE) on which the program libraries reside on the server, but modification/development and testing are done from PC workstations. Which of the following would be a strength of an IDE?

- ☐ Controls the proliferation of multiple versions of programs
- ☐ Expands the programming resources and aids available
- ☐ Increases program and processing integrity
- ☐ Prevents valid changes from being overwritten by other changes

Licensed to Berend Post berend.post@it-university.nl

Question 1344

The effectiveness of an information security governance framework will BEST be enhanced if:

- ☐ consultants review the information security governance framework
- ☐ a culture of legal and regulatory compliance is promoted by management
- ☐ IS auditors are empowered to evaluate governance activities
- ☐ risk management is built into operational and strategic activities

Question 1345

Which of the following should the IS auditor do FIRST to ensure data transfer integrity for Internet of Things (IoT) devices?

- ☐ Verify access control lists to the database where collected data is stored.
- ☐ Confirm that acceptable limits of data bandwidth are defined for each device.
- ☐ Ensure that message queue telemetry transport (MQTT) is used.
- ☐ Determine how devices are connected to the local network.

Question 1346

A validated patch to address a new vulnerability that may affect a mission-critical server has been released. What should be done immediately?

- ☐ Add mitigating controls.
- ☐ Check the server's security and install the patch.
- ☐ Conduct an impact analysis.
- ☐ Take the server off-line and install the patch.

Question 1347

Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the _____. (fill-in-the-blank)

- ☐ Security administrator
- ☐ Systems auditor
- ☐ Board of directors
- ☐ Financial auditor

Licensed to Berend Post berend.post@it-university.nl

Question 1348

In a security server audit, focus should be placed on (Choose two.):

- ☐ proper segregation of duties
- ☐ adequate user training
- ☐ continuous and accurate audit trail
- ☐ proper application licensing
- ☐ system stability
- ☐ performance and controls of the system
- ☐ None of the choices.

Question 1349

Which of the following comparisons are used for identification and authentication in a biometric system?

- ☐ One-to-many for identification and authentication
- ☐ One-to-one for identification and authentication
- ☐ One-to-many for identification and one-to-one for authentication
- ☐ One-to-one for identification and one-to-many for authentication

Question 1350

Which of the following is an advantage of an integrated test facility (ITF)?

- ☐ It uses actual master files or dummies and the IS auditor does not have to review the source of the transaction.
- ☐ Periodic testing does not require separate test processes.
- ☐ It validates application systems and tests the ongoing operation of the system.
- ☐ The need to prepare test data is eliminated.

Question 1351

Which of the following audit risk is related to material errors or misstatements that have occurred that will not be detected by an IS auditor?

- ☐ Inherent Risk
- ☐ Control Risk
- ☐ Detection Risk
- ☐ Overall Audit Risk

Licensed to Berend Post berend.post@it-university.nl

Question 1352

In an online banking application, which of the following would BEST protect against identity theft?

- ☐ Encryption of personal password
- ☐ Restricting the user to a specific terminal
- ☐ Two-factor authentication
- ☐ Periodic review of access logs

Question 1353

Which of the following risk handling technique involves the practice of being proactive so that the risk in question is not realized?

- ☐ Risk Mitigation
- ☐ Risk Acceptance
- ☐ Risk Avoidance
- ☐ Risk transfer

Question 1354

Before implementing an IT balanced scorecard, an organization must:

- ☐ deliver effective and efficient services.
- ☐ define key performance indicators.
- ☐ provide business value to IT projects.
- ☐ control IT expenses.

Question 1355

An auditor notes the administrator user ID is shared among three financial managers to perform month-end updates. Which of the following is the BEST recommendation to ensure the administrator ID in the financial system is controlled effectively?

- ☐ Implement use of individual software tokens
- ☐ Conduct employee awareness training
- ☐ Institute user ID logging and monitoring
- ☐ Ensure data in the financial systems has been classified

Licensed to Berend Post berend.post@it-university.nl

Question 1356

A company has located its computer center on a moderate earthquake fault. Which of the following is the MOST important consideration in establishing a contingency plan and an alternate processing site?

- ☐ The alternative site does not reside on the same fault no matter how far the distance apart.
- ☐ The contingency plan for high priority applications does not involve a shared cold site.
- ☐ The alternative site is a hot site with equipment ready to resume processing immediately.
- ☐ The contingency plan provides for backup tapes to be taken to the alternative site.

Question 1357

Who provides the funding to the project and works closely with the project manager to define critical success factor (CSF)?

- ☐ Project Sponsor
- ☐ Security Officer
- ☐ User Management
- ☐ Senior Management

Question 1358

An IS auditor reviewing wireless network security determines that the Dynamic Host Configuration Protocol is disabled at all wireless access points. This practice:

- ☐ reduces the risk of unauthorized access to the network.
- ☐ is not suitable for small networks.
- ☐ automatically provides an IP address to anyone.
- ☐ increases the risks associated with Wireless Encryption Protocol (WEP).

Question 1359

To preserve chain of custody following an internal server compromise, which of the following should be the FIRST step?

- ☐ Take a system image including memory dump
- ☐ Safely shut down the server
- ☐ Replicate the attack using the remaining evidence
- ☐ Trace the attacking route

Licensed to Berend Post berend.post@it-university.nl

Question 1360

Which of the following would BEST indicate the effectiveness of a security awareness training program?

- ☐ Increased number of employees completing training
- ☐ Employee satisfaction with training
- ☐ Reduced unintentional violations
- ☐ Results of third-party social engineering tests.

Question 1361

Which of the following ensures a sender's authenticity and an e-mail's confidentiality?

- ☐ Encrypting the hash of the message with the sender's private key and thereafter encrypting the hash of the message with the receiver's public key
- ☐ The sender digitally signing the message and thereafter encrypting the hash of the message with the sender's private key
- ☐ Encrypting the hash of the message with the sender's private key and thereafter encrypting the message with the receiver's public key
- ☐ Encrypting the message with the sender's private key and encrypting the message hash with the receiver's public key.

Question 1362

Which of the following attacks could capture network user passwords?

- ☐ Data diddling
- ☐ Sniffing
- ☐ IP Spoofing
- ☐ Surfing

Question 1363

Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

- ☐ Cold site
- ☐ Alternate site
- ☐ Hot site
- ☐ Warm site

Licensed to Berend Post berend.post@it-university.nl

Question 1364

When using a digital signature, the message digest is computed:

- ☐ only by the sender.
- ☐ only by the receiver.
- ☐ by both the sender and the receiver.
- ☐ by the certificate authority (CA).

Question 1365

To effectively classify data, which of the following MUST be determined?

- ☐ Data controls
- ☐ Data ownership
- ☐ Data users
- ☐ Data volume

Question 1366

A malicious code that changes itself with each file it infects is called a:

- ☐ logic bomb.
- ☐ stealth virus.
- ☐ trojan horse.
- ☐ polymorphic virus.

Question 1367

Which of the following would provide the BEST justification for a new information security investment?

- ☐ Defined key performance indicators (KPIs)
- ☐ Projected reduction in risk
- ☐ Results of a comprehensive threat analysis
- ☐ Senior management involvement in project prioritization

Question 1368

Which of the following PBX feature provides the possibility to break into a busy line to inform another user of an important message?

- ☐ Account Codes
- ☐ Access Codes
- ☐ Override
- ☐ Tenanting

Licensed to Berend Post berend.post@it-university.nl

Question 1369

Which of the following online auditing techniques is most effective for the early detection of errors or irregularities?

- ☐ Embedded audit module
- ☐ Integrated test facility
- ☐ Snapshots
- ☐ Audit hooks

Question 1370

In-house personnel performing IS audits should possess which of the following knowledge and/or skills (Choose two.):

- ☐ information systems knowledge commensurate with the scope of the IT environment in question
- ☐ sufficient analytical skills to determine root cause of deficiencies in question
- ☐ sufficient knowledge on secure system coding
- ☐ sufficient knowledge on secure platform development
- ☐ information systems knowledge commensurate outside of the scope of the IT environment in question

Question 1371

Which of the following should be established FIRST when initiating a control self-assessment program in a small organization?

- ☐ Control baselines
- ☐ Client questionnaires
- ☐ External consultants
- ☐ Facilitated workshops

Question 1372

During a review of an organization's network threat response process, the IS auditor noticed that the majority of alerts were closed without resolution. Management responded that those alerts were unworkable due to lack of actionable intelligence, and therefore the support team is allowed to close them. What is the BEST way for the auditor to address this situation?

- ☐ Further review closed unactioned alerts to identify mishandling of threats.
- ☐ Omit the finding from the report as this practice is in compliance with the current policy.
- ☐ Recommend that management enhance the policy and improve threat awareness training.
- ☐ Reopen unactioned alerts and report to the audit committee.

Licensed to Berend Post berend.post@it-university.nl

Question 1373

From a risk management point of view, the BEST approach when implementing a large and complex IT infrastructure is:

- ☐ a big bang deployment after proof of concept.
- ☐ prototyping and a one-phase deployment.
- ☐ a deployment plan based on sequenced phases.
- ☐ to simulate the new infrastructure before deployment.

Question 1374

Which of the following ensures the availability of transactions in the event of a disaster?

- ☐ Send tapes hourly containing transactions offsite,
- ☐ Send tapes daily containing transactions offsite.
- ☐ Capture transactions to multiple storage devices.
- ☐ Transmit transactions offsite in real time.

Question 1375

Over the last year, an information security manager has performed risk assessments on multiple third-party vendors. Which of the following criteria would be MOST helpful in determining the associated level of risk applied to each vendor?

- ☐ Compensating controls in place to protect information security
- ☐ Corresponding breaches associated with each vendor
- ☐ Criticality of the service to the organization
- ☐ Compliance requirements associated with the regulation

Question 1376

When conducting a post-incident review, the GREATEST benefit of collecting mean time to resolution (MTTR) data is the ability to:

- ☐ reduce the costs of future preventive controls
- ☐ provide metrics for reporting to senior management
- ☐ verify compliance with the service level agreement (SLA)
- ☐ learn of potential areas of improvement

Licensed to Berend Post berend.post@it-university.nl

Question 1377

In which of the following WAN message transmission technique does two network nodes establish a dedicated communications channel through the network before the nodes may communicate?

- ☐ Message Switching
- ☐ Packet switching
- ☐ Circuit switching
- ☐ Virtual Circuits

Question 1378

A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

- ☐ dials back to the user machine based on the user id and password using a telephone number from its database.
- ☐ dials back to the user machine based on the user id and password using a telephone number provided by the user during this connection.
- ☐ waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using its database.
- ☐ waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using the sender's database.

Question 1379

Which of the following is a technique that could be used to capture network user passwords?

- ☐ Encryption
- ☐ Sniffing
- ☐ Spoofing
- ☐ Data destruction

Question 1380

A benefit of open system architecture is that it:

- ☐ facilitates interoperability.
- ☐ facilitates the integration of proprietary components.
- ☐ will be a basis for volume discounts from equipment vendors.
- ☐ allows for the achievement of more economies of scale for equipment.

Licensed to Berend Post berend.post@it-university.nl

Question 1381

An organization has begun using social media to communicate with current and potential clients. Which of the following should be of PRIMARY concern to the auditor?

- ☐ Using a third-party provider to host and manage content
- ☐ Lack of guidance on appropriate social media usage and monitoring
- ☐ Negative posts by customers affecting the organization's image
- ☐ Reduced productivity of stuff using social media

Question 1382

Which of the following should be an information security manager's MOST important consideration when conducting a physical security review of a potential outsourced data center?

- ☐ Environmental factors of the surrounding location
- ☐ Proximity to law enforcement
- ☐ Availability of network circuit connections
- ☐ Distance of the data center from the corporate office

Question 1383

Which of the following layer of an OSI model controls dialog between computers?

- ☐ Application layer
- ☐ Presentation layer
- ☐ Session layer
- ☐ Transport layer

Question 1384

Which of the following is the MOST important privacy consideration for an organization that uses a cloud service provider to process customer data?

- ☐ Data privacy must be monitored in accordance with industry standards and best practices.
- ☐ All customer data transferred to the service provider must be reported to the regulatory authority.
- ☐ No personal information may be transferred to the service provider without the consent of the customer.
- ☐ Data privacy must be managed in accordance with the regulations applicable to the organization.

Licensed to Berend Post berend.post@it-university.nl

Question 1385

Utilizing external resources for highly technical information security tasks allows an information security manager to:

- ☐ transfer business risk.
- ☐ distribute technology risk.
- ☐ outsource responsibility.
- ☐ leverage limited resources.

Question 1386

An organization's business continuity plan (BCP) should be:

- ☐ updated based on changes to personnel and environments.
- ☐ tested whenever new applications are implemented.
- ☐ tested after successful intrusions into the organization's hot site.
- ☐ updated only after independent audit review by a third party.

Question 1387

Which of the following control checks would utilize data analytics?

- ☐ Evaluating configuration settings for the credit card application system
- ☐ Reviewing credit card applications submitted in the past month for blank data fields
- ☐ Attempting to submit credit card applications with blank data fields
- ☐ Reviewing the business requirements document for the credit card application system

Question 1388

An IS auditor has completed an audit on the organization's IT strategic planning process. Which of the following findings should be given the HIGHEST priority?

- ☐ The IT strategic plan was completed prior to the formulation of the business strategic plan
- ☐ Assumptions in the IT strategic plan have not been communicated to business stakeholders
- ☐ The IT strategic plan was formulated based on the current IT capabilities
- ☐ The IT strategic plan does not include resource requirements for implementation

Licensed to Berend Post berend.post@it-university.nl

Question 1389

Which of the following is the MOST reliable sender authentication method?

- ☐ Digital signatures
- ☐ Asymmetric cryptography
- ☐ Digital certificates
- ☐ Message authentication code

Question 1390

Business Continuity Planning (BCP) is not defined as a preparation that facilitates:

- ☐ the rapid recovery of mission-critical business operations
- ☐ the continuation of critical business functions
- ☐ the monitoring of threat activity for adjustment of technical controls
- ☐ the reduction of the impact of a disaster

Question 1391

Which of the following typically consists of a computer, some real looking data and/or a network site that appears to be part of a production network but which is in fact isolated and well prepared?

- ☐ honeypot
- ☐ superpot
- ☐ IDS
- ☐ IPS
- ☐ firewall
- ☐ None of the choices.

Question 1392

Which of the following control provides an alternative measure of control?

- ☐ Deterrent
- ☐ Preventive
- ☐ Detective
- ☐ Compensating

Licensed to Berend Post berend.post@it-university.nl

Question 1393

An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

- ☐ Personally delete all copies of the unauthorized software.
- ☐ Inform the auditee of the unauthorized software, and follow up to confirm deletion.
- ☐ Report the use of the unauthorized software and the need to prevent recurrence to auditee management.
- ☐ Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.

Question 1394

Which of the following analytical methods would be MOST useful when trying to identify groups with similar behavior or characteristics in a large population?

- ☐ Classification
- ☐ Correlation analysis
- ☐ Deviation detection
- ☐ Clustering

Question 1395

Several remote users have been unable to communicate with a secured network news transfer protocol (NNTP) server. Of the following, the MOST likely cause is:

- ☐ the use of a password cracker
- ☐ a hacker impersonating the server
- ☐ a hacker using a sniffer
- ☐ a replay attack by an eavesdropper

Question 1396

Which of the following type of network service is used by network computer to obtain an IP addresses and other parameters such as default gateway, subnet mask?

- ☐ DHCP
- ☐ DNS
- ☐ Directory Service
- ☐ Network Management

Licensed to Berend Post berend.post@it-university.nl

Question 1397

Which of the following BEST ensures that only authorized software is moved into a production environment?

- ☐ Restricting read/write access to production code to computer programmers only
- ☐ Assigning programming managers to transfer tested programs to production
- ☐ A librarian compiling source code into production after independent testing
- ☐ Requiring programming staff to move tested code into production

Question 1398

ALL computer programming languages are vulnerable to command injection attack.

- ☐ True
- ☐ False

Question 1399

Test and development environments should be separated. True or false?

- ☐ True
- ☐ False

Question 1400

An IS auditor issues an audit report pointing out the lack of firewall protection features at the perimeter network gateway and recommends a vendor product to address this vulnerability. The IS auditor has failed to exercise:

- ☐ professional independence
- ☐ organizational independence.
- ☐ technical competence.
- ☐ professional competence.

Question 1401

Which of the following presents the GREATEST concern when implementing data flow across borders?

- ☐ Software piracy laws
- ☐ National privacy laws
- ☐ Political unrest
- ☐ Equipment incompatibilities

Licensed to Berend Post berend.post@it-university.nl

Question 1402

Which of the following is the BEST indicator of an effective employee information security program?

- ☐ Increased management support for security
- ☐ More efficient and effective incident handling
- ☐ Increased detection and reporting of incidents
- ☐ Reduced operational cost of security

Question 1403

Which of the following is MOST effective in the strategic alignment of security initiatives?

- ☐ A security steering committee is set up within the IT department.
- ☐ Key information security policies are updated on a regular basis.
- ☐ Business leaders participate in information security decision making.
- ☐ Policies are created with input from business unit managers.

Question 1404

An internal review reveals an out-of-support human resources system. Which of the following is MOST important to determine when evaluating the associated risk?

- ☐ Frequency of outages associated with the out-of-support system
- ☐ The number of people accessing the out-of-support system
- ☐ Exposure of the out-of-support system outside of the network
- ☐ Timeline to replace the out-of-support system

Question 1405

The PRIMARY purpose of a business impact analysis (BIA) is to:

- ☐ provide a plan for resuming operations after a disaster.
- ☐ identify the events that could impact the continuity of an organization's operations.
- ☐ publicize the commitment of the organization to physical and logical security.
- ☐ provide the framework for an effective disaster recovery plan.

Question 1406

Which of the following is the GREATEST advantage of application penetration testing over vulnerability scanning?

- ☐ Penetration testing does not require a special skill set to be executed.
- ☐ Penetration testing provides a more accurate picture of gaps in application controls.
- ☐ Penetration testing can be conducted in a relatively short time period.
- ☐ Penetration testing creates relatively smaller risks to application availability and integrity.

Licensed to Berend Post berend.post@it-university.nl

Question 1407

Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

- ☐ Function point analysis
- ☐ PERT chart
- ☐ Rapid application development
- ☐ Object-oriented system development

Question 1408

Which of the following is a sophisticated computer based switch that can be thought of as essentially a small in-house phone company for the organization?

- ☐ Private Branch Exchange
- ☐ Virtual Local Area Network
- ☐ Voice over IP
- ☐ Dial-up connection

Question 1409

The PRIMARY objective of testing a business continuity plan is to:

- ☐ familiarize employees with the business continuity plan.
- ☐ ensure that all residual risks are addressed.
- ☐ exercise all possible disaster scenarios.
- ☐ identify limitations of the business continuity plan.

Question 1410

Which of the following is MOST important for an information security manager to ensure is included in a business case for a new system?

- ☐ Intangible benefits of the system
- ☐ Risk associated with the system
- ☐ Effectiveness of controls
- ☐ Audit-logging capabilities

Licensed to Berend Post berend.post@it-university.nl

Question 1411

The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

- ☐ Utilization of an intrusion detection system to report incidents
- ☐ Mandating the use of passwords to access all software
- ☐ Installing an efficient user log system to track the actions of each user
- ☐ Training provided on a regular basis to all current and new employees

Question 1412

When conducting a follow-up of previous audit findings, an IS auditor is told by management that a recommendation to make security changes to an application has not been implemented. The IS auditor should FIRST determine whether:

- ☐ additional time to implement changes is needed.
- ☐ the associated risk is still relevant.
- ☐ the recommendation should be re-issued.
- ☐ the issue should be escalated.

Question 1413

Who is responsible for the overall direction, costs, and timetables for systems-development projects?

- ☐ The project sponsor
- ☐ The project steering committee
- ☐ Senior management
- ☐ The project team leader

Question 1414

The PRIMARY role of a control self-assessment (CSA) facilitator is to:

- ☐ report on the internal control weaknesses.
- ☐ focus the team on internal controls.
- ☐ provide solutions for control weaknesses.
- ☐ conduct interviews to gain background information.

Licensed to Berend Post berend.post@it-university.nl

Question 1415

_____ risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a _____ risk assessment is more appropriate. Fill in the blanks.

- ☐ Quantitative; qualitative
- ☐ Qualitative; quantitative
- ☐ Residual; subjective
- ☐ Quantitative; subjective

Question 1416

Which of the following ACID property in DBMS means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors?

- ☐ Atomicity
- ☐ Consistency
- ☐ Isolation
- ☐ Durability

Question 1417

Nonrepudiation of the client for e-commerce transactions is accomplished through which of the following control mechanisms?

- ☐ Password security
- ☐ Internet protocol (IP) address verification
- ☐ Public key infrastructure (PKI)
- ☐ Secure Sockets Layer (SSL)

Question 1418

An IS auditor has identified the lack of an authorization process for users of an application. The IS auditor's main concern should be that:

- ☐ more than one individual can claim to be a specific user.
- ☐ there is no way to limit the functions assigned to users.
- ☐ user accounts can be shared.
- ☐ users have a need-to-know privilege.

Licensed to Berend Post berend.post@it-university.nl

Question 1419

The decision to accept an IT control risk related to data quality should be the responsibility of the:

- ☐ information security team
- ☐ chief information officer
- ☐ business owner
- ☐ IS audit manager

Question 1420

The MOST useful technique for maintaining management support for the information security program is:

- ☐ identifying the risks and consequences of failure to comply with standards
- ☐ benchmarking the security programs of comparable organizations
- ☐ implementing a comprehensive security awareness and training program
- ☐ informing management about the security of business operations

Question 1421

What is the MOST effective way to ensure security policies and procedures are up-to-date?

- ☐ Verify security requirements are being identified and consistently applied.
- ☐ Align the organization's security practices with industry standards and best practice.
- ☐ Define and document senior management's vision for the direction of the security
- ☐ Prevent security documentation audit issues from being raised

Question 1422

Which of the following term in business continuity defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 1423

The reliability of an application system's audit trail may be questionable if:

- ☐ user IDs are recorded in the audit trail.
- ☐ the security administrator has read-only rights to the audit file.
- ☐ date and time stamps are recorded when an action occurs.
- ☐ users can amend audit trail records when correcting system errors.

Licensed to Berend Post berend.post@it-university.nl

Question 1424

Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing.
True or false?

- ☐ True
- ☐ False

Question 1425

Which of the following should be done FIRST to effectively define the IT audit universe for an entity with multiple business lines?

- ☐ Identify aggregate residual IT risk for each business line.
- ☐ Obtain a complete listing of the entity's IT processes.
- ☐ Obtain a complete listing of assets fundamental to the entity's businesses.
- ☐ Identify key control objectives for each business line's core processes.

Question 1426

Which of the following is MOST likely to prevent social engineering attacks?

- ☐ Security awareness program
- ☐ Employee background checks
- ☐ Implementing positive identification policies
- ☐ Enforcing stronger hiring policies

Question 1427

An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

- ☐ defining the conceptual schema.
- ☐ defining security and integrity checks.
- ☐ liaising with users in developing data model.
- ☐ mapping data model with the internal schema.

Question 1428

Which of the following is MOST important for an IS auditor to review when evaluating the effectiveness of an organization's incident response process?

- ☐ Past incident response actions
- ☐ Incident response staff experience and qualifications
- ☐ Results from management testing of incident response procedures
- ☐ Incident response roles and responsibilities

Licensed to Berend Post berend.post@it-university.nl

Question 1429

How often should a Business Continuity Plan be reviewed?

- ☐ At least once a month
- ☐ At least every six months
- ☐ At least once a year
- ☐ At least Quarterly

Question 1430

Which of the following would MOST effectively enhance the security of a challenge- response based authentication system?

- ☐ Selecting a more robust algorithm to generate challenge strings
- ☐ implementing measures to prevent session hijacking attacks
- ☐ increasing the frequency of associated password changes
- ☐ increasing the length of authentication strings

Question 1431

What is the best defense against Distributed DoS Attack?

- ☐ patch your systems.
- ☐ run a virus checker.
- ☐ run an anti-spy software.
- ☐ find the DoS program and kill it.
- ☐ None of the choices.

Question 1432

Which of the following type of a computer network covers a broad area such as city, region, nation or international link?

- ☐ LAN
- ☐ WAN
- ☐ SAN
- ☐ PAN

Question 1433

Which of the following provides nonrepudiation services for e-commerce transactions?

- ☐ Public key infrastructure (PKI)
- ☐ Data Encryption Standard (DES)
- ☐ Message authentication code (MAC)
- ☐ Personal identification number (PIN)

Licensed to Berend Post berend.post@it-university.nl

Question 1434

In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

- ☐ identify and assess the risk assessment process used by management.
- ☐ identify information assets and the underlying systems.
- ☐ disclose the threats and impacts to management.
- ☐ identify and evaluate the existing controls.

Question 1435

While copying files from a floppy disk, a user introduced a virus into the network. Which of the following would MOST effectively detect the existence of the virus?

- ☐ A scan of all floppy disks before use
- ☐ A virus monitor on the network file server
- ☐ Scheduled daily scans of all network drives
- ☐ A virus monitor on the user's personal computer

Question 1436

When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

- ☐ incorporates state of the art technology.
- ☐ addresses the required operational controls.
- ☐ articulates the IT mission and vision.
- ☐ specifies project management practices.

Question 1437

The scheduling of audit follow-ups should be based PRIMARILY on:

- ☐ costs and audit efforts involved.
- ☐ auditee and auditor time commitments.
- ☐ the risk and exposure involved.
- ☐ control and detection processes.

Question 1438

Which of the following is the GREATEST security threat when an organization allows remote access to a virtual private network (VPN)?

- ☐ Client logins are subject to replay attack.
- ☐ VPN traffic could be sniffed and captured.
- ☐ Compromised VPN clients could impact the network.
- ☐ Attackers could compromise the VPN gateway.

Licensed to Berend Post berend.post@it-university.nl

Question 1439

The PRIMARY purpose of a periodic threat and risk assessment report to senior management is to communicate the:

- ☐ cost-benefit of security controls.
- ☐ status of the security posture.
- ☐ probability of future incidents.
- ☐ risk acceptance criteria.

Question 1440

Who should be responsible for network security operations?

- ☐ Business unit managers
- ☐ Security administrators
- ☐ Network administrators
- ☐ IS auditors

Question 1441

Which of the following is MOST important for the successful establishment of a security vulnerability management program?

- ☐ A comprehensive asset inventory
- ☐ A tested incident response plan
- ☐ An approved patching policy
- ☐ A robust tabletop exercise plan

Question 1442

An organization's senior management is encouraging employees to use social media for promotional purposes. Which of the following should be the information security manager's FIRSTstep to support this strategy?

- ☐ Develop a business case for a data loss prevention solution
- ☐ Develop a guideline on the acceptable use of social media
- ☐ Incorporate social media into the security awareness program
- ☐ Employ the use of a web content filtering solution

Licensed to Berend Post berend.post@it-university.nl

Question 1443

An enterprise receiving email should have procedures to control:

- ☐ insufficient end-points.
- ☐ unsolicited executable code.
- ☐ outdated protocols.
- ☐ insufficient connectivity.

Question 1444

As part of an audit response, an auditee has concerns with the recommendations and is hesitant to implement them. Which of the following would be the BEST course of action for the IS auditor?

- ☐ Accept the auditee's response and perform additional testing.
- ☐ Conduct further discussions with the auditee to develop a mitigation plan.
- ☐ Suggest hiring a third-party consultant to perform a current state assessment.
- ☐ Issue a final report without including the opinion of the auditee.

Question 1445

After implementation of a disaster recovery plan, pre-disaster and post-disaster operational costs for an organization will:

- ☐ decrease.
- ☐ not change (remain the same).
- ☐ increase.
- ☐ increase or decrease depending upon the nature of the business.

Question 1446

The BEST way to avoid session hijacking is to use:

- ☐ a reverse lookup
- ☐ a secure protocol
- ☐ a firewall
- ☐ strong password controls

Question 1447

Who is responsible for reviewing the result and deliverables within and at the end of each phase, as well as confirming compliance with requirements?

- ☐ Project Sponsor
- ☐ Quality Assurance
- ☐ User Management
- ☐ Senior Management

Licensed to Berend Post berend.post@it-university.nl

Question 1448

Which significant risk is introduced by running the file transfer protocol (FTP) service on a server in a demilitarized zone (DMZ)?

- ☐ A user from within could send a file to an unauthorized person.
- ☐ FTP services could allow a user to download files from unauthorized sources.
- ☐ A hacker may be able to use the FTP service to bypass the firewall.
- ☐ FTP could significantly reduce the performance of a DMZ server.

Question 1449

Default permit is only a good approach in an environment where:

- ☐ security threats are non-existent or negligible.
- ☐ security threats are non-negligible.
- ☐ security threats are serious and severe.
- ☐ users are trained.
- ☐ None of the choices.

Question 1450

Security should ALWAYS be an all or nothing issue.

- ☐ True
- ☐ True for trusted systems only
- ☐ True for untrusted systems only
- ☐ False
- ☐ None of the choices.

Question 1451

When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

- ☐ establishment of a review board.
- ☐ creation of a security unit.
- ☐ effective support of an executive sponsor.
- ☐ selection of a security process owner.

Licensed to Berend Post berend.post@it-university.nl

Question 1452

Which of the following statement INCORRECTLY describes device and where they sit within the TCP/IP model?

- ☐ Layer 4 switch work at Network interface layer in TCP/IP model
- ☐ Router works at Network interface layer in TCP/IP model
- ☐ Layer 3 switch work at Network interface layer in TCP/IP model
- ☐ Hub works at LAN or WAN interface layer of a TCP/IP model

Question 1453

Which of the following is the MOST reliable way for an IS auditor to evaluate the operational effectiveness of an organization's data loss prevention (DLP) controls?

- ☐ Verify that confidential files cannot be transmitted to a personal USB device.
- ☐ Conduct interviews to identify possible data protection vulnerabilities.
- ☐ Review data classification levels based on industry best practice.
- ☐ Verify that current DLP software is installed on all computer systems.

Question 1454

When designing metrics for information security, the MOST important consideration is that the metrics:

- ☐ provide actionable data.
- ☐ apply to all business units.
- ☐ are easy to understand.
- ☐ track trends over time.

Question 1455

An IS auditor reviewing a database application discovers that the current configuration does not match the originally designed structure. Which of the following should be the IS auditor's next action?

- ☐ Analyze the need for the structural change.
- ☐ Recommend restoration to the originally designed structure.
- ☐ Recommend the implementation of a change control process.
- ☐ Determine if the modifications were properly approved.

Licensed to Berend Post berend.post@it-university.nl

Question 1456

Which of the following should be of GREATEST concern to an IS auditor reviewing actions taken during a forensic investigation?

- ☐ The investigation report does not indicate a conclusion.
- ☐ An image copy of the attacked system was not taken.
- ☐ The proper authorities were not notified.
- ☐ The handling procedures of the attacked system are not documented.

Question 1457

In which of the following WAN message transmission technique messages are divided into packets before they are sent and each packet is then transmitted individually and can even follow different routes to its destination?

- ☐ Message Switching
- ☐ Packet switching
- ☐ Circuit switching
- ☐ Virtual Circuits

Question 1458

Use of asymmetric encryption in an internet e-commerce site, where there is one private key for the hosting server and the public key is widely distributed to the customers, is MOST likely to provide comfort to the:

- ☐ customer over the authenticity of the hosting organization.
- ☐ hosting organization over the authenticity of the customer.
- ☐ customer over the confidentiality of messages from the hosting organization.
- ☐ hosting organization over the confidentiality of messages passed to the customer.

Question 1459

Which of the following is the BEST performance criterion for evaluating the adequacy of an organization's security awareness training?

- ☐ Senior management is aware of critical information assets and demonstrates an adequate concern for their protection.
- ☐ Job descriptions contain clear statements of accountability for information security.
- ☐ In accordance with the degree of risk and business impact, there is adequate funding for security efforts.
- ☐ No actual incidents have occurred that have caused a loss or a public embarrassment.

Licensed to Berend Post berend.post@it-university.nl

Question 1460

When facilitating the alignment of corporate governance and information security governance, which of the following is the MOST important role of an organization's security steering committee?

- ☐ Obtaining support for the integration from business owners
- ☐ Obtaining approval for the information security budget
- ☐ Evaluating and reporting the degree of integration
- ☐ Defining metrics to demonstrate alignment

Question 1461

What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?

- ☐ Business risk
- ☐ Detection risk
- ☐ Residual risk
- ☐ Inherent risk

Question 1462

Business process re-engineering often results in _____ automation, which results in _____ number of people using technology. Fill in the blanks.

- ☐ Increased; a greater
- ☐ Increased; a fewer
- ☐ Less; a fewer
- ☐ Increased; the same

Question 1463

An organization's HR department would like to outsource its employee management system to a cloud-hosted solution due to features and cost savings offered. Management has identified this solution as a business need and wants to move forward. What should be the PRIMARY role of information security in this effort?

- ☐ Ensure a security audit is performed of the service provider.
- ☐ Ensure the service provider has the appropriate certifications.
- ☐ Determine how to securely implement the solution.
- ☐ Explain security issues associated with the solution to management.

Licensed to Berend Post berend.post@it-university.nl

Question 1464

An IS auditor reviewing an organization's data privacy controls observes that privacy notices do not clearly state how the organization uses customer data for its processing operations. Which of the following data protection principles MUST be implemented to address this gap?

- ☐ Maintenance of data integrity
- ☐ Access to collected data
- ☐ Retention of consent documentation
- ☐ Purpose for data collection

Question 1465

Which of the following type of honey pot essentially gives a hacker a real environment to attack?

- ☐ High-interaction
- ☐ Low-interaction
- ☐ Med-interaction
- ☐ None of the choices

Question 1466

The objectives of business process improvement should PRIMARILY include:

- ☐ minimal impact on staff
- ☐ incremental changes in productivity
- ☐ changes of organizational boundaries
- ☐ performance optimization

Question 1467

Which of the following is the BEST source of information when assessing the amount of time a project will take?

- ☐ GANTT chart
- ☐ Workforce estimate
- ☐ Critical path analysis
- ☐ Scheduling budget

Licensed to Berend Post berend.post@it-university.nl

Question 1468

How is risk affected if users have direct access to a database at the system level?

- ☐ Risk of unauthorized access increases, but risk of untraceable changes to the database decreases.
- ☐ Risk of unauthorized and untraceable changes to the database increases.
- ☐ Risk of unauthorized access decreases, but risk of untraceable changes to the database increases.
- ☐ Risk of unauthorized and untraceable changes to the database decreases.

Question 1469

What is the BEST backup strategy for a large database with data supporting online sales?

- ☐ Weekly full backup with daily incremental backup
- ☐ Daily full backup
- ☐ Clustered servers
- ☐ Mirrored hard disks

Question 1470

Which of the following is MOST is critical during the business impact assessment phase of business continuity planning?

- ☐ End-user involvement
- ☐ Senior management involvement
- ☐ Security administration involvement
- ☐ IS auditing involvement

Question 1471

Due to changes in IT, the disaster recovery plan of a large organization has been changed. What is the PRIMARY risk if the new plan is not tested?

- ☐ Catastrophic service interruption
- ☐ High consumption of resources
- ☐ Total cost of the recovery may not be minimized
- ☐ Users and recovery teams may face severe difficulties when activating the plan

Licensed to Berend Post berend.post@it-university.nl

Question 1472

Calculation of the recovery time objective (RTO) is necessary to determine the:

- ☐ time required to restore files.
- ☐ annual loss expectancy (ALE).
- ☐ point of synchronization.
- ☐ priority of restoration.

Question 1473

Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

- ☐ Cold site
- ☐ Hot site
- ☐ Alternate site
- ☐ Warm site

Question 1474

After identifying potential security vulnerabilities, what should be the IS auditor's next step?

- ☐ To evaluate potential countermeasures and compensatory controls
- ☐ To implement effective countermeasures and compensatory controls
- ☐ To perform a business impact analysis of the threats that would exploit the vulnerabilities
- ☐ To immediately advise senior management of the findings

Question 1475

Which of the following functionality is NOT performed by the application layer of a TCP/IP model?

- ☐ Print service, application services
- ☐ Data encryption and compression
- ☐ Dialog management
- ☐ End-to-end connection

Licensed to Berend Post berend.post@it-university.nl

Question 1476

An organization that has outsourced its incident management capabilities just discovered a significant privacy breach by an unknown attacker. Which of the following is the MOST important action of the security manager?

- ☐ Follow the outsourcer's response plan
- ☐ Refer to the organization's response plan
- ☐ Notify the outsourcer of the privacy breach
- ☐ Alert the appropriate law enforcement authorities

Question 1477

Which of the following is normally a responsibility of the chief security officer (CSO)?

- ☐ Periodically reviewing and evaluating the security policy
- ☐ Executing user application and software testing and evaluation
- ☐ Granting and revoking user access to IT resources
- ☐ Approving access to data and applications

Question 1478

An IS audit manager finds that data manipulation logic developed by the audit analytics team leads to incorrect conclusions. This inaccurate logic is MOST likely an indication of which of the following?

- ☐ Incompatibility between data volume and analytics processing capacity.
- ☐ Poor security controls that grant inappropriate access to analysis produced.
- ☐ The team's poor understanding of the business process being analyzed.
- ☐ Poor change controls over data sets collected from the business.

Question 1479

Which of the following is MOST important to ensure when planning a black box penetration test?

- ☐ The test results will be documented and communicated to management.
- ☐ Diagrams of the organization's network architecture are available.
- ☐ The environment and penetration test scope have been determined.
- ☐ The management of the client organization is aware of the testing.

Licensed to Berend Post berend.post@it-university.nl

Question 1480

Which of the following is an estimation technique where the results can be measure by the functional size of an information system based on the number and complexity of input, output, interface and queries?

- ☐ Functional Point analysis
- ☐ Gantt Chart
- ☐ Time box management
- ☐ Critical path methodology

Question 1481

Which of the following should be seen as one of the most significant factors considered when determining the frequency of IS audits within your organization?

- ☐ The cost of risk analysis
- ☐ The income generated by the business function
- ☐ Resource allocation strategy
- ☐ The nature and level of risk
- ☐ None of the choices.

Question 1482

An IS auditor finds that a DBA has read and write access to production data. The IS auditor should:

- ☐ accept the DBA access as a common practice.
- ☐ assess the controls relevant to the DBA function.
- ☐ recommend the immediate revocation of the DBA access to production data.
- ☐ review user access authorizations approved by the DBA.

Question 1483

Which of the following security testing techniques is MOST effective in discovering unknown malicious attacks?

- ☐ Vulnerability testing
- ☐ Reverse engineering
- ☐ Penetration testing
- ☐ Sandboxing

Licensed to Berend Post berend.post@it-university.nl

Question 1484

Who is accountable for maintaining appropriate security measures over information assets?

- ☐ Data and systems owners
- ☐ Data and systems users
- ☐ Data and systems custodians
- ☐ Data and systems auditors

Question 1485

Which of the following is MOST useful to include in a report to senior management on a regular basis to demonstrate the effectiveness of the information security program?

- ☐ Critical success factors (CSFs)
- ☐ Key risk indicators (KRIs)
- ☐ Capability maturity models
- ☐ Key performance indicators (KPIs)

Question 1486

The frequent updating of which of the following is key to the continued effectiveness of a disaster recovery plan (DRP)?

- ☐ Contact information of key personnel
- ☐ Server inventory documentation
- ☐ individual roles and responsibilities
- ☐ Procedures for declaring a disaster

Question 1487

Which of the following is MOST likely to be included in an enterprise information security policy?

- ☐ Password composition requirements
- ☐ Consequences of noncompliance
- ☐ Audit trail review requirements
- ☐ Security monitoring strategy

Question 1488

The PRIMARY advantage of object-oriented technology is enhanced:

- ☐ efficiency due to the re-use of elements of logic.
- ☐ management of sequential program execution for data access.
- ☐ management of a restricted variety of data types for a data object.
- ☐ grouping of objects into methods for data access.

Licensed to Berend Post berend.post@it-university.nl

Question 1489

Which of the following cloud computing service model provides a way to rent operating systems, storage and network capacity over the Internet?

- ☐ Software as a service
- ☐ Data as a service
- ☐ Platform as a service
- ☐ Infrastructure as a service

Question 1490

Following a malicious security incident, an organization has decided to prosecute those responsible. Which of the following will BEST facilitate the forensic investigation?

- ☐ Identifying the affected environment
- ☐ Performing a backup of affected systems
- ☐ Determining the degree of loss
- ☐ Maintaining chain of custody

Question 1491

Which of the following term related to network performance refers to the number of corrupted bits expressed as a percentage or fraction of the total sent?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Error Rate

Question 1492

Which of the following controls will BEST ensure that the board of directors receives sufficient information about IT?

- ☐ The CIO reports on performance and corrective actions in a timely manner.
- ☐ Regular meetings occur between the board, the CIO. and a technology committee.
- ☐ The CIO regularly sends IT trend reports to the board.
- ☐ Board members are knowledgeable about IT, and the CIO is consulted on IT issues.

Licensed to Berend Post berend.post@it-university.nl

Question 1493

Which of the following encryption techniques will BEST protect a wireless network from a man-in-the-middle attack?

- ☐ 128-bit wired equivalent privacy (WEP)
- ☐ MAC-based pre-shared key(PSK)
- ☐ Randomly generated pre-shared key (PSKJ
- ☐ Alphanumeric service set identifier (SSID)

Question 1494

When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

- ☐ True
- ☐ False

Question 1495

Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting from normal network activity?

- ☐ Statistical-based
- ☐ Signature-based
- ☐ Neural network
- ☐ Host-based

Question 1496

An IS auditor finds that intellectual property is not being protected to the level specified in the organization's data classification and protection policy. The business owner is aware of this issue and chooses to accept the risk. Which of the following is the auditor's BEST course of action?

- ☐ Note the finding and request formal acceptance.
- ☐ Include the finding in the follow-up audit.
- ☐ Amend the data classification policy.
- ☐ Form a committee and further investigate the issue.

Licensed to Berend Post berend.post@it-university.nl

Question 1497

What is the primary security concern for EDI environments?

- ☐ Transaction authentication
- ☐ Transaction completeness
- ☐ Transaction accuracy
- ☐ Transaction authorization

Question 1498

When the inherent risk of a business activity is lower than the acceptable risk level, the BEST course of action would be to:

- ☐ implement controls to mitigate the risk.
- ☐ report compliance to management.
- ☐ review the residual risk level.
- ☐ monitor for business changes.

Question 1499

Which of the following IT governance best practices improves strategic alignment?

- ☐ Supplier and partner risks are managed.
- ☐ A knowledge base on customers, products, markets and processes is in place.
- ☐ A structure is provided that facilitates the creation and sharing of business information.
- ☐ Top management mediate between the imperatives of business and technology.

Question 1500

Which of the following should an IS auditor expect to see in a network vulnerability assessment?

- ☐ Misconfiguration and missing updates
- ☐ Malicious software and spyware
- ☐ Security design flaws
- ☐ Zero-day vulnerabilities

Question 1501

Which of the following is a good control for protecting confidential data residing on a PC?

- ☐ Personal firewall
- ☐ File encapsulation
- ☐ File encryption
- ☐ Host-based intrusion detection

Licensed to Berend Post berend.post@it-university.nl

Question 1502

A database administrator should be prevented from:

- ☐ using an emergency user ID.
- ☐ accessing sensitive information.
- ☐ having end user responsibilities.
- ☐ having access to production files.

Question 1503

An airline's online booking system uses an automated script that checks whether fares are within the defined threshold of what is reasonable before the fares are displayed on the website. Which type of control is in place?

- ☐ Compensating control
- ☐ Preventive control
- ☐ Detective control
- ☐ Corrective control

Question 1504

Which of the following penetration tests would MOST effectively evaluate incident handling and response capabilities of an organization?

- ☐ Targeted testing
- ☐ External testing
- ☐ internal testing
- ☐ Double-blind testing

Question 1505

During the implementation of a new system, an IS auditor must assess whether certain automated calculations comply with the regulatory requirements. Which of the following is the BEST way to obtain this assurance?

- ☐ Inspect user acceptance test results.
- ☐ Re-perform the calculation with audit software.
- ☐ Review sign-off documentation.
- ☐ Review the source code related to the calculation.

Licensed to Berend Post berend.post@it-university.nl

Question 1506

An IS auditor reviewing digital rights management (DRM) applications should expect to find an extensive use for which of the following technologies?

- ☐ Digitalized signatures
- ☐ Hashing
- ☐ Parsing
- ☐ Steganography

Question 1507

With the objective of mitigating the risk and impact of a major business interruption, a disaster recovery plan should endeavor to reduce the length of recovery time necessary, as well as costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs. True or false?

- ☐ True
- ☐ False

Question 1508

Which cloud deployment model is MOST likely to be limited in scalability?

- ☐ Public
- ☐ Private
- ☐ Hybrid
- ☐ Community

Question 1509

An IS auditor has been assigned to review IT structures and activities recently outsourced to various providers. Which of the following should the IS auditor determine FIRST?

- ☐ That an audit clause is present in all contracts
- ☐ That the SLA of each contract is substantiated by appropriate KPIs
- ☐ That the contractual warranties of the providers support the business needs of the organization
- ☐ That at contract termination, support is guaranteed by each outsourcer for new outsourcers

Licensed to Berend Post berend.post@it-university.nl

Question 1510

Which of the following attack involves slicing small amount of money from a computerize transaction or account?

- ☐ Eavesdropping
- ☐ Traffic Analysis
- ☐ Salami
- ☐ Masquerading

Question 1511

Which of the following is the PRIMARY benefit of including IT management and staff when conducting control self-assessments (CSAs) within an organization?

- ☐ It helps to identify risk to the business.
- ☐ It improves the efficiency of business and IT operational processes.
- ☐ It increases buy-in for more stringent controls.
- ☐ It reduces the workload of external and internal auditors.

Question 1512

The risks associated with electronic evidence gathering would MOST likely be reduced by an e- mail:

- ☐ destruction policy.
- ☐ security policy.
- ☐ archive policy.
- ☐ audit policy.

Question 1513

During a follow-up audit, an IS auditor finds that some critical recommendations have not been addressed as management has decided to accept the risk. Which of the following is the IS auditor's BEST course of action?

- ☐ Adjust the annual risk assessment accordingly.
- ☐ Require the auditee to address the recommendations in full.
- ☐ Evaluate senior management's acceptance of the risk.
- ☐ Update the audit program based on management's acceptance of risk.

Licensed to Berend Post berend.post@it-university.nl

Question 1514

An organization is using an enterprise resource management (ERP) application. Which of the following would be an effective access control?

- ☐ User-level permissions
- ☐ Role-based
- ☐ Fine-grained
- ☐ Discretionary

Question 1515

The PRIMARY purpose of an IT forensic audit is:

- ☐ to participate in investigations related to corporate fraud.
- ☐ the systematic collection of evidence after a system irregularity.
- ☐ to assess the correctness of an organization's financial statements
- ☐ to determine that there has been criminal activity.

Question 1516

Which of the following tasks should be performed during an organization's business continuity plan (BCP) test?

- ☐ Evaluate the security at the offsite facility.
- ☐ Review the coverage of insurance.
- ☐ Assess the critical information retrieval capability.
- ☐ Review the alternate processing site contract.

Question 1517

Which of the following is the most fundamental step in preventing virus attacks?

- ☐ Adopting and communicating a comprehensive antivirus policy
- ☐ Implementing antivirus protection software on users' desktop computers
- ☐ Implementing antivirus content checking at all network-to-Internet gateways
- ☐ Inoculating systems with antivirus code

Question 1518

Which of the following factors will BEST promote effective information security management?

- ☐ Senior management commitment
- ☐ Identification and risk assessment of sensitive resources
- ☐ Security awareness training
- ☐ Security policy framework

Licensed to Berend Post berend.post@it-university.nl

Question 1519

During a computer forensics investigation, what is the PRIMARY reason for obtaining a bit-for-bit copy of data in storage?

- ☐ To document findings
- ☐ To obtain residual data
- ☐ To obtain data as well as source code details
- ☐ To transfer the data into a controlled location

Question 1520

Which of the following attack is against computer network and involves fragmented or invalid ICMP packets sent to the target?

- ☐ Nuke attack
- ☐ Brute force attack
- ☐ Buffer overflow
- ☐ Pulsing Zombie

Question 1521

A disk management system's PRIMARY function is to:

- ☐ monitor disk accesses for analytical review
- ☐ deny access to disk resident data files
- ☐ provide data on efficient disk usage
- ☐ provide the method of control for disk usage

Question 1522

Which of the following provides the strongest authentication for physical access control?

- ☐ Sign-in logs
- ☐ Dynamic passwords
- ☐ Key verification
- ☐ Biometrics

Question 1523

Which of the following is the MOST critical characteristic of a biometric system?

- ☐ Registration time
- ☐ Throughput rate
- ☐ Accuracy
- ☐ Ease of use

Licensed to Berend Post berend.post@it-university.nl

Question 1524

A transaction journal provides the information necessary for detecting unauthorized _____ (fill in the blank) from a terminal.

- ☐ Deletion
- ☐ Input
- ☐ Access
- ☐ Duplication

Question 1525

When protecting the confidentiality of information assets, the MOST effective control practice is the:

- ☐ awareness training of personnel on regulatory requirements.
- ☐ enforcement of a need-to-know access control philosophy.
- ☐ utilization of a dual-factor authentication mechanism.
- ☐ configuration of read-only access to all users.

Question 1526

A system administrator recently informed the IS auditor about the occurrence of several unsuccessful intrusion attempts from outside the organization. Which of the following is MOST effective in detecting such an intrusion?

- ☐ Installing biometrics-based authentication
- ☐ Configuring the router as a firewall
- ☐ Periodically reviewing log files
- ☐ Using smart cards with one-time passwords

Question 1527

Which of the following cloud deployment models would BEST meet the needs of a startup software development organization with limited initial capital?

- ☐ Private
- ☐ Public
- ☐ Community
- ☐ Hybrid

Licensed to Berend Post berend.post@it-university.nl

Question 1528

The MOSTimportant objective of security awareness training for business staff is to:

- ☐ understand intrusion methods
- ☐ reduce negative audit findings
- ☐ increase compliance
- ☐ modify behavior

Question 1529

An IS auditor has discovered that a cloud-based application was not included in an application inventory that was used to confirm the scope of an audit. The business process owner explained that the application will be audited by a third party in the next year. The auditor's NEXT step should be to:

- ☐ evaluate the impact of the cloud application on the audit scope
- ☐ revise the audit scope to include the cloud-based application
- ☐ review the audit report when performed by the third party
- ☐ report the control deficiency to senior management

Question 1530

The PRIMARY purpose of a security information and event management (SIEM) system is to:

- ☐ identify potential incidents
- ☐ provide status of incidents
- ☐ resolve incidents
- ☐ track ongoing incidents

Question 1531

Which of the following is a mechanism for mitigating risks?

- ☐ Security and control practices
- ☐ Property and liability insurance
- ☐ Audit and certification
- ☐ Contracts and service level agreements (SLAs)

Question 1532

Which of the following is the BEST course of action for an information security manager to align security and business goals?

- ☐ Reviewing the business strategy
- ☐ Actively engaging with stakeholders
- ☐ Conducting a business impact analysis
- ☐ Defining key performance indicators

Licensed to Berend Post berend.post@it-university.nl

Question 1533

A disaster recovery plan for an organization's financial system specifies that the recovery point objective (RPO) is no data loss and the recovery time objective (RTO) is 72 hours. Which of the following is the MOST cost-effective solution?

- ☐ A hot site that can be operational in eight hours with asynchronous backup of the transaction logs
- ☐ Distributed database systems in multiple locations updated asynchronously
- ☐ Synchronous updates of the data and standby active systems in a hot site
- ☐ Synchronous remote copy of the data in a warm site that can be operational in 48 hours

Question 1534

An organization plans to launch a social media presence as part of a new customer service campaign. Which of the following is the MOST significant risk from the perspective of potential litigation?

- ☐ The policy stating what employees can post on the organization’s behalf is unclear.
- ☐ Access to corporate-sponsored social media accounts requires only single-factor authentication.
- ☐ Approved employees can use personal devices to post on the company’s behalf.
- ☐ There is a lack of clear procedures for responding to customers on social media outlets.

Question 1535

When performing a database review, an IS auditor notices that some tables in the database are not normalized. The IS auditor should next:

- ☐ recommend that the database be normalized.
- ☐ review the conceptual data model.
- ☐ review the stored procedures.
- ☐ review the justification.

Question 1536

What is the MOST effective method of preventing unauthorized use of data files?

- ☐ Automated file entry
- ☐ Tape librarian
- ☐ Access control software
- ☐ Locked library

Licensed to Berend Post berend.post@it-university.nl

Question 1537

Which of the following typically focuses on making alternative processes and resources available for transaction processing?

- ☐ Cold-site facilities
- ☐ Disaster recovery for networks
- ☐ Diverse processing
- ☐ Disaster recovery for systems

Question 1538

Which of the following is the GREATEST risk when implementing a data warehouse?

- ☐ increased response time on the production systems
- ☐ Access controls that are not adequate to prevent data modification
- ☐ Data duplication
- ☐ Data that is not updated or current

Question 1539

An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:

- ☐ hardware configuration.
- ☐ access control software.
- ☐ ownership of intellectual property.
- ☐ application development methodology.

Question 1540

Which of the following BEST supports the prioritization of new IT projects?

- ☐ Internal control self-assessment (CSA)
- ☐ Information systems audit
- ☐ Investment portfolio analysis
- ☐ Business risk assessment

Question 1541

The MAIN reason an organization's incident management procedures should include a post-incident review is to:

- ☐ ensure evidence is collected for possible post-event litigation.
- ☐ take appropriate action when procedures are not followed.
- ☐ enable better reporting for executives and the audit committee.
- ☐ improve processes by learning from identified weaknesses.

Licensed to Berend Post berend.post@it-university.nl

Question 1542

During a follow-up audit, an IS auditor discovers that a recommendation has not been implemented. However, the auditee has implemented a manual workaround that addresses the identified risk, through far less efficiency than the recommended action would. Which of the following would be the auditor's BEST course of action?

- ☐ Notify management that the risk has been addressed and take no further action.
- ☐ Escalate the remaining issue for further discussion and resolution.
- ☐ Note that the risk has been addressed and notify management of the inefficiency.
- ☐ Insist to management that the original recommendation be implemented.

Question 1543

The MAJOR reason for segregating test programs from production programs is to:

- ☐ achieve segregation of duties between IS staff and end users.
- ☐ limit access rights of IS staff to the development environment.
- ☐ provide control over program changes.
- ☐ provide the basis for efficient system change management.

Question 1544

Which of the following would contribute MOST to employees' understanding of data handling responsibilities?

- ☐ Requiring staff acknowledgement of security policies
- ☐ Labeling documents according to appropriate security classification
- ☐ Implementing a tailored security awareness training program
- ☐ Demonstrating support by senior management of the security program

Question 1545

In auditing a web server, an IS auditor should be concerned about the risk of individuals gaining unauthorized access to confidential information through:

- ☐ common gateway interface (CGI) scripts.
- ☐ enterprise Java beans (EJBs).
- ☐ applets.
- ☐ web services.

Licensed to Berend Post berend.post@it-university.nl

Question 1546

Which of the following is an example of the defense in-depth security principle?

- ☐ Using two firewalls of different vendors to consecutively check the incoming network traffic
- ☐ Using a firewall as well as logical access controls on the hosts to control incoming network traffic
- ☐ Having no physical signs on the outside of a computer center building
- ☐ Using two firewalls in parallel to check different types of incoming traffic

Question 1547

Which of the following attack redirects outgoing message from the client back onto the client, preventing outside access as well as flooding the client with the sent packets?

- ☐ Banana attack
- ☐ Brute force attack
- ☐ Buffer overflow
- ☐ Pulsing Zombie

Question 1548

An organization uses two data centers. Which of the following would BEST address the organization's need for high resiliency?

- ☐ The data centers act as mirrored sites.
- ☐ Each data center is recoverable via tape backups.
- ☐ A hot site is used for the second site.
- ☐ There is data replication across the data centers.

Question 1549

Which of the following would be the MOST effective audit technique for identifying segregation of duties violations in a new enterprise resource planning (ERP) implementation?

- ☐ Reviewing a report of security rights in the system
- ☐ Reviewing the complexities of authorization objects
- ☐ Building a program to identify conflicts in authorization
- ☐ Examining recent access rights violation cases

Licensed to Berend Post berend.post@it-university.nl

Question 1550

Which of the following is often used as a detection and deterrent control against Internet attacks?

- ☐ Honeypots
- ☐ CCTV
- ☐ VPN
- ☐ VLAN

Question 1551

Reevaluation of risk is MOST critical when there is:

- ☐ resistance to the implementation of mitigating controls
- ☐ a change in security policy
- ☐ a management request for updated security reports
- ☐ a change in the threat landscape

Question 1552

An organization with extremely high security requirements is evaluating the effectiveness of biometric systems. Which of the following performance indicators is MOST important?

- ☐ False-acceptance rate (FAR)
- ☐ Equal-error rate (EER)
- ☐ False-rejection rate (FRR)
- ☐ False-identification rate (FIR)

Question 1553

How does the digital envelop work? What are the correct steps to follow?

- ☐ You encrypt the data using a session key and then encrypt session key using private key of a sender
- ☐ You encrypt the data using the session key and then you encrypt the session key using sender's public key
- ☐ You encrypt the data using the session key and then you encrypt the session key using the receiver's public key
- ☐ You encrypt the data using the session key and then you encrypt the session key using the receiver's private key

Licensed to Berend Post berend.post@it-university.nl

Question 1554

In an EDI process, the device which transmits and receives electronic documents is the:

- ☐ communications handler.
- ☐ EDI translator.
- ☐ application interface.
- ☐ EDI interface.

Question 1555

Of the following, who should the security manager consult FIRST when determining the severity level of a security incident involving a third-party vendor?

- ☐ IT process owners
- ☐ Business partners
- ☐ Risk manager
- ☐ Business process owners

Question 1556

When planning to add personnel to tasks imposing time constraints on the duration of a project, which of the following should be revalidated FIRST?

- ☐ The project budget
- ☐ The critical path for the project
- ☐ The length of the remaining tasks
- ☐ The personnel assigned to other tasks

Question 1557

When assessing a business case as part of a post-implementation review, the IS auditor must ensure that the:

- ☐ feasibility of alternative project approaches has been assessed.
- ☐ business case has not been amended since project approval.
- ☐ quality assurance measures have been applied throughout the project.
- ☐ amendments to the business case have been approved.

Licensed to Berend Post berend.post@it-university.nl

Question 1558

An IS audit report highlighting inadequate network internal controls is challenged because no serious incident has ever occurred. Which of the following actions performed during the audit would have BEST supported the findings?

- ☐ Compliance testing
- ☐ Threat risk assessment
- ☐ Penetration testing
- ☐ Vulnerability assessment

Question 1559

During the review of a biometrics system operation, an IS auditor should FIRST review the stage of:

- ☐ enrollment.
- ☐ identification.
- ☐ verification.
- ☐ storage.

Question 1560

A vendor service level agreement (SLA) requires backups to be physically secured. An IS audit of the backup system revealed a number of the backup media were missing. Which of the following should be the auditor's NEXT step?

- ☐ Recommend a review of the vendor's contract.
- ☐ Recommend identification of the data stored on the missing media.
- ☐ Notify executive management.
- ☐ Include the missing backup media finding in the audit report.

Question 1561

Which of the following should be of MOST concern to an IS auditor?

- ☐ Lack of reporting of a successful attack on the network
- ☐ Failure to notify police of an attempted intrusion
- ☐ Lack of periodic examination of access rights
- ☐ Lack of notification to the public of an intrusion

Licensed to Berend Post berend.post@it-university.nl

Question 1562

Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

- ☐ System owners
- ☐ System users
- ☐ System designers
- ☐ System builders

Question 1563

An organization has purchased a security information and event management (SIEM) tool. Which of the following would be MOST important to consider before implementation?

- ☐ The contract with the SIEM vendor
- ☐ Controls to be monitored
- ☐ Available technical support
- ☐ Reporting capabilities

Question 1564

The rate of change in technology increases the importance of:

- ☐ outsourcing the IS function.
- ☐ implementing and enforcing good processes.
- ☐ hiring personnel willing to make a career within the organization.
- ☐ meeting user requirements.

Question 1565

During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

- ☐ an unauthorized user may use the ID to gain access.
- ☐ user access management is time consuming.
- ☐ passwords are easily guessed.
- ☐ user accountability may not be established.

Question 1566

Which of the following would present the GREATEST need to revise information security policies?

- ☐ An increase in reported incidents
- ☐ A merger with a competing company
- ☐ Implementation of a new firewall
- ☐ Changes in standards and procedures

Licensed to Berend Post berend.post@it-university.nl

Question 1567

The prioritization of incident response actions should be PRIMARILY based on which of the following?

- ☐ Scope of disaster
- ☐ Business impact
- ☐ Availability of personnel
- ☐ Escalation process

Question 1568

Which of the following findings would be of GREATEST concern to an IS auditor performing an information security audit of critical server log management activities?

- ☐ Log records can be overwritten before being reviewed.
- ☐ Logging procedures are insufficiently documented.
- ☐ Log records are dynamically into different servers.
- ☐ Logs are monitored using manual processes.

Question 1569

Which of the following types of attack makes use of common consumer devices that can be used to transfer data surreptitiously?

- ☐ Direct access attacks
- ☐ Indirect access attacks
- ☐ Port attack
- ☐ Window attack
- ☐ Social attack
- ☐ None of the choices.

Question 1570

Which of the following risks could result from inadequate software baselining?

- ☐ Scope creep
- ☐ Sign-off delays
- ☐ Software integrity violations
- ☐ inadequate controls

Licensed to Berend Post berend.post@it-university.nl

Question 1571

Which of the following should be the FIRST step when conducting an IT risk assessment?

- ☐ Assess vulnerabilities
- ☐ Identify assets to be protected
- ☐ Evaluate controls in place
- ☐ Identify potential threats

Question 1572

What is an acceptable mechanism for extremely time-sensitive transaction processing?

- ☐ Off-site remote journaling
- ☐ Electronic vaulting
- ☐ Shadow file processing
- ☐ Storage area network

Question 1573

Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would MOST likely focus on a review of:

- ☐ pre-BPR process flowcharts.
- ☐ post-BPR process flowcharts.
- ☐ BPR project plans.
- ☐ continuous improvement and monitoring plans.

Question 1574

A finance department director has decided to outsource the organization's budget application and has identified potential providers. Which of the following actions should be initiated FIRST by the information security manager?

- ☐ Validate that connectivity to the service provider can be made securely.
- ☐ Obtain audit reports on the service providers hosting environment.
- ☐ Review the disaster recovery plans (DRP) of the providers.
- ☐ Align the roles of the organization's and the service providers' staffs.

Question 1575

Which of the following biometrics has the highest reliability and lowest false-acceptance rate (FAR)?

- ☐ Palm scan
- ☐ Face recognition
- ☐ Retina scan
- ☐ Hand geometry

Licensed to Berend Post berend.post@it-university.nl

Question 1576

An organization is replacing a mission-critical system. Which of the following is the BEST implementation strategy to mitigate and reduce the risk of system failure?

- ☐ Stage
- ☐ Phase
- ☐ Parallel
- ☐ Big-bang

Question 1577

An IS auditor finds that application servers had inconsistent security settings leading to potential vulnerabilities. Which of the following is the BEST recommendation by the IS auditor?

- ☐ Improve the change management process
- ☐ Perform a configuration review
- ☐ Establish security metrics
- ☐ Perform a penetration test

Question 1578

Which of the following answer specifies the correct sequence of levels within the Capability Maturity Model (CMM)?

- ☐ Initial, Managed, Defined, Quantitatively managed, optimized
- ☐ Initial, Managed, Defined, optimized, Quantitatively managed
- ☐ Initial, Defined, Managed, Quantitatively managed, optimized
- ☐ Initial, Managed, Quantitatively managed, Defined, optimized

Question 1579

An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling, when:

- ☐ the probability of error must be objectively quantified.
- ☐ the auditor wishes to avoid sampling risk.
- ☐ generalized audit software is unavailable.
- ☐ the tolerable error rate cannot be determined.

Licensed to Berend Post berend.post@it-university.nl

Question 1580

Which of the following terms is used more generally for describing concealment routines in a malicious program?

- ☐ virus
- ☐ worm
- ☐ trojan horse
- ☐ spyware
- ☐ rootkits
- ☐ backdoor
- ☐ None of the choices.

Question 1581

An IS auditor is planning to audit an organization's infrastructure for access, patching, and change management. Which of the following is the BEST way to prioritize the systems?

- ☐ Complexity of the environment
- ☐ Criticality of the system
- ☐ System hierarchy within the infrastructure
- ☐ System retirement plan

Question 1582

An internet-based attack using password sniffing can:

- ☐ enable one party to act as if they are another party.
- ☐ cause modification to the contents of certain transactions.
- ☐ be used to gain access to systems containing proprietary information.
- ☐ result in major problems with billing systems and transaction processing agreements.

Question 1583

Which of the following BEST indicates the effectiveness of an organization's risk management program?

- ☐ Control risk is minimized.
- ☐ Inherent risk is eliminated.
- ☐ Residual risk is minimized.
- ☐ Overall risk is quantified.

Licensed to Berend Post berend.post@it-university.nl

Question 1584

An organization has implemented data storage hardware. Which of the following should an IS auditor review to assess if IT is maximizing storage and network utilization?

- ☐ Capacity management plans
- ☐ Downtime statistics
- ☐ The quality management systems
- ☐ Routine and non-routine job schedules

Question 1585

An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the GREATEST risk?

- ☐ Pilot
- ☐ Parallel
- ☐ Direct cutover
- ☐ Phased

Question 1586

The BEST test to determine whether an application's internal security controls are configured in compliance with the organization's security standards is an evaluation of the:

- ☐ availability and frequency of security reports
- ☐ intrusion detection system (IDS) logs
- ☐ application's user accounts and passwords
- ☐ business application's security parameter settings

Question 1587

A TCP/IP-based environment is exposed to the Internet. Which of the following BEST ensures that complete encryption and authentication protocols exist for protecting information while transmitted?

- ☐ Work is completed in tunnel mode with IP security using the nested services of authentication header (AH) and encapsulating security payload (ESP).
- ☐ A digital signature with RSA has been implemented.
- ☐ Digital certificates with RSA are being used.
- ☐ Work is being completed in TCP services.

Licensed to Berend Post berend.post@it-university.nl

Question 1588

Change management procedures are established by IS management to:

- ☐ control the movement of applications from the test environment to the production environment.
- ☐ control the interruption of business operations from lack of attention to unresolved problems.
- ☐ ensure the uninterrupted operation of the business in the event of a disaster.
- ☐ verify that system changes are properly documented.

Question 1589

IS management has decided to replace the current single-server-based local area network (LAN) with three interconnected servers running different operating systems. Existing applications and data on the old server have been exclusively distributed on the new servers. This will MOST likely result in:

- ☐ disclosure of information.
- ☐ multiple authentication.
- ☐ data incompleteness.
- ☐ data unavailability.

Question 1590

Senior management has approved employees working off-site by using a virtual private network (VPN) connection. It is MOST important for the information security manager to periodically:

- ☐ review firewall configuration
- ☐ review the security policy
- ☐ perform a cost-benefit analysis
- ☐ perform a risk assessment

Question 1591

When auditing an organization's software acquisition process, the BEST way for an IS auditor to understand the software benefits to the organization would be to review the:

- ☐ request for proposal (RFP).
- ☐ feasibility study.
- ☐ alignment with IT strategy.
- ☐ business case.

Licensed to Berend Post berend.post@it-university.nl

Question 1592

Controls related to authorized modifications to production programs are BEST tested by:

- ☐ testing only the authorizations to implement the new program.
- ☐ tracing modifications from the executable program back to the original request for change.
- ☐ reviewing only the actual lines of source code changed in the program.
- ☐ tracing modifications from the original request for change forward to the executable program.

Question 1593

An organization is migrating from a legacy system to an enterprise resource planning (ERP) system. While reviewing the data migration activity, the MOST important concern for the IS auditor is to determine that there is a:

- ☐ correlation of semantic characteristics of the data migrated between the two systems.
- ☐ correlation of arithmetic characteristics of the data migrated between the two systems.
- ☐ correlation of functional characteristics of the processes between the two systems.
- ☐ relative efficiency of the processes between the two systems.

Question 1594

Which of the following is the MOST reliable control to prevent double payments made as a result of payment system batch jobs restarting after processing errors?

- ☐ Database rollback in case of processing errors
- ☐ Review of batch job competition logs
- ☐ Duplicate verification at the last possible point in processing
- ☐ Restart procedures integrated in job controls

Question 1595

Which of the following is MOST likely to result from a business process reengineering (BPR) project?

- ☐ An increased number of people using technology
- ☐ Significant cost savings, through a reduction in the complexity of information technology
- ☐ A weaker organizational structures and less accountability
- ☐ Increased information protection (IP) risk will increase

Licensed to Berend Post berend.post@it-university.nl

Question 1596

A database administrator has detected a performance problem with some tables which could be solved through denormalization. This situation will increase the risk of:

- ☐ concurrent access.
- ☐ deadlocks.
- ☐ unauthorized access to data.
- ☐ a loss of data integrity.

Question 1597

Which of the following would be the FIRST step to help ensure the necessary regulatory requirements are addressed in an organization's cross-border data protection policy?

- ☐ Conduct a risk assessment
- ☐ Perform a gap analysis
- ☐ Conduct stakeholder interviews
- ☐ Perform a business impact analysis

Question 1598

What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

- ☐ Test data/deck
- ☐ Base-case system evaluation
- ☐ Integrated test facility (ITF)
- ☐ Parallel simulation

Question 1599

A programmer maliciously modified a production program to change data and then restored the original code. Which of the following would MOST effectively detect the malicious activity?

- ☐ Comparing source code
- ☐ Reviewing system log files
- ☐ Comparing object code
- ☐ Reviewing executable and source code integrity

Licensed to Berend Post berend.post@it-university.nl

Question 1600

An organization implemented a mandatory information security awareness training program a year ago. What is the BEST way to determine its effectiveness?

- ☐ Analyze responses from an employee survey on training satisfaction.
- ☐ Analyze results from training completion reports.
- ☐ Analyze results of a social engineering test.
- ☐ Analyze findings from previous audit reports.

Question 1601

An IS auditor reviewing the risk assessment process of an organization should FIRST:

- ☐ identify the reasonable threats to the information assets.
- ☐ analyze the technical and organizational vulnerabilities.
- ☐ identify and rank the information assets.
- ☐ evaluate the effect of a potential security breach.

Question 1602

A previously agreed-upon recommendation was not implemented because the auditee no longer agrees with the original findings. The IS auditor's FIRST course of action should be to:

- ☐ exclude the finding in the follow-up audit report.
- ☐ escalate the disagreement to the audit committee.
- ☐ assess the reason for the disagreement.
- ☐ require implementation of the original recommendation.

Question 1603

Internal audit reports should be PRIMARILY written for and communicated to:

- ☐ audit management, as they are responsible for the quality of the audit.
- ☐ external auditors, as they provide an opinion on the financial statements.
- ☐ auditees, as they will eventually have to implement the recommendations.
- ☐ senior management, as they should be informed about the identified risks.

Question 1604

Which of the following is the MOST important reason to use statistical sampling?

- ☐ The results are more defensible
- ☐ It ensures that all relevant cases are covered
- ☐ It reduces time required for testing
- ☐ The results can reduce error rates

Licensed to Berend Post berend.post@it-university.nl

Question 1605

An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

- ☐ Evidence collected through personal observation
- ☐ Evidence collected through systems logs provided by the organization's security administration
- ☐ Evidence collected through surveys collected from internal staff
- ☐ Evidence collected through transaction reports provided by the organization's IT administration

Question 1606

An organization's information security department is creating procedures for handling digital evidence that may be used in court. Which of the following would be the MOST important consideration from a risk standpoint?

- ☐ Ensuring the entire security team reviews the evidence
- ☐ Ensuring that analysis is conducted on the original data
- ☐ Ensuring the original data is kept confidential
- ☐ Ensuring the integrity of the data is preserved

Question 1607

Which of the following user profiles should be of MOST concern to an IS auditor when performing an audit of an EFT system?

- ☐ Three users with the ability to capture and verify their own messages
- ☐ Five users with the ability to capture and send their own messages
- ☐ Five users with the ability to verify other users and to send their own messages
- ☐ Three users with the ability to capture and verify the messages of other users and to send their own messages

Question 1608

Which of the following is the GREATEST concern with conducting penetration testing on an internally developed application in the production environment?

- ☐ The testing could create application availability issues.
- ☐ The testing may identify only known operating system vulnerabilities.
- ☐ The issues identified during the testing may require significant remediation efforts.
- ☐ Internal security staff may not be qualified to conduct application penetration testing.

Licensed to Berend Post berend.post@it-university.nl

Question 1609

During an application audit, an IS auditor finds several problems related to corrupted data in the database. Which of the following is a corrective control that the IS auditor should recommend?

- ☐ implement data backup and recovery procedures.
- ☐ Define standards and closely monitor for compliance.
- ☐ Ensure that only authorized personnel can update the database.
- ☐ Establish controls to handle concurrent access problems.

Question 1610

An IS auditor finds that a mortgage origination team receives customer mortgage applications via a shared repository. Which of the following test procedures is the BEST way to assess whether there are adequate privacy controls over this process?

- ☐ Validate whether the encryption is compliant with the organization's requirements.
- ☐ Validate that data is entered accurately and timely.
- ☐ Validate whether documents are deleted according to data retention procedures.
- ☐ Validate whether complex passwords are required.

Question 1611

The GREATEST benefit of using a prototyping approach in software development is that it helps to:

- ☐ decrease the time allocated for user testing and review
- ☐ minimize scope changes to the system
- ☐ conceptualize and clarify requirements
- ☐ improve efficiency of quality assurance (QA) testing

Question 1612

An organization globally distributes a free phone application that includes a module to gather and report user information. The application includes a privacy notice alerting users to the data gathering. Which of the following presents the GREATEST risk?

- ☐ The data gathering notice is available in only one language.
- ☐ There is no framework to delete personal data.
- ☐ There may be a backlash among users when the data gathering is revealed.
- ☐ The data is not properly encrypted on the application server.

Licensed to Berend Post berend.post@it-university.nl

Question 1613

The initial step in establishing an information security program is the:

- ☐ development and implementation of an information security standards manual.
- ☐ performance of a comprehensive security control review by the IS auditor.
- ☐ adoption of a corporate information security policy statement.
- ☐ purchase of security access control software.

Question 1614

The MOST effective method for an IS auditor to determine which controls are functioning in an operating system is to:

- ☐ compare the current configuration to the corporate standard.
- ☐ consult with the systems programmer.
- ☐ consult with the vendor of the system.
- ☐ compare the current configuration to the default configuration.

Question 1615

Which of the following would be MOST useful for determining whether the goals of IT are aligned with the organization's goals?

- ☐ Balanced scorecard
- ☐ Enterprise architecture
- ☐ Key performance indicators
- ☐ Enterprise dashboard

Question 1616

Which of the following procedures would BEST contribute to the reliability of information in a data warehouse?

- ☐ Retaining only current data
- ☐ Storing only a single type of data
- ☐ Maintaining archive data
- ☐ Maintaining current metadata

Question 1617

A maturity model can be used to aid the implementation of IT governance by identifying:

- ☐ critical success factors (CSF)
- ☐ performance drivers
- ☐ improvement opportunities
- ☐ accountabilities

Licensed to Berend Post berend.post@it-university.nl

Question 1618

Which of the following should be used to assess the level of security required to protect information on a corporate network?

- ☐ Data classification
- ☐ Business intelligence
- ☐ Access rights
- ☐ Access control matrix

Question 1619

Iptables is based on which of the following frameworks?

- ☐ Netfilter
- ☐ NetDoom
- ☐ NetCheck
- ☐ NetSecure
- ☐ None of the choices.

Question 1620

An IS auditor finds that application servers had inconsistent configurations leading to potential security vulnerabilities. Which of the following should the auditor recommend FIRST?

- ☐ Enforce server baseline standards.
- ☐ Improve change management processes using a workflow tool.
- ☐ Hold the application owner accountable for monitoring metrics.
- ☐ Use a single vendor for the application servers.

Question 1621

Which of the following controls should be implemented to BEST minimize system downtime for maintenance?

- ☐ Nightly full backups
- ☐ Virtualization
- ☐ Warm site
- ☐ Clustering

Licensed to Berend Post berend.post@it-university.nl

Question 1622

An organization's audit charter should:

- ☐ set the enterprise strategic direction.
- ☐ detail the audit objectives.
- ☐ define the auditors' right to access information.
- ☐ include the IS audit plan.

Question 1623

Which of the following would provide the highest degree of server access control?

- ☐ A mantrap-monitored entryway to the server room
- ☐ Host-based intrusion detection combined with CCTV
- ☐ Network-based intrusion detection
- ☐ A fingerprint scanner facilitating biometric access control

Question 1624

An organization has outsourced its wide area network (WAN) to a third-party service provider. Under these circumstances, which of the following is the PRIMARY task the IS auditor should perform during an audit of business continuity (BCP) and disaster recovery planning (DRP)?

- ☐ Review whether the service provider's BCP process is aligned with the organization's BCP and contractual obligations.
- ☐ Review whether the service level agreement (SLA) contains a penalty clause in case of failure to meet the level of service in case of a disaster.
- ☐ Review the methodology adopted by the organization in choosing the service provider.
- ☐ Review the accreditation of the third-party service provider's staff.

Question 1625

During the review of a business process reengineering project, the PRIMARY concern of an IS auditor is to determine whether the new business model:

- ☐ is aligned with industry best practices.
- ☐ is aligned with organizational goals.
- ☐ leverages benchmarking results.
- ☐ meets its key performance measures.

Licensed to Berend Post berend.post@it-university.nl

Question 1626

Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

- ☐ The preservation of the chain of custody for electronic evidence
- ☐ Time and cost savings
- ☐ Efficiency and effectiveness
- ☐ Ability to search for violations of intellectual property rights

Question 1627

What should be the GREATEST concern to an IS auditor when employees use portable media (MP3 players, flash drives)?

- ☐ The copying of sensitive data on them
- ☐ The copying of songs and videos on them
- ☐ The cost of these devices multiplied by all the employees could be high
- ☐ They facilitate the spread of malicious code through the corporate network

Question 1628

A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server. Which of the following would MOST effectively allow the hospital to avoid paying the ransom?

- ☐ A continual server replication process
- ☐ A property tested offline backup system
- ☐ A property configured firewall
- ☐ Employee training on ransomware

Question 1629

Which of the following represents the GREATEST risk created by a reciprocal agreement for disaster recovery made between two companies?

- ☐ Developments may result in hardware and software incompatibility.
- ☐ Resources may not be available when needed.
- ☐ The recovery plan cannot be tested.
- ☐ The security infrastructures in each company may be different.

Licensed to Berend Post berend.post@it-university.nl

Question 1630

In a high-volume, real-time system, the MOST effective technique by which to continuously monitor and analyze transaction processing is:

- ☐ integrated test facility (ITF).
- ☐ embedded audit modules.
- ☐ parallel simulation.
- ☐ transaction tagging.

Question 1631

Who is responsible for ensuring that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures?

- ☐ Project Sponsor
- ☐ Security Officer
- ☐ User Management
- ☐ Senior Management

Question 1632

Which of the following type of testing uses a set of test cases that focus on control structure of the procedural design?

- ☐ Interface testing
- ☐ Unit Testing
- ☐ System Testing
- ☐ Final acceptance testing

Question 1633

Functional acknowledgements are used:

- ☐ as an audit trail for EDI transactions.
- ☐ to functionally describe the IS department.
- ☐ to document user roles and responsibilities.
- ☐ as a functional description of application software.

Licensed to Berend Post berend.post@it-university.nl

Question 1634

Which of the following backup techniques is the MOST appropriate when an organization requires extremely granular data restore points, as defined in the recovery point objective (RPO)?

- ☐ Virtual tape libraries
- ☐ Disk-based snapshots
- ☐ Continuous data backup
- ☐ Disk-to-tape backup

Question 1635

A hub is a device that connects:

- ☐ two LANs using different protocols.
- ☐ a LAN with a WAN.
- ☐ a LAN with a metropolitan area network (MAN).
- ☐ two segments of a single LAN.

Question 1636

As IS auditor discovers that due to resource constraints, a database administrator (DBA) is responsible for developing and executing changes into the production environment. Which of the following should the auditor do FIRST?

- ☐ Identify whether any compensating controls exist
- ☐ Report a potential segregation of duties (SoD) violation
- ☐ Determine whether another database administrator could make the changes
- ☐ Ensure a change management process is followed prior to implementation

Question 1637

Authentication techniques for sending and receiving data between EDI systems is crucial to prevent which of the following?

- ☐ Unsynchronized transactions
- ☐ Unauthorized transactions
- ☐ Inaccurate transactions
- ☐ Incomplete transactions

Licensed to Berend Post berend.post@it-university.nl

Question 1638

The GREATEST risk of database denormalization is:

- ☐ decreased performance.
- ☐ loss of data confidentiality.
- ☐ loss of database integrity.
- ☐ incorrect metadata.

Question 1639

The IS auditor has identified a potential fraud perpetrated by the network administrator. The IS auditor should:

- ☐ issue a report to ensure a timely resolution
- ☐ review the audit finding with the audit committee prior to any other discussions
- ☐ perform more detailed tests prior to disclosing the audit results
- ☐ share the potential audit finding with the security administrator

Question 1640

Which of the following provides the best evidence of the adequacy of a security awareness program?

- ☐ The number of stakeholders including employees trained at various levels
- ☐ Coverage of training at all locations across the enterprise
- ☐ The implementation of security devices from different vendors
- ☐ Periodic reviews and comparison with best practices

Question 1641

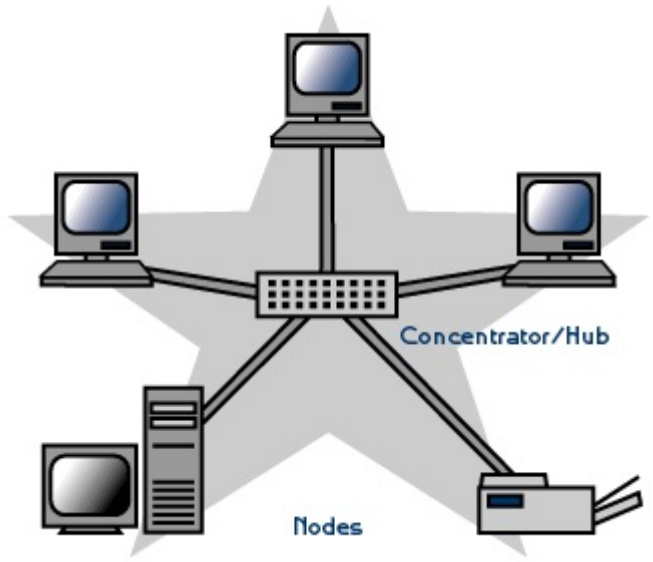
In which of the following database models is the data represented in terms of tulles and grouped into relations?

- ☐ Hierarchical database model
- ☐ Network database model
- ☐ Relational database model
- ☐ Object-relational database model

Licensed to Berend Post berend.post@it-university.nl

Question 1642

Identify the network topology from below diagram presented below:



Network Topology

- ☐ Bus
- ☐ Star
- ☐ Ring
- ☐ Mesh

Question 1643

Identify the payment model from description presented below:
A users write an electronic check, which is digitally signed with instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

- ☐ Electronic Money Model
- ☐ Electronics Checks model
- ☐ Electronic transfer model
- ☐ Electronic withdraw model

Question 1644

An organization is deciding whether to outsource its customer relationship management systems to a provider located in another country. Which of the following should be the PRIMARY influence in the outsourcing decision?

- ☐ Time zone differences
- ☐ The service provider’s disaster recovery plan
- ☐ Cross-border privacy laws
- ☐ Current geopolitical conditions

Licensed to Berend Post berend.post@it-university.nl

Question 1645

When should systems administrators first assess the impact of applications or systems patches?

- ☐ Within five business days following installation
- ☐ Prior to installation
- ☐ No sooner than five business days following installation
- ☐ Immediately following installation

Question 1646

A design company has multiple name and address files for its customers in several of its independent systems. Which of the following is the BEST control to ensure that the customer name and address agree across all files?

- ☐ Use of hash totals on customer records
- ☐ Periodic review of each master file by management
- ☐ Matching of records and review of exception reports
- ☐ Use of authorized master file change forms

Question 1647

An IS steering committee should:

- ☐ include a mix of members from different departments and staff levels.
- ☐ ensure that IS security policies and procedures have been executed properly.
- ☐ have formal terms of reference and maintain minutes of its meetings.
- ☐ be briefed about new trends and products at each meeting by a vendor.

Question 1648

Which of the following will BEST protect an organization against spear phishing?

- ☐ Email content filtering
- ☐ Acceptable use policy
- ☐ End-user training
- ☐ Antivirus software

Question 1649

Which type of control is being implemented when a biometric access device is installed at the entrance to a facility?

- ☐ Preventive
- ☐ Deterrent
- ☐ Corrective
- ☐ Detective

Licensed to Berend Post berend.post@it-university.nl

Question 1650

An IS auditor is assessing risk associated with peer-to-peer file sharing within an organization. Which of the following should be of GREATEST concern?

- ☐ File-sharing policies have not been reviewed since last year
- ☐ Only some employees are required to attend security awareness training
- ☐ Not all devices are running antivirus programs
- ☐ The organization does not have an efficient patch management process

Question 1651

Who is responsible for providing adequate physical and logical security for IS program, data and equipment?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☐ Security Administrator

Question 1652

When developing a risk management program, what is the FIRST activity to be performed?

- ☐ Threat assessment
- ☐ Classification of data
- ☐ Inventory of assets
- ☐ Criticality analysis

Question 1653

Which of the following ISO/OSI layers performs transformations on data to provide a standardized application interface and to provide common communication services such as encryption?

- ☐ Application layer
- ☐ Session layer
- ☐ Presentation layer
- ☐ Transport layer

Question 1654

Who is responsible for implementing cost-effective controls in an automated system?

- ☐ Security policy administrators
- ☐ Business unit management
- ☐ Senior management
- ☐ Board of directors

Licensed to Berend Post berend.post@it-university.nl

Question 1655

Which of the following is the PRIMARY risk when business units procure IT assets without IT involvement?

- ☐ Corporate procurement standards are not followed.
- ☐ The business units want IT to be responsible for maintenance costs.
- ☐ Data security requirements are not considered.
- ☐ System inventory becomes inaccurate.

Question 1656

Network Data Management Protocol (NDMP) technology should be used for backup if:

- ☐ a network attached storage (NAS) appliance is required.
- ☐ the use of TCP/I P must be avoided.
- ☐ file permissions that can not be handled by legacy backup systems must be backed up.
- ☐ backup consistency over several related data volumes must be ensured.

Question 1657

An IT steering committee should review information systems PRIMARILY to assess:

- ☐ whether IT processes support business requirements.
- ☐ if proposed system functionality is adequate
- ☐ the stability of existing software.
- ☐ the complexity of installed technology.

Question 1658

Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?

- ☐ Field checks
- ☐ Control totals
- ☐ Reasonableness checks
- ☐ A before-and-after maintenance report

Question 1659

Which of the following would be a result of utilizing a top-down maturity model process?

- ☐ A means of benchmarking the effectiveness of similar processes with peers
- ☐ Identification of older, more established processes to ensure timely review
- ☐ Identification of processes with the most improvement opportunities
- ☐ A means of comparing the effectiveness of other processes within the enterprise

Licensed to Berend Post berend.post@it-university.nl

Question 1660

Which of the following is the PRIMARY responsibility of an organization's information security function?

- ☐ Reviewing unauthorized attempts to access sensitive files
- ☐ Managing the organization's security procedures
- ☐ Approving access to data files
- ☐ Installing network security programs

Question 1661

Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits vulnerability in a protocol?

- ☐ Install the vendor's security fix for the vulnerability.
- ☐ Block the protocol traffic in the perimeter firewall.
- ☐ Block the protocol traffic between internal network segments.
- ☐ Stop the service until an appropriate security fix is installed.

Question 1662

Which of the following type of lock uses a magnetic or embedded chip based plastic card key or token entered into a sensor/reader to gain access?

- ☐ Bolting door locks
- ☐ Combination door lock
- ☐ Electronic door lock
- ☐ Biometric door lock

Question 1663

Which of the following would be MOST critical for an IS auditor to look for when evaluating fire precautions in a manned data center located in the upper floor of a multi-story building?

- ☐ Existence of handheld fire extinguishers in highly visible locations
- ☐ Documentation of regular inspections by the local fire department
- ☐ Adequacy of the HVAC system throughout the facility
- ☐ Documentation of tested emergency evacuation plans

Licensed to Berend Post berend.post@it-university.nl

Question 1664

Which of the following layer of an enterprise data flow architecture is responsible for data copying, transformation in Data Warehouse (DW) format and quality control?

- ☐ Data Staging and quality layer
- ☐ Desktop Access Layer
- ☐ Data Mart layer
- ☐ Data access layer

Question 1665

When should application controls be considered within the system-development process?

- ☐ After application unit testing
- ☐ After application module testing
- ☐ After applications systems testing
- ☐ As early as possible, even in the development of the project's functional specifications

Question 1666

The quality assurance (QA) function should be prevented from:

- ☐ developing naming conventions.
- ☐ establishing analysis techniques.
- ☐ amending review procedures.
- ☐ changing programs for business functions.

Question 1667

Which of the following BEST determines if a batch update job was completed?

- ☐ Reviewing the job log
- ☐ Testing a sample of transactions
- ☐ Reviewing a copy of the script
- ☐ Obtaining process owner confirmation

Question 1668

What is an IS auditor's BEST recommendation for management if a network vulnerability assessment confirms that critical patches have not been applied since the last assessment?

- ☐ Implement a process to test and apply appropriate patches.
- ☐ Apply available patches and continue periodic monitoring.
- ☐ Configure servers to automatically apply available patches.
- ☐ Remove unpatched devices from the network.

Licensed to Berend Post berend.post@it-university.nl

Question 1669

Which of the following is the BEST type of backup to minimize the associated time and media?

- ☐ Differential
- ☐ Incremental
- ☐ Mirror
- ☐ Compressed full

Question 1670

An offsite information processing facility:

- ☐ should have the same amount of physical access restrictions as the primary processing site.
- ☐ should be easily identified from the outside so that, in the event of an emergency, it can be easily found.
- ☐ should be located in proximity to the originating site, so it can quickly be made operational.
- ☐ need not have the same level of environmental monitoring as the originating site.

Question 1671

Following a security breach in which a hacker exploited a well-known vulnerability in the domain controller, an IS auditor has been asked to conduct a control assessment. The auditor's BEST course of action would be to determine if:

- ☐ the domain controller was classified for high availability.
- ☐ the network traffic was being monitored.
- ☐ the patches were updated.
- ☐ the logs were monitored.

Question 1672

An IS auditor is evaluating the security of an organization's data backup process, which includes the transmission of daily incremental backups to a dedicated offsite server. Which of the following findings poses the GREATEST risk to the organization?

- ☐ Backup transmissions are not encrypted
- ☐ Backup transmissions occasionally fail
- ☐ Data recovery testing is conducted once per year
- ☐ The archived data log is incomplete

Licensed to Berend Post berend.post@it-university.nl

Question 1673

An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

- ☐ Availability of online network documentation
- ☐ Support of terminal access to remote hosts
- ☐ Handling file transfer between hosts and interuser communications
- ☐ Performance management, audit and control

Question 1674

The directory system of a database-management system describes:

- ☐ The access method to the data
- ☐ The location of data AND the access method
- ☐ The location of data
- ☐ Neither the location of data NOR the access method

Question 1675

Phishing attack works primarily through:

- ☐ email and hyperlinks
- ☐ SMS
- ☐ chat
- ☐ email attachment
- ☐ news
- ☐ file download
- ☐ None of the choices.

Question 1676

Which of the following is the BEST preventative control to protect the confidentiality of data on a corporate smartphone in the event it is lost?

- ☐ Encryption of the data stored on the device
- ☐ Biometric authentication for the device
- ☐ Password for device authentication
- ☐ Remote data wipe program

Licensed to Berend Post berend.post@it-university.nl

Question 1677

Which of the following layer of an OSI model ensures that messages are delivered error-free, in sequence, and with no losses or duplications?

- ☐ Application layer
- ☐ Presentation layer
- ☐ Session layer
- ☐ Transport layer

Question 1678

The objective of concurrency control in a database system is to:

- ☐ restrict updating of the database to authorized users.
- ☐ prevent integrity problems when two processes attempt to update the same data at the same time.
- ☐ prevent inadvertent or unauthorized disclosure of data in the database.
- ☐ ensure the accuracy, completeness and consistency of data.

Question 1679

Which policy helps an auditor to gain a better understanding of biometrics system in an organization?

- ☐ BIMS Policy
- ☐ BOMS Policy
- ☐ BMS Policy
- ☐ BOS Policy

Question 1680

Who is mainly responsible for protecting information assets they have been entrusted with on a daily basis by defining who can access the data, it's sensitivity level, type of access, and adhering to corporate information security policies?

- ☐ Data Owner
- ☐ Security Officer
- ☐ Senior Management
- ☐ End User

Licensed to Berend Post berend.post@it-university.nl

Question 1681

The PRIMARY purpose of asset valuation for the management of information security is to:

- ☐ eliminate the least significant assets.
- ☐ provide a basis for asset classification.
- ☐ determine the value of each asset.
- ☐ prioritize risk management activities.

Question 1682

Which of the following is an effective method for controlling downloading of files via FTP?

- ☐ An application-layer gateway, or proxy firewall, but not stateful inspection firewalls
- ☐ An application-layer gateway, or proxy firewall
- ☐ A circuit-level gateway
- ☐ A first-generation packet-filtering firewall

Question 1683

During an audit of information security procedures of a large retailer's online store, an IS auditor notes that operating system (OS) patches are automatically deployed upon release. Which of the following should be of GREATEST concern to the auditor?

- ☐ Patches are in conflict with current licensing agreements.
- ☐ Patches are pushed from the vendor increasing Internet traffic.
- ☐ Patches are not reflected in the configuration management database.
- ☐ Patches are not tested before installation on critical servers.

Question 1684

Identify the correct sequence which needs to be followed as a chain of event in regards to evidence handling in computer forensics?

- ☐ Identify, Analyze, preserve and Present
- ☐ Analyze, Identify, preserve and present
- ☐ Preserve, Identify, Analyze and Present
- ☐ Identify, Preserve, Analyze and Present

Licensed to Berend Post berend.post@it-university.nl

Question 1685

When developing an incident response plan, the information manager should:

- ☐ allow IT to decide which systems can be removed from the infrastructure
- ☐ include response scenarios that have been approved previously by business management
- ☐ require IT to invoke the business continuity plan
- ☐ determine recovery time objectives (RTOs)

Question 1686

Which of the following control fixes a component or system after an incident has occurred?

- ☐ Deterrent
- ☐ Preventive
- ☐ Corrective
- ☐ Recovery

Question 1687

Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

- ☐ Apply single sign-on for access control.
- ☐ Enforce an internal data access policy.
- ☐ Enforce the use of digital signatures.
- ☐ Implement segregation of duties.

Question 1688

Which of the following cloud computing service model is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components?

- ☐ Software as a service
- ☐ Data as a service
- ☐ Platform as a service
- ☐ Infrastructure as a service

Licensed to Berend Post berend.post@it-university.nl

Question 1689

An organization is concerned about duplicate vendor payments on a complex system with a high volume of transactions. Which of the following would be MOST helpful to an IS auditor to determine whether duplicate vendor payments exist?

- ☐ Computer-assisted technique
- ☐ Stop-and-go testing
- ☐ Statistical sampling
- ☐ Judgmental sampling

Question 1690

Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

- ☐ Paper test
- ☐ Post test
- ☐ Preparedness test
- ☐ Walk-through

Question 1691

During an audit, the client learns that the IS auditor has recently completed a similar security review at a competitor. The client inquires about the competitor's audit results. What is the BEST way for the auditor to address this inquiry?

- ☐ Explain that it would be inappropriate to discuss the results of another audit client.
- ☐ Escalate the question to the audit manager for further action.
- ☐ Discuss the results of the audit omitting specifics related to names and products.
- ☐ Obtain permission from the competitor to use the audit results as examples for future clients.

Question 1692

When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

- ☐ sufficient evidence will be collected.
- ☐ all significant deficiencies identified will be corrected within a reasonable period.
- ☐ all material weaknesses will be identified.
- ☐ audit costs will be kept at a minimum level.

Licensed to Berend Post berend.post@it-university.nl

Question 1693

Which of the following types of attack makes use of unfiltered user input as the format string parameter in the print () function of the C language?

- ☐ buffer overflows
- ☐ format string vulnerabilities
- ☐ integer overflow
- ☐ code injection
- ☐ command injection
- ☐ None of the choices.

Question 1694

Which of the following provides the BEST evidence of an organization's disaster recovery readiness?

- ☐ A disaster recovery plan
- ☐ Customer references for the alternate site provider
- ☐ Processes for maintaining the disaster recovery plan
- ☐ Results of tests and drills

Question 1695

During a post-incident review. the sequence and correlation of actions must be analyzed PRIMARLY based on:

- ☐ interviews with personnel
- ☐ a consolidated event time line
- ☐ logs from systems involved
- ☐ documents created during the incident

Question 1696

The MOST significant security concerns when using flash memory (e.g., USB removable disk) is that the:

- ☐ contents are highly volatile.
- ☐ data cannot be backed up.
- ☐ data can be copied.
- ☐ device may not be compatible with other peripherals.

Licensed to Berend Post berend.post@it-university.nl

Question 1697

Which of the following is the MOST important part of an incident response plan?

- ☐ Recovery point objective (RPO)
- ☐ Recovery time objective (RTO)
- ☐ Mean time to report (MTR)
- ☐ Business impact analysis (BIA)

Question 1698

A start-up organization wants to develop a data loss prevention program (DLP). The FIRST step should be to implement:

- ☐ data encryption.
- ☐ access controls.
- ☐ data classification.
- ☐ security awareness training.

Question 1699

In a cloud technology environment, which of the following would pose the GREATESTchallenge to the investigation of security incidents?

- ☐ Data encryption
- ☐ Access to the hardware
- ☐ Compressed customer data
- ☐ Non-standard event logs

Question 1700

Which of the following is a general operating system access control function?

- ☐ Creating database profiles
- ☐ Verifying user authorization at a field level
- ☐ Creating individual accountability
- ☐ Logging database access activities for monitoring access violation

Question 1701

Which of the following should be of GREATEST concern to an IS auditor when evaluating a new system's production readiness?

- ☐ A system defect was found during user acceptance testing.
- ☐ Functional design documentation is not complete.
- ☐ Functional requirements have not been met.
- ☐ Projected benefits have not been realized.

Licensed to Berend Post berend.post@it-university.nl

Question 1702

A security administrator should have read-only access for which of the following?

- ☐ Router configuration
- ☐ Password policy
- ☐ Security logs
- ☐ Services/daemons configuration

Question 1703

In an IT organization where many responsibilities are shared, which of the following would be the BEST control for detecting unauthorized data changes?

- ☐ Data changes are independently reviewed by another group.
- ☐ Users are required to periodically rotate responsibilities.
- ☐ Segregation of duties conflicts are periodically reviewed.
- ☐ Data changes are logged in an outside application.

Question 1704

The PRIMARY responsibility of a project steering committee is to:

- ☐ ensure that each project deadline is met
- ☐ undertake final acceptance of the system for implementation
- ☐ ensure that systems developed meet business needs
- ☐ provide day-to-day guidance and oversight

Question 1705

A web application is developed in-house by an organization. Which of the following would provide the BEST evidence to an IS auditor that the application is secure from external attack?

- ☐ Penetration test results
- ☐ Database application monitoring logs
- ☐ Code review by a third party
- ☐ Web application firewall implementation

Licensed to Berend Post berend.post@it-university.nl

Question 1706

What is the BEST way for an IS auditor to address the risk associated with over-retention of personal data after identifying a large number of customer records retained beyond the retention period defined by law?

- ☐ Recommend automating deletion of records beyond the retention period.
- ☐ Schedule regular internal audits to identify records for deletion.
- ☐ Report the retention period noncompliance to the regulatory authority.
- ☐ Escalate the over-retention issue to the data privacy officer for follow-up.

Question 1707

Which of the following would MOST effectively reduce social engineering incidents?

- ☐ Security awareness training
- ☐ increased physical security measures
- ☐ E-mail monitoring policy
- ☐ intrusion detection systems

Question 1708

During development of an information security policy, which of the following would BEST ensure alignment to business objectives?

- ☐ Incorporation of industry best practices
- ☐ Linkage between policy and procedures
- ☐ Use of a balanced scorecard
- ☐ Input from relevant stakeholders

Question 1709

The objective of using coding standards for systems development is to:

- ☐ facilitate program maintenance.
- ☐ facilitate user testing.
- ☐ ensure the completeness of requirements.
- ☐ ensure that business needs are met.

Licensed to Berend Post berend.post@it-university.nl

Question 1710

When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

- ☐ Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.
- ☐ Reviewing an audit client's business plan should be performed after reviewing an organization's IT strategic plan.
- ☐ Reviewing an audit client's business plan should be performed during the review of an organization's IT strategic plan.
- ☐ Reviewing an audit client's business plan should be performed without regard to an organization's IT strategic plan.

Question 1711

Which of the following is MOST important for successful incident response?

- ☐ The timeless of attack recognition
- ☐ The ability to trace the source of the attack
- ☐ The quantity of data logged by the attack control tools
- ☐ Blocking the attack route immediately

Question 1712

Identify the correct sequence of Business Process Reengineering (BPR) benchmarking process from the given choices below?

- ☐ PLAN, RESEARCH, OBSERVE, ANALYZE, ADOPT and IMPROVE
- ☐ OBSERVE, PLAN, RESEACH, ANALYZE, ADOPT and IMPROVE
- ☐ PLAN, OBSERVE, RESEARCH, ANALYZE, ADOPT and IMPROVE
- ☐ PLAN, RESEARCH, ANALYZE, OBSERVE, ADOPT and IMPROVE

Question 1713

Which of the following processes are performed during the design phase of the systems development life cycle (SDLC) model?

- ☐ Develop test plans.
- ☐ Baseline procedures to prevent scope creep.
- ☐ Define the need that requires resolution, and map to the major requirements of the solution.
- ☐ Program and test the new system. The tests verify and validate what has been developed.

Licensed to Berend Post berend.post@it-university.nl

Question 1714

Which of the following is MOST important for an IS auditor to ensure is included in a global organization's online data privacy notification to customers?

- ☐ Consequences to the organization for mishandling the data
- ☐ Consent terms including the purpose of data collection
- ☐ Contact information for reporting violations of consent
- ☐ Industry standards for data breach notification

Question 1715

What is often assured through table link verification and reference checks?

- ☐ Database integrity
- ☐ Database synchronization
- ☐ Database normalcy
- ☐ Database accuracy

Question 1716

Network ILD&P are typically installed:

- ☐ on the organization's internal network connection.
- ☐ on the organization's internet network connection.
- ☐ on each end user stations.
- ☐ on the firewall.
- ☐ None of the choices.

Question 1717

The MOST likely explanation for a successful social engineering attack is:

- ☐ that computers make logic errors.
- ☐ that people make judgment errors.
- ☐ the computer knowledge of the attackers.
- ☐ the technological sophistication of the attack method.

Question 1718

An organization has outsourced its help desk. Which of the following indicators would be the best to include in the SLA?

- ☐ Overall number of users supported
- ☐ Percentage of incidents solved in the first call
- ☐ Number of incidents reported to the help desk
- ☐ Number of agents answering the phones

Licensed to Berend Post berend.post@it-university.nl

Question 1719

Following a recent internal data breach, an IS auditor was asked to evaluate information security practices within the organization. Which of the following findings would be MOST important to report to senior management?

- ☐ Employees are not required to sign a non-compete agreement.
- ☐ Security education and awareness workshops have not been completed.
- ☐ Users lack technical knowledge related to security and data protection.
- ☐ Desktop passwords do not require special characters.

Question 1720

Which of the following are used in a firewall to protect the entity's internal resources?

- ☐ Internet Protocol (IP) address restrictions
- ☐ Remote access servers
- ☐ Secure Sockets Layers (SSLs)
- ☐ Fail-over services

Question 1721

Which of the following is the BEST methodology to use for estimating the complexity of developing a large business application?

- ☐ Function point analysis
- ☐ Software cost estimation
- ☐ Work breakdown structure
- ☐ Critical path analysis

Question 1722

Time constraints and expanded needs have been found by an IS auditor to be the root causes for recent violations of corporate data definition standards in a new business intelligence project. Which of the following is the MOST appropriate suggestion for an auditor to make?

- ☐ Achieve standards alignment through an increase of resources devoted to the project
- ☐ Align the data definition standards after completion of the project
- ☐ Delay the project until compliance with standards can be achieved
- ☐ Enforce standard compliance by adopting punitive measures against violators

Licensed to Berend Post berend.post@it-university.nl

Question 1723

Which of the following is the MOST effective way for an organization to ensure its third-party service providers are aware of information security requirements and expectations?

- ☐ Providing information security training to third-party personnel
- ☐ Auditing the service delivery of third-party providers
- ☐ Inducting information security clauses within contracts
- ☐ Requiring third parties to sign confidentiality agreements

Question 1724

Which of the following layer in in an enterprise data flow architecture is directly death with by end user with information?

- ☐ Desktop access layer
- ☐ Data preparation layer
- ☐ Data mart layer
- ☐ Data access layer

Question 1725

An IS auditor is reviewing a contract for the outsourcing of IT facilities. If missing, which of the following should present the GREATEST concern to the auditor?

- ☐ Access control requirements
- ☐ Hardware configurations
- ☐ Perimeter network security diagram
- ☐ Help desk availability

Question 1726

To ensure an organization is complying with privacy requirements, an IS auditor should FIRST review:

- ☐ the IT infrastructure.
- ☐ organizational policies, standards and procedures.
- ☐ legal and regulatory requirements.
- ☐ the adherence to organizational policies, standards and procedures.

Licensed to Berend Post berend.post@it-university.nl

Question 1727

An organization has been recently downsized, in light of this, an IS auditor decides to test logical access controls. The IS auditor's PRIMARY concern should be that:

- ☐ all system access is authorized and appropriate for an individual's role and responsibilities.
- ☐ management has authorized appropriate access for all newly-hired individuals.
- ☐ only the system administrator has authority to grant or modify access to individuals.
- ☐ access authorization forms are used to grant or modify access to individuals.

Question 1728

The GREATEST benefit of risk-based auditing is that it:

- ☐ demonstrates compliance with regulatory requirements.
- ☐ enables alignment of resources to significant risk areas.
- ☐ allows an organization to identify and eliminate low-risk areas.
- ☐ identifies problem areas within an organization.

Question 1729

At what point in software development should the user acceptance test plan be prepared?

- ☐ Implementation planning
- ☐ Requirements definition
- ☐ Transfer into production
- ☐ Feasibility study

Question 1730

During an audit of a financial application, it was determined that many terminated users' accounts were not disabled. Which of the following should be the IS auditor's NEXT step?

- ☐ Perform a review of terminated users' account activity.
- ☐ Conclude that IT general controls are ineffective.
- ☐ Communicate risks to the application owner.
- ☐ Perform substantive testing of terminated users' access rights.

Licensed to Berend Post berend.post@it-university.nl

Question 1731

What are trojan horse programs?

- ☐ A common form of internal attack
- ☐ Malicious programs that require the aid of a carrier program such as email
- ☐ Malicious programs that can run independently and can propagate without the aid of a carrier program such as email
- ☐ A common form of Internet attack

Question 1732

Which of the following would be MOST helpful in ensuring security procedures are followed by employees in a multinational organization?

- ☐ Security architecture review
- ☐ Regular clean desk reviews
- ☐ Comprehensive end-user training
- ☐ Regular policy updates by management

Question 1733

Which of the following is the MOST significant concern when backup tapes are encrypted?

- ☐ Loss of the encryption key
- ☐ Lack of physical security over the tapes
- ☐ Incompatibility with future software versions
- ☐ Inaccurate data due to encryption processing

Question 1734

An organization has implemented an automated match between purchase orders, goods receipts, and invoices. Which of the following risks will this control BESTmitigate?

- ☐ Customer discounts not being applied
- ☐ A legitimate transaction being paid multiple times
- ☐ Invalid payments being processed by the system
- ☐ Delay of purchase orders

Licensed to Berend Post berend.post@it-university.nl

Question 1735

Which of the following controls BEST ensures appropriate segregation of duties within an accounts payable department?

- ☐ Ensuring that audit trails exist for transactions
- ☐ Restricting access to update programs to accounts payable staff only
- ☐ Restricting program functionality according to user security profiles
- ☐ Including the creator's user ID as a field in every transaction record created

Question 1736

An IS auditor is conducting a pre-implementation review to determine a new system's production readiness. The auditor's PRIMARY concern should be whether:

- ☐ the project adhered to the budget and target date
- ☐ users were involved in the quality assurance (QA) testing
- ☐ there are unresolved high-risk items
- ☐ benefits realization has been evidenced

Question 1737

Which of the following is an advantage of decentralized security administration?

- ☐ Greater integrity
- ☐ Faster turnaround
- ☐ More uniformity
- ☐ Better-trained administrators

Question 1738

The PRIMARY benefit of integrating information security activities into change management processes is to:

- ☐ protect the organization from unauthorized changes.
- ☐ ensure required controls are included in changes.
- ☐ provide greater accountability for security-related changes in the business.
- ☐ protect the business from collusion and compliance threats.

Licensed to Berend Post berend.post@it-university.nl

Question 1739

The effectiveness of an incident response team will be GREATEST when:

- ☐ the incident response process is updated based on lessons learned
- ☐ incidents are identified using a security information and event monitoring (SIEM) system
- ☐ the incident response team members are trained security personnel
- ☐ the incident response team meets on a regular basis to review log files

Question 1740

Which of the following is the MOST effective control to minimize the risk of cross-site scripting (XSS)?

- ☐ Periodic vulnerability assessments
- ☐ Secure coding practices
- ☐ Network intrusion prevention system
- ☐ Web firewall policy

Question 1741

An IT organization's incident response plan is which type of control?

- ☐ Preventive
- ☐ Corrective
- ☐ Detective
- ☐ Directive

Question 1742

Which of the following is the BEST method to prevent wire transfer fraud by bank employees?

- ☐ Re-keying of wire dollar amounts
- ☐ Independent reconciliation
- ☐ Two-factor authentication control
- ☐ System-enforced dual control

Question 1743

An IS auditor performing an application maintenance audit would review the log of program changes for the:

- ☐ authorization of program changes.
- ☐ creation date of a current object module.
- ☐ number of program changes actually made.
- ☐ creation date of a current source program.

Licensed to Berend Post berend.post@it-university.nl

Question 1744

In which of the following cloud computing service model are applications hosted by the service provider and made available to the customers over a network?

- ☐ Software as a service
- ☐ Data as a service
- ☐ Platform as a service
- ☐ Infrastructure as a service

Question 1745

Which of the following intrusion detection systems (IDSs) monitors the general patterns of activity and traffic on a network and creates a database?

- ☐ Signature-based
- ☐ Neural networks-based
- ☐ Statistical-based
- ☐ Host-based

Question 1746

When an organization is outsourcing their information security function, which of the following should be kept in the organization?

- ☐ Accountability for the corporate security policy
- ☐ Defining the corporate security policy
- ☐ Implementing the corporate security policy
- ☐ Defining security procedures and guidelines

Question 1747

What would be the major purpose of rootkit?

- ☐ to hide evidence from system administrators.
- ☐ to encrypt files for system administrators.
- ☐ to corrupt files for system administrators.
- ☐ to hijack system sessions.
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 1748

A company has implemented a new client-server enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following would BEST ensure that the orders are entered accurately and the corresponding products are produced?

- ☐ Verifying production to customer orders
- ☐ Logging all customer orders in the ERP system
- ☐ Using hash totals in the order transmitting process
- ☐ Approving (production supervisor) orders prior to production

Question 1749

Documentation of a business case used in an IT development project should be retained until:

- ☐ the end of the system's life cycle.
- ☐ the project is approved.
- ☐ user acceptance of the system.
- ☐ the system is in production.

Question 1750

Which of the following processes is the FIRST step in establishing an information security policy?

- ☐ Security controls evaluation
- ☐ Business risk assessment
- ☐ Review of current global standards
- ☐ Information security audit

Question 1751

An IS auditor examining a biometric user authentication system establishes the existence of a control weakness that would allow an unauthorized individual to update the centralized database on the server that is used to store biometric templates. Of the following, which is the BEST control against this risk?

- ☐ Kerberos
- ☐ Vitality detection
- ☐ Multimodal biometrics
- ☐ Before-image/after-image logging

Licensed to Berend Post berend.post@it-university.nl

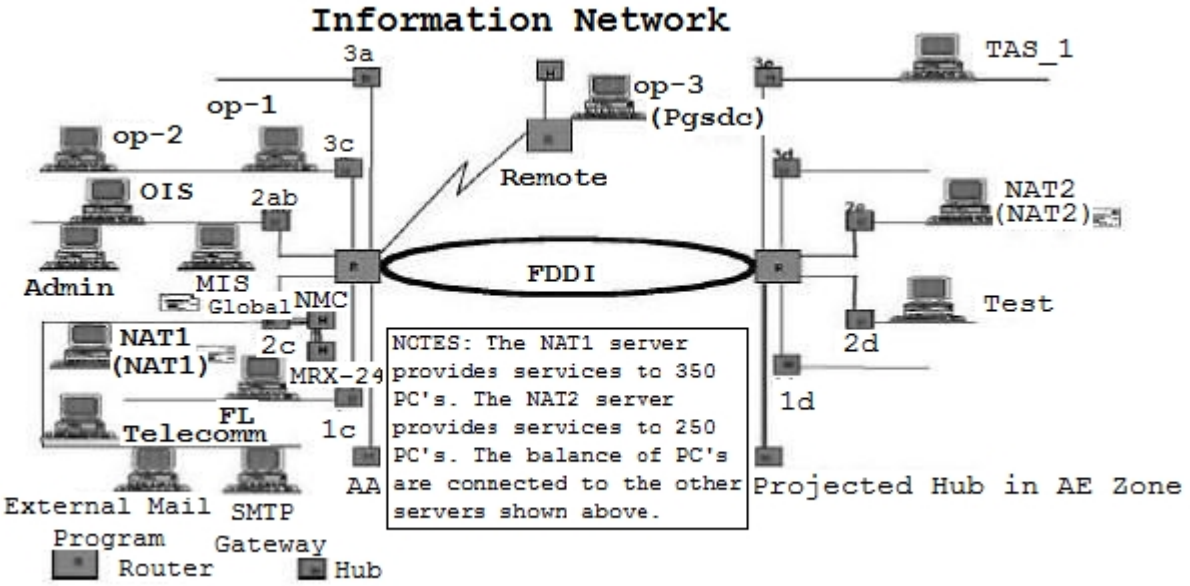
Question 1752

An accurate biometric system usually exhibits (Choose two.):

- ☐ low EER
- ☐ low CER
- ☐ high EER
- ☐ high CER
- ☐ None of the choices.

Question 1753

For locations 3a, 1d and 3d, the diagram indicates hubs with lines that appear to be open and active. Assuming that is true, what control, if any, should be recommended to mitigate this weakness?



- ☐ Intelligent hub
- ☐ Physical security over the hubs
- ☐ Physical security and an intelligent hub
- ☐ No controls are necessary since this is not a weakness

Question 1754

To confirm integrity for a hashed message, the receiver should use:

- ☐ a different hashing algorithm from the sender's to create a numerical representation of the file.
- ☐ a different hashing algorithm from the sender's to create a binary image of the file.
- ☐ the same hashing algorithm as the sender's to create a binary image of the file.
- ☐ the same hashing algorithm as the sender's to create a numerical representation of the file.

Licensed to Berend Post berend.post@it-university.nl

Question 1755

An IS auditor is assessing an organization's data loss prevention (DLP) solution for protecting intellectual property from insider theft. Which of the following would the auditor consider MOST important for effective data protection?

- ☐ Employee training on information handling
- ☐ Creation of DLP policies and procedures
- ☐ Encryption of data copied to flash drives
- ☐ Identification and classification of sensitive data

Question 1756

Which of the following would be the GREATEST cause for concern when data are sent over the Internet using HTTPS protocol?

- ☐ Presence of spyware in one of the ends
- ☐ The use of a traffic sniffing tool
- ☐ The implementation of an RSA-compliant solution
- ☐ A symmetric cryptography is used for transmitting data

Question 1757

A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

- ☐ Unit testing
- ☐ Integration testing
- ☐ Design walk-throughs
- ☐ Configuration management

Question 1758

The 'trusted systems' approach has been predominant in the design of:

- ☐ many earlier Microsoft OS products
- ☐ the IBM AS/400 series
- ☐ the SUN Solaris series
- ☐ most OS products in the market
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 1759

Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

- ☐ Parallel
- ☐ Preparedness
- ☐ Walk-thorough
- ☐ Paper

Question 1760

Which of the following must exist to ensure the viability of a duplicate information processing facility?

- ☐ The site is near the primary site to ensure quick and efficient recovery.
- ☐ The site contains the most advanced hardware available.
- ☐ The workload of the primary site is monitored to ensure adequate backup is available.
- ☐ The hardware is tested when it is installed to ensure it is working properly.

Question 1761

Which of the following is the GREATEST security risk associated with data migration from a legacy HR system to a cloud-based system?

- ☐ System performance may be impacted by the migration.
- ☐ Records past their retention period may not be migrated to the new system.
- ☐ Data from the source and target system may have different data formats.
- ☐ Data from the source and target system may be intercepted.

Question 1762

Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

- ☐ The use of diskless workstations
- ☐ Periodic checking of hard drives
- ☐ The use of current antivirus software
- ☐ policies that result in instant dismissal if violated

Licensed to Berend Post berend.post@it-university.nl

Question 1763

Which of the following would BEST provide an information security manager with sufficient assurance that a service provider complies with organization's information security requirements?

- ☐ A live demonstration of the third-party supplier's security capabilities
- ☐ Third-party security control self-assessment results
- ☐ An independent review report indicating compliance with industry standards
- ☐ The ability to audit the third-party supplier's IT systems and processes

Question 1764

Which of the following should be included in a feasibility study for a project to implement an EDI process?

- ☐ The encryption algorithm format
- ☐ The detailed internal control procedures
- ☐ The necessary communication protocols
- ☐ The proposed trusted third-party agreement

Question 1765

The performance of an order-processing system can be measured MOST reliably by monitoring:

- ☐ input/request queue length.
- ☐ turnaround time of completed transactions.
- ☐ application and database servers' CPU load.
- ☐ heartbeats between server systems.

Question 1766

Minimum password length and password complexity verification are examples of:

- ☐ detection controls.
- ☐ control objectives.
- ☐ audit objectives.
- ☐ control procedures.

Question 1767

Which of the following should be the PRIMARY consideration when developing an IT strategy?

- ☐ IT key performance indicators based on business objectives
- ☐ Alignment with overall business objectives
- ☐ Alignment with the IT investment portfolio
- ☐ Short and long-term plans for the enterprise IT architecture

Licensed to Berend Post berend.post@it-university.nl

Question 1768

During an incident management audit, an IS auditor finds that several similar incidents were logged during the audit period. Which of the following is the auditor's MOST important course of action?

- ☐ Document the finding and present it to management.
- ☐ Determine if a root cause analysis was conducted.
- ☐ Validate whether all incidents have been actioned.
- ☐ Confirm the resolution time of the incidents.

Question 1769

Overall responsibility for approving logical access rights to information assets should reside with the:

- ☐ data and systems owners.
- ☐ systems delivery and operations group.
- ☐ security administrator.
- ☐ systems administrator.

Question 1770

Which of the following type of testing validate functioning of the application under test with other system, where a set of data is transferred from one system to another?

- ☐ Interface testing
- ☐ Unit Testing
- ☐ System Testing
- ☐ Final acceptance testing

Question 1771

Which of the following attack is also known as Time of Check(TOC)/Time of Use(TOU)?

- ☐ Eavesdropping
- ☐ Traffic analysis
- ☐ Masquerading
- ☐ Race Condition

Question 1772

When an information security manager presents an information security program status report to senior management, the MAIN focus should be:

- ☐ key performance indicators (KPIs)
- ☐ critical risks indicators
- ☐ net present value (NPV)
- ☐ key controls evaluation

Licensed to Berend Post berend.post@it-university.nl

Question 1773

Off-site data backup and storage should be geographically separated so as to _____ (fill in the blank) the risk of a widespread physical disaster such as a hurricane or earthquake.

- ☐ Accept
- ☐ Eliminate
- ☐ Transfer
- ☐ Mitigate

Question 1774

Squid is an example of:

- ☐ IDS
- ☐ caching proxy
- ☐ security proxy
- ☐ connection proxy
- ☐ dialer
- ☐ None of the choices.

Question 1775

An organization has detected sensitive data leakage caused by an employee of a third-party contractor. What is the BEST course of action to address this issue?

- ☐ Include security requirements in outsourcing contracts.
- ☐ Activate the organization's incident response plan.
- ☐ Limit access to the third-party contractor.
- ☐ Terminate the agreement with the third-party contractor.

Question 1776

Which of the following is the BEST reason for delaying the application of a critical security patch?

- ☐ Lack of vulnerability management
- ☐ Conflicts with software development life cycle
- ☐ Technology interdependencies
- ☐ Resource limitations

Licensed to Berend Post berend.post@it-university.nl

Question 1777

Which of the following conditions would be of MOST concern to an IS auditor assessing the risk of a successful brute force attack encrypted data at rest?

- ☐ Use of symmetric encryption
- ☐ Use of asymmetric encryption
- ☐ Random key generation
- ☐ Short key length

Question 1778

Loading of illegal software packages onto a network by an employee is MOST effectively detected by:

- ☐ diskless workstations.
- ☐ regular scanning of hard drives
- ☐ maintaining current antivirus software.
- ☐ logging of activity on network drives.

Question 1779

A web server is attacked and compromised. Which of the following should be performed FIRST to handle the incident?

- ☐ Dump the volatile storage data to a disk.
- ☐ Run the server in a fail-safe mode.
- ☐ Disconnect the web server from the network.
- ☐ Shut down the web server.

Question 1780

Which of the following reports should an IS auditor use to check compliance with a service level agreements (SLA) requirement for uptime?

- ☐ Utilization reports
- ☐ Hardware error reports
- ☐ System logs
- ☐ Availability reports

Question 1781

The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

- ☐ a lack of investment in technology.
- ☐ a lack of a methodology for systems development.
- ☐ technology not aligning with the organization's objectives.
- ☐ an absence of control over technology contracts.

Licensed to Berend Post berend.post@it-university.nl

Question 1782

Validated digital signatures in an e-mail software application will:

- ☐ help detect spam.
- ☐ provide confidentiality.
- ☐ add to the workload of gateway servers.
- ☐ significantly reduce available bandwidth.

Question 1783

The GREATEST benefit of using a maturity model when providing security reports to management is that it presents the:

- ☐ current and target security state for the business.
- ☐ security program priorities to achieve an accepted risk level.
- ☐ assessed level of security risk at a particular point in time.
- ☐ level of compliance with internal policy.

Question 1784

The responsibilities of a disaster recovery relocation team include:

- ☐ obtaining, packaging and shipping media and records to the recovery facilities, as well as establishing and overseeing an offsite storage schedule.
- ☐ locating a recovery site, if one has not been predetermined, and coordinating the transport of company employees to the recovery site.
- ☐ managing the relocation project and conducting a more detailed assessment of the damage to the facilities and equipment.
- ☐ coordinating the process of moving from the hot site to a new location or to the restored original location.

Question 1785

An IS auditor evaluating a three-tier client/server architecture observes an issue with graphical user interface (GUI) tasks. Which layer should the auditor recommend the client address?

- ☐ Presentation layer
- ☐ Application layer
- ☐ Storage layer
- ☐ Transport layer

Licensed to Berend Post berend.post@it-university.nl

Question 1786

In which of the following SDLC phases would the IS auditor expect to find that controls have been incorporated into system specifications?

- ☐ Development
- ☐ Implementation
- ☐ Design
- ☐ Feasibility

Question 1787

The PRIMARY objective of service-level management (SLM) is to:

- ☐ define, agree, record and manage the required levels of service.
- ☐ ensure that services are managed to deliver the highest achievable level of availability.
- ☐ keep the costs associated with any service at a minimum.
- ☐ monitor and report any legal noncompliance to business management.

Question 1788

Which of the following would an IS auditor consider to be the MOST important to review when conducting a business continuity audit?

- ☐ A hot site contracted and available as needed.
- ☐ A business continuity manual is available and current.
- ☐ insurance coverage is adequate and premiums are current.
- ☐ Media backups are performed on a timely basis and stored offsite.

Question 1789

The BEST way to prevent fraudulent payments is to implement segregation of duties between payment processing and:

- ☐ requisition creation.
- ☐ vendor setup.
- ☐ payment approval.
- ☐ check creation.

Licensed to Berend Post berend.post@it-university.nl

Question 1790

During the extraction and transfer process of data from an application database to an enterprise data warehouse, some of the fields were not picked up in the extraction process and therefore did not end up in the data warehouse. Which of the following is the GREATEST concern with this situation?

- ☐ Costs associated with correcting the process may exceed budget
- ☐ Transaction errors may occur within the application
- ☐ Management decisions may be based on incorrect data
- ☐ Management reporting could be delayed

Question 1791

Which of the following would help determine the maturity of an information security awareness program?

- ☐ A review of the annual penetration test results
- ☐ A network vulnerability assessment
- ☐ A simulated social engineering test
- ☐ A gap assessment against an established model

Question 1792

Which of the following statement INCORRECTLY describes Asynchronous Transfer Mode (ATM) technique?

- ☐ ATM uses cell switching method
- ☐ ATM is high speed network technology used for LAN, MAN and WAN
- ☐ ATM works at session layer of an OSI model
- ☐ Data are segmented into fixed size cell of 53 bytes

Question 1793

Which of the following should be the MOST important consideration when implementing an information security framework?

- ☐ Compliance requirements
- ☐ Audit findings
- ☐ Technical capabilities
- ☐ Risk appetite

Licensed to Berend Post berend.post@it-university.nl

Question 1794

Which of the following is the INCORRECT Layer to Protocol mapping used in the DOD TCP/IP model?

- ☐ Application layer – Telnet
- ☐ Transport layer – ICMP
- ☐ Internet layer – IP
- ☐ Network Access layer – Ethernet

Question 1795

To determine if unauthorized changes have been made to production code the BEST audit procedure is to:

- ☐ examine the change control system records and trace them forward to object code files.
- ☐ review access control permissions operating within the production program libraries.
- ☐ examine object code to find instances of changes and trace them back to change control records.
- ☐ review change approved designations established within the change control system.

Question 1796

An organization has purchased a replacement mainframe computer to cope with the demands of increased business. Which of the following should be the PRIMARY concern of an IS auditor?

- ☐ The disaster recovery plan has been reviewed and updated.
- ☐ Application access controls are adequate.
- ☐ Appropriate tender evaluation processes have been followed.
- ☐ The procurement is within the planned budget for the year.

Question 1797

Which of the following is the PRIMARY advantage of using virtualization technology for corporate applications?

- ☐ Better utilization of resources
- ☐ Stronger data security
- ☐ Increased application performance
- ☐ Improved disaster recovery

Licensed to Berend Post berend.post@it-university.nl

Question 1798

With respect to business continuity strategies, an IS auditor interviews key stakeholders in an organization to determine whether they understand their roles and responsibilities. The IS auditor is attempting to evaluate the:

- ☐ clarity and simplicity of the business continuity plans.
- ☐ adequacy of the business continuity plans.
- ☐ effectiveness of the business continuity plans.
- ☐ ability of IS and end-user personnel to respond effectively in emergencies.

Question 1799

An IS auditor is planning on utilizing attribute sampling to determine the error rate for health care claims processed. Which of the following factors will cause the sample size to decrease?

- ☐ Population size increase
- ☐ Expected error rate increase
- ☐ Acceptable risk level decrease
- ☐ Tolerate error rate increase

Question 1800

Which of the following should MOST concern an IS auditor reviewing an intrusion detection system (IDS)?

- ☐ Number of false negatives
- ☐ Number of false positives
- ☐ Legitimate traffic blocked by the system
- ☐ Reliability of IDS logs

Question 1801

Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

- ☐ True
- ☐ False

Question 1802

An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

- ☐ conclude that the controls are inadequate.
- ☐ expand the scope to include substantive testing
- ☐ place greater reliance on previous audits.
- ☐ suspend the audit.

Licensed to Berend Post berend.post@it-university.nl

Question 1803

Which of the following is a rewrite of ipfwadm?

- ☐ ipchains
- ☐ iptables
- ☐ Netfilter
- ☐ ipcook
- ☐ None of the choices.

Question 1804

The performance, risks, and capabilities of an IT infrastructure are BEST measured using a:

- ☐ balanced scorecard.
- ☐ risk management review.
- ☐ service level agreement (SLA).
- ☐ control self-assessment (CSA).

Question 1805

Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

- ☐ True
- ☐ False

Question 1806

An auditor is creating an audit program in which the objective is to establish the adequacy of personal data privacy controls in a payroll process. Which of the following would be MOST important to include?

- ☐ Approval of data changes
- ☐ Audit logging of administrative user activity
- ☐ Segregation of duties controls
- ☐ User access provisioning

Question 1807

An information security manager's PRIMARY objective for presenting key risks to the board of directors is to:

- ☐ re-evaluate the risk appetite.
- ☐ quantify reputational risks.
- ☐ meet information security compliance requirements.
- ☐ ensure appropriate information security governance.

Licensed to Berend Post berend.post@it-university.nl

Question 1808

Web and e-mail filtering tools are PRIMARILY valuable to an organization because they:

- ☐ protect the organization from viruses and nonbusiness materials.
- ☐ maximize employee performance.
- ☐ safeguard the organization's image.
- ☐ assist the organization in preventing legal issues

Question 1809

An IS auditor should aware of various analysis models used by data architecture. Which of the following analysis model outline the major process of an organization and the external parties with which business interacts?

- ☐ Context Diagrams
- ☐ Activity Diagrams
- ☐ Swim-lane diagrams
- ☐ Entity relationship diagrams

Question 1810

While designing the business continuity plan (BCP) for an airline reservation system, the MOST appropriate method of data transfer/backup at an offsite location would be:

- ☐ shadow file processing.
- ☐ electronic vaulting.
- ☐ hard-disk mirroring.
- ☐ hot-site provisioning.

Question 1811

Which of the following is MOST important for an IS auditor to verify when reviewing a critical business application that requires high availability?

- ☐ Algorithms are reviewed to resolve process inefficiencies.
- ☐ Users participate in offsite business continuity testing.
- ☐ There is no single point of failure.
- ☐ Service level agreement (SLAs) are monitored.

Licensed to Berend Post berend.post@it-university.nl

Question 1812

Which of the following is MOST likely to be included in computer operating procedures in a large data center?

- ☐ Instructions for job scheduling
- ☐ Procedures for resequencing source code
- ☐ Procedures for utility configuration
- ☐ Guidance on setting security parameters

Question 1813

Which of the following would MOST likely require a business continuity plan to be invoked?

- ☐ A distributed denial of service attack on an email server
- ☐ An unauthorized visitor discovered in the data center
- ☐ An epidemic preventing staff from performing job functions
- ☐ A hacker holding personally identifiable information hostage.

Question 1814

Which of the following is the MOST important reason to periodically review data that has already been classified?

- ☐ The associated risk may change over time.
- ☐ Additional data may have been added to the inventory.
- ☐ Older data may need to be archived on removable media.
- ☐ The classification nomenclature has changed.

Question 1815

Which of the following is an IS auditor's BEST course of action upon learning that preventive controls have been replaced with detective and corrective controls?

- ☐ Report the issue to management as the risk level has increased.
- ☐ Recommend the implementation of preventive controls in addition to the other controls.
- ☐ Verify the revised controls enhance the efficiency of related business processes.
- ☐ Evaluate whether new controls manage the risk at an acceptable level.

Licensed to Berend Post berend.post@it-university.nl

Question 1816

An IS auditor notes that patches for the operating system used by an organization are deployed by the IT department as advised by the vendor. The MOST significant concern an IS auditor should have with this practice is the nonconsideration by IT of:

- ☐ the training needs for users after applying the patch.
- ☐ any beneficial impact of the patch on the operational systems.
- ☐ delaying deployment until testing the impact of the patch.
- ☐ the necessity of advising end users of new patches.

Question 1817

Management disagrees with a finding in a draft audit report and provides supporting documentation. Which of the following should be the IS auditor's NEXT course of action?

- ☐ Document management's disagreement in the final report
- ☐ Evaluate the supporting documentation
- ☐ Escalate the issue with supporting documentation to senior management
- ☐ Finalize the draft audit report without changes

Question 1818

Whenever business processes have been re-engineered, the IS auditor attempts to identify and quantify the impact of any controls that might have been removed, or controls that might not work as effectively after business process changes. True or false?

- ☐ True
- ☐ False

Question 1819

Which of the following observations noted during a review of the organization's social media practices should be of MOST concern to the IS auditor?

- ☐ The organization does not require approval for social media posts.
- ☐ More than one employee is authorized to publish on social media on behalf of the organization.
- ☐ Not all employees using social media have attended the security awareness program.
- ☐ The organization does not have a documented social media policy.

Licensed to Berend Post berend.post@it-university.nl

Question 1820

The PRIMARY reason for using digital signatures is to ensure data:

- ☐ confidentiality.
- ☐ integrity.
- ☐ availability.
- ☐ timeliness.

Question 1821

Which of the following is MOST important to consider when creating audit follow-up procedures?

- ☐ Whether the organization has sufficient funds to address the issue
- ☐ Whether management has determined if risk is within the organization's risk appetite
- ☐ Whether follow-up procedures would determine if identified risks have been mitigated
- ☐ Whether the auditee has allotted sufficient time for the follow-up

Question 1822

An organization has recently converted its infrastructure to a virtualized environment. The GREATEST benefit related to disaster recovery is that virtualized servers:

- ☐ reduce the time it takes to successfully create backups.
- ☐ decrease the recovery time objective (RTO).
- ☐ eliminate the manpower necessary to restore the server.
- ☐ can be recreated on similar hardware faster than restoring from backups.

Question 1823

Reviewing which of the following would provide the GREATEST input to the asset classification process:

- ☐ Risk assessment
- ☐ Sensitivity of the data
- ☐ Replacement cost of the asset
- ☐ Compliance requirements

Licensed to Berend Post berend.post@it-university.nl

Question 1824

Within a virus, which component is responsible for what the virus does to the victim file?

- ☐ the payload
- ☐ the signature
- ☐ the trigger
- ☐ the premium
- ☐ None of the choices.

Question 1825

Which of the following is the MOST important consideration when investigating a security breach of an e-commerce application?

- ☐ Chain of custody
- ☐ Skill set of the response team
- ☐ Notifications to law enforcement
- ☐ Procedures to analyze evidence

Question 1826

In assessing the priority given to systems covered in an organization's business continuity plan (BCP), an IS auditor should FIRST:

- ☐ review results of previous business continuity plan (BCP) tests.
- ☐ review the backup and restore processes.
- ☐ verify the criteria for disaster recovery site selection.
- ☐ validate the recovery time objectives and recovery point objectives.

Question 1827

An IS auditor is reviewing an organization's network vulnerability scan results. Which of the following processes would the scan results MOST likely feed into?

- ☐ Firewall maintenance
- ☐ Patch management
- ☐ Incident response
- ☐ Traffic management

Licensed to Berend Post berend.post@it-university.nl

Question 1828

Back Orifice is an example of:

- ☐ a virus.
- ☐ a legitimate remote control software.
- ☐ a backdoor that takes the form of an installed program.
- ☐ an eavesdropper.
- ☐ None of the choices.

Question 1829

To maintain the confidentiality of information moved between office and home on removable media, which of the following is the MOST effective control?

- ☐ Mandatory file passwords
- ☐ Security awareness training
- ☐ Digitally signed media
- ☐ Data encryption

Question 1830

A CIO has asked an IS auditor to implement several security controls for an organization's IT processes and systems. The auditor should:

- ☐ perform the assignment and future audits with due professional care.
- ☐ obtain approval from executive management for the implementation.
- ☐ refuse due to independence issues.
- ☐ communicate the conflict of interest to audit management.

Question 1831

Which of the following is the BEST way to control scope creep during application system development?

- ☐ Involve key stakeholders.
- ☐ Implement project steering committee review.
- ☐ Implement a quality management system.
- ☐ Establish key performance indicators (KPIs).

Licensed to Berend Post berend.post@it-university.nl

Question 1832

A firm is considering using biometric fingerprint identification on all PCs that access critical datA. This requires:

- ☐ that a registration process is executed for all accredited PC users.
- ☐ the full elimination of the risk of a false acceptance.
- ☐ the usage of the fingerprint reader be accessed by a separate password.
- ☐ assurance that it will be impossible to gain unauthorized access to critical data.

Question 1833

Which of the following is the MOST effective control to ensure electronic records beyond their retention periods are deleted from IT systems?

- ☐ Review the record retention register regularly to initiate data deletion.
- ☐ Build in system logic to trigger data deletion at predefined times.
- ☐ Perform a sample check of current data against the retention schedule.
- ☐ Execute all data deletions at a predefined month during the year.

Question 1834

Which of the following is a MAJOR benefit of using a wireless network?

- ☐ Faster network speed
- ☐ Stronger authentication
- ☐ Protection against eavesdropping
- ☐ Lower installation cost

Question 1835

Creating which of the following is how a hacker can insure his ability to return to the hacked system at will?

- ☐ rootsec
- ☐ checksum
- ☐ CRC
- ☐ backdoors
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 1836

Which of the following is the FIRST consideration when developing a data retention policy?

- ☐ Determining the backup cycle based on retention period
- ☐ Designing an infrastructure storage strategy
- ☐ Identifying the legal and contractual retention period for data
- ☐ Determining the security access privileges to the data

Question 1837

A PRIMARY advantage of involving business management in evaluating and managing information security risks is that they:

- ☐ better understand the security architecture
- ☐ better understand organizational risks
- ☐ can balance technical and business risks
- ☐ are more objective than security management

Question 1838

As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:

- ☐ performance measurement.
- ☐ strategic alignment.
- ☐ value delivery.
- ☐ resource management.

Question 1839

Which of the following MOST effectively provides assurance of ongoing service delivery by a vendor?

- ☐ Regular status reporting provided by the vendor
- ☐ Short incident response time by the vendor
- ☐ Pre-defined service and operational level agreements
- ☐ Regular monitoring by service management team

Question 1840

Which of the following does a lack of adequate security controls represent?

- ☐ Threat
- ☐ Asset
- ☐ Impact
- ☐ Vulnerability

Licensed to Berend Post berend.post@it-university.nl

Question 1841

During a review of an application system, an IS auditor identifies automated controls designed to prevent the entry of duplicate transactions. What is the BEST way to verify that the controls work as designed?

- ☐ Implement periodic reconciliations.
- ☐ Review quality assurance (QA) test results.
- ☐ Use generalized audit software for seeking data corresponding to duplicate transactions.
- ☐ Enter duplicate transactions in a copy of the live system.

Question 1842

Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital?

- ☐ Multiplexer
- ☐ Modem
- ☐ Protocol converter
- ☐ Concentrator

Question 1843

An IS auditor performing an audit of backup procedures observes that backup tapes are picked up weekly and stored offsite at a third-party hosting facility. Which of the following recommendations would be the BEST way to protect the data on the backup tapes?

- ☐ Ensure that data is encrypted before leaving the facility.
- ☐ Ensure that the transport company obtains signatures for all shipments.
- ☐ Confirm that data is transported in locked tamper-evident containers.
- ☐ Confirm that data transfers are logged and recorded.

Question 1844

What should an IS auditor do if he or she observes that project-approval procedures do not exist?

- ☐ Advise senior management to invest in project-management training for the staff
- ☐ Create project-approval procedures for future project implementations
- ☐ Assign project leaders
- ☐ Recommend to management that formal approval procedures be adopted and documented

Licensed to Berend Post berend.post@it-university.nl

Question 1845

Within IPSEC which of the following defines security parameters which should be applied between communicating parties such as encryption algorithms, key initialization vector, life span of keys, etc?

- ☐ Security Parameter Index (SPI)
- ☐ Security Association (SA)
- ☐ Encapsulation Security Payload (ESP)
- ☐ Authentication Header (AH)

Question 1846

The purpose of business continuity planning and disaster-recovery planning is to:

- ☐ Transfer the risk and impact of a business interruption or disaster
- ☐ Mitigate, or reduce, the risk and impact of a business interruption or disaster
- ☐ Accept the risk and impact of a business
- ☐ Eliminate the risk and impact of a business interruption or disaster

Question 1847

A large insurance company is about to replace a major financial application. Which of the following is the IS auditor's PRIMARY focus when conducting the pre-implementation review?

- ☐ Procedure updates
- ☐ Migration of data
- ☐ System manuals
- ☐ Unit testing

Question 1848

A firewall is being deployed at a new location. Which of the following is the MOST important factor in ensuring a successful deployment?

- ☐ Reviewing logs frequently
- ☐ Testing and validating the rules
- ☐ Training a local administrator at the new location
- ☐ Sharing firewall administrative duties

Licensed to Berend Post berend.post@it-university.nl

Question 1849

An IS auditor is reviewing the upgrading of an operating system. Which of the following would be the GREATEST audit concern?

- ☐ The lack of release notes
- ☐ The lack of change control
- ☐ The lack of malware protection
- ☐ The lack of activity logging

Question 1850

Following a successful attack on an organization's web server, which of the following actions should be performed FIRST?

- ☐ Review the boundary configuration rules to ensure that outbound packets are limited
- ☐ Evaluate and deploy an intrusion detection system
- ☐ Periodically scan the network for systems with well-known vulnerabilities
- ☐ Establish reference systems using cryptographic checksum tools

Question 1851

The PRIMARY objective of business continuity and disaster recovery plans should be to:

- ☐ safeguard critical IS assets.
- ☐ provide for continuity of operations.
- ☐ minimize the loss to an organization.
- ☐ protect human life.

Question 1852

An IS auditor is performing an audit of a remotely managed server backup. The IS auditor reviews the logs for one day and finds one case where logging on a server has failed with the result that backup restarts cannot be confirmed. What should the auditor do?

- ☐ Issue an audit finding
- ☐ Seek an explanation from IS management
- ☐ Review the classifications of data held on the server
- ☐ Expand the sample of logs reviewed

Licensed to Berend Post berend.post@it-university.nl

Question 1853

Which of the following is the MOST likely result of the ongoing deterioration of a detective control?

- ☐ Increased number of data loss events
- ☐ Increased security incident response time
- ☐ Decreased effectiveness of root cause analysis
- ☐ Decreased overall recovery time

Question 1854

Which of the following is the MOST important outcome of effective risk treatment?

- ☐ Timely reporting of incidents
- ☐ Elimination of risk
- ☐ Implementation of corrective actions
- ☐ Reduced cost of maintaining controls

Question 1855

Which of the following is the MOST important consideration for an organization when strategizing to comply with privacy regulations?

- ☐ Ensuring there are staff members with in-depth knowledge of the privacy regulations
- ☐ Ensuring up-to-date knowledge of where customer data is saved
- ☐ Ensuring regularly updated contracts with third parties that process customer data
- ☐ Ensuring appropriate access to information systems containing privacy information.

Question 1856

The final decision to include a material finding in an audit report should be made by the:

- ☐ audit committee.
- ☐ auditee's manager.
- ☐ IS auditor.
- ☐ CEO of the organization

Question 1857

Which of the following is MOST important for an IS auditor to determine when evaluating a database for privacy-related risks?

- ☐ Whether copies of production data are masked
- ☐ Whether the integrity of the data dictionary is maintained
- ☐ Whether data import and export procedures are approved
- ☐ Whether all database tables are normalized

Licensed to Berend Post berend.post@it-university.nl

Question 1858

The business case for an IS project has changed during the course of the project due to new requirements being added. What should be done NEXT?

- ☐ The project should go through the formal reapproval process.
- ☐ The changes to the business case should be documented in the project plan.
- ☐ Additional resources should be allocated to the project due to the new requirements.
- ☐ Project stakeholders should be notified of the changes.

Question 1859

Which of the following is MOSTimportant to consider when developing a bring your own device (BYOD) policy?

- ☐ Supported operating systems
- ☐ Procedure for accessing the network
- ☐ Application download restrictions
- ☐ Remote wipe procedures

Question 1860

When implementing a new risk assessment methodology, which of the following is the MOST important requirement?

- ☐ The methodology must be approved by the chief executive officer.
- ☐ Risk assessments must be reviewed annually.
- ☐ Risk assessments must be conducted by certified staff.
- ☐ The methodology used must be consistent across the organization.

Question 1861

As described at security policy, the CSO implemented an e-mail package solution that allows for ensuring integrity of messages sent using SMIME. Which of the options below BEST describes how it implements the environment to suite policy﷽s requirement?

- ☐ Implementing PGP and allowing for recipient to receive the private key used to sign e-mail message.
- ☐ Implementing RSA standard for messages envelope and instructing users to sign all messages using their private key from their PKI digital certificate.
- ☐ Implementing RSA standard for messages envelope and instructing users to sign all messages using their public key from their PKI digital certificate.
- ☐ Implementing MIME solutions and providing a footer within each message sent, referencing to policy constraints related to e-mail usage.

Licensed to Berend Post berend.post@it-university.nl

Question 1862

An IS auditor has audited a business continuity plan (BCP). Which of the following findings is the MOST critical?

- ☐ Nonavailability of an alternate private branch exchange (PBX) system
- ☐ Absence of a backup for the network backbone
- ☐ Lack of backup systems for the users' PCs
- ☐ Failure of the access card system

Question 1863

Which of the following provides the MOST reliable audit evidence on the validity of transactions in a financial application?

- ☐ Substantive testing
- ☐ Walk-through reviews
- ☐ Compliance testing
- ☐ Design documentation reviews

Question 1864

The Federal Information Processing Standards (FIPS) are primarily for use by (Choose two.):

- ☐ all non-military government agencies
- ☐ US government contractors
- ☐ all military government agencies
- ☐ all private and public colleges in the US
- ☐ None of the choices.

Question 1865

A hard disk containing confidential data was damaged beyond repair. What should be done to the hard disk to prevent access to the data residing on it?

- ☐ Rewrite the hard disk with random Os and Is.
- ☐ Low-level format the hard disk.
- ☐ Demagnetize the hard disk.
- ☐ Physically destroy the hard disk.

Licensed to Berend Post berend.post@it-university.nl

Question 1866

Which of the following procedures would BEST determine whether adequate recovery/restart procedures exist?

- ☐ Reviewing program code
- ☐ Reviewing operations documentation
- ☐ Turning off the UPS, then the power
- ☐ Reviewing program documentation

Question 1867

During an audit, which of the following would be MOST helpful in establishing a baseline for measuring data quality?

- ☐ Built-in data error prevention application controls
- ☐ Industry standard business definitions
- ☐ Input from customers
- ☐ Validation of rules by the business

Question 1868

In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

- ☐ Optimized
- ☐ Managed
- ☐ Defined
- ☐ Repeatable

Question 1869

An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

- ☐ True
- ☐ False

Licensed to Berend Post berend.post@it-university.nl

Question 1870

Which is the PRIMARY objective of evaluating the readiness of information systems for implementation?

- ☐ Determine whether IT systems projects are on schedule.
- ☐ Determine whether the systems comply with the organization's policy.
- ☐ Determine whether the systems meet user requirements.
- ☐ Determine whether the systems meet business requirements.

Question 1871

An IS auditor finds a number of system accounts that do not have documented approvals. Which of the following should be performed FIRST by the auditor?

- ☐ Have the accounts removed immediately
- ☐ Obtain sign-off on the accounts from the application owner
- ☐ Document a finding and report an ineffective account provisioning control
- ☐ Determine the purpose and risk of the accounts

Question 1872

During a postimplementation review of an enterprise resource management system, an IS auditor would MOST likely:

- ☐ review access control configuration
- ☐ evaluate interface testing.
- ☐ review detailed design documentation.
- ☐ evaluate system testing.

Question 1873

Which of the following findings would have the GREATEST impact on the objective of a business intelligence system?

- ☐ Key control have not been tested in a year.
- ☐ Decision support queries use database functions proprietary to the vendor.
- ☐ The hot site for disaster recovery does not include the decision support system.
- ☐ Management reports have not been evaluated since implementation.

Licensed to Berend Post berend.post@it-university.nl

Question 1874

When performing an IS strategy audit, an IS auditor should review both short-term (one- year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered. The auditor should especially focus on procedures in an audit of IS strategy. True or false?

- ☐ True
- ☐ False

Question 1875

Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

- ☐ has been approved by line management.
- ☐ does not vary from the IS department's preliminary budget.
- ☐ complies with procurement procedures.
- ☐ supports the business objectives of the organization.

Question 1876

Which of the following activities is MOST important in determining whether a test of a disaster recovery plan (DRP) has been successful?

- ☐ Evaluating participation by key personnel
- ☐ Testing at the backup data center
- ☐ Analyzing whether predetermined test objectives were met
- ☐ Testing with offsite backup files

Question 1877

A multinational organization is introducing a security governance framework. The information security manager’s concern is that regional security practices differ. Which of the following should be evaluated FIRST?

- ☐ Local regulatory requirements
- ☐ Local IT requirements
- ☐ Cross-border data mobility
- ☐ Corporate security objectives

Licensed to Berend Post berend.post@it-university.nl

Question 1878

Which of the following provides nonrepudiation in an electronic communication session without confidentiality?

- ☐ Message encryption
- ☐ Log-on ID and password
- ☐ Certification authority
- ☐ Digital signature

Question 1879

When using digital signatures, a sender transmits an encrypted message digest. This ensures that the:

- ☐ message is not intercepted during transmission
- ☐ message is not altered during transmission
- ☐ message sender obtains acknowledgement of delivery
- ☐ message remains confidential during transmission

Question 1880

What is a reliable technique for estimating the scope and cost of a software-development project?

- ☐ Function point analysis (FPA)
- ☐ Feature point analysis (FPA)
- ☐ GANTT
- ☐ PERT

Question 1881

An IS auditor is performing a consulting engagement and needs to make a recommendation for securing all doors to a data center to prevent unauthorized access. Which of the following access control techniques would be MOST difficult for an intruder to compromise?

- ☐ Dead-man door and swipe card
- ☐ Smart card and numeric keypad
- ☐ USB token and password
- ☐ Biometrics and PIN

Licensed to Berend Post berend.post@it-university.nl

Question 1882

To develop a robust data security program, the FIRST course of action should be to:

- ☐ implement monitoring controls
- ☐ implement data loss prevention controls
- ☐ perform an inventory of assets
- ☐ interview IT senior management

Question 1883

An IS auditor notes that the anticipated benefits from an ongoing infrastructure project have changed due to recent organizational restructuring. Which of the following is the IS auditor's BEST recommendation?

- ☐ Review and reapprove the business case.
- ☐ Revise business goals and objectives.
- ☐ Conduct a new feasibility study.
- ☐ Review and update the business impact analysis (BIA).

Question 1884

The Secure Sockets Layer (SSL) protocol addresses the confidentiality of a message through:

- ☐ symmetric encryption.
- ☐ message authentication code.
- ☐ hash function.
- ☐ digital signature certificates.

Question 1885

On a public-key cryptosystem when there is no previous knowledge between parties, which of the following will BEST help to prevent one person from using a fictitious key to impersonate someone else?

- ☐ Encrypt the message containing the sender's public key, using a private-key cryptosystem.
- ☐ Send a certificate that can be verified by a certification authority with the public key.
- ☐ Encrypt the message containing the sender's public key; using the recipient's pubic key.
- ☐ Send the public key to the recipient prior to establishing the connection.

Licensed to Berend Post berend.post@it-university.nl

Question 1886

An IS auditor considering use of another auditor's workpapers should:

- ☐ rarely rely on the work of another auditor.
- ☐ determine that the workpapers were completed within the past month.
- ☐ determine that then auditee agrees with key issues in these workpapers.
- ☐ consider the appropriateness and sufficiency of the workpapers.

Question 1887

After observing suspicious activities in a server, a manager requests a forensic analysis. Which of the following findings should be of MOST concern to the investigator?

- ☐ Server is a member of a workgroup and not part of the server domain
- ☐ Guest account is enabled on the server
- ☐ Recently, 100 users were created in the server
- ☐ Audit logs are not enabled for the server

Question 1888

An IS auditor reviews an organizational chart PRIMARILY for:

- ☐ an understanding of workflows.
- ☐ investigating various communication channels.
- ☐ understanding the responsibilities and authority of individuals.
- ☐ investigating the network connected to different employees.

Question 1889

During audit follow-up, an IS auditor finds that a control has been implemented differently than recommended. The auditor should:

- ☐ verify whether the control objectives are adequately addressed.
- ☐ compare the control to the action plan.
- ☐ report as a repeat finding.
- ☐ inform management about incorrect implementation.

Question 1890

Reconfiguring which of the following firewall types will prevent inward downloading of files through the File Transfer Protocol (FTP)?

- ☐ Circuit gateway
- ☐ Application gateway
- ☐ Packet filter
- ☐ Screening router

Licensed to Berend Post berend.post@it-university.nl

Question 1891

Which of the following is the BEST source of information for an IS auditor when planning an audit of a business application's controls?

- ☐ User documentation
- ☐ Change control procedures
- ☐ Access control lists
- ☐ Process flow diagrams

Question 1892

Which of the following will BEST provide an organization with ongoing assurance of the information security services provided by a cloud provider?

- ☐ Continuous monitoring of an information security risk profile
- ☐ Evaluating the provider's security incident response plan
- ☐ Requiring periodic self-assessment by the provider
- ☐ Ensuring the provider's roles and responsibilities are established

Question 1893

An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

- ☐ reverse engineering.
- ☐ prototyping.
- ☐ software reuse.
- ☐ reengineering.

Question 1894

Which of the following are BEST suited for continuous auditing?

- ☐ Manual transactions
- ☐ Irregular transactions
- ☐ Low-value transactions
- ☐ Real-time transactions

Question 1895

Which of the following acts as a decoy to detect active internet attacks?

- ☐ Honeypots
- ☐ Firewalls
- ☐ Trapdoors
- ☐ Traffic analysis

Licensed to Berend Post berend.post@it-university.nl

Question 1896

What topology provides the greatest redundancy of routes and the greatest network fault tolerance?

- ☐ A star network topology
- ☐ A mesh network topology with packet forwarding enabled at each host
- ☐ A bus network topology
- ☐ A ring network topology

Question 1897

The BEST overall quantitative measure of the performance of biometric control devices is:

- ☐ false-rejection rate.
- ☐ false-acceptance rate.
- ☐ equal-error rate.
- ☐ estimated-error rate.

Question 1898

Which of the following would be an IS auditor's GREATEST concern when evaluating a cybersecurity incident response plan?

- ☐ The plan has not been recently tested.
- ☐ Roles and responsibilities are not detailed for each process.
- ☐ Stakeholder contact details are not up-to-date.
- ☐ The plan does not include incident response metrics.

Question 1899

Which of the following must be in place before an IS auditor initiates audit follow-up activities?

- ☐ A heat map with the gaps and recommendations displayed in terms of risk
- ☐ A management response in the final report with a committed implementation date
- ☐ Supporting evidence for the gaps and recommendations mentioned in the audit report
- ☐ Available resources for the activities included in the action plan

Question 1900

The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

- ☐ understand the business process.
- ☐ comply with auditing standards.
- ☐ identify control weakness.
- ☐ plan substantive testing.

Licensed to Berend Post berend.post@it-university.nl

Question 1901

Which of the following biometrics methods provides the HIGHEST accuracy and is LEAST accepted by users?

- ☐ Palm Scan
- ☐ Hand Geometry
- ☐ Fingerprint
- ☐ Retina scan

Question 1902

Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management?

- ☐ Governing
- ☐ Culture
- ☐ Enabling and support
- ☐ Emergence

Question 1903

Which of the following is a network diagnostic tool that monitors and records network information?

- ☐ Online monitor
- ☐ Downtime report
- ☐ Help desk report
- ☐ Protocol analyzer

Question 1904

Which of the following is a dynamic analysis tool for the purpose of testing software modules?

- ☐ Blackbox test
- ☐ Desk checking
- ☐ Structured walk-through
- ☐ Design and code

Licensed to Berend Post berend.post@it-university.nl

Question 1905

What is an edit check to determine whether a field contains valid data?

- ☐ Completeness check
- ☐ Accuracy check
- ☐ Redundancy check
- ☐ Reasonableness check

Question 1906

An organization is in the process of acquiring a competitor. The information security manager has been asked to report on the security posture of the target acquisition. Which of the following should be the security manager's FIRSTcourse of action?

- ☐ Implement a security dashboard
- ☐ Quantity the potential risk
- ☐ Perform a gap analysis
- ☐ Perform a vulnerability assessment

Question 1907

Which of the following BEST describes the concept of ""defense in depth""?

- ☐ more than one subsystem needs to be compromised to compromise the security of the system and the information it holds.
- ☐ multiple firewalls are implemented.
- ☐ multiple firewalls and multiple network OS are implemented.
- ☐ intrusion detection and firewall filtering are required.
- ☐ None of the choices.

Question 1908

A potential risk of executing a program on an Internet site is that it may:

- ☐ install executable code on the computer.
- ☐ lack version control, which may result in the use of an older program.
- ☐ overwrite system files with older versions.
- ☐ be browser-dependent, and therefore abort.

Licensed to Berend Post berend.post@it-university.nl

Question 1909

To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

- ☐ schedule the audits and monitor the time spent on each audit.
- ☐ train the IS audit staff on current technology used in the company.
- ☐ develop the audit plan on the basis of a detailed risk assessment.
- ☐ monitor progress of audits and initiate cost control measures.

Question 1910

Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

- ☐ True
- ☐ False

Question 1911

When using a universal storage bus (USB) flash drive to transport confidential corporate data to an offsite location, an effective control would be to:

- ☐ carry the flash drive in a portable safe.
- ☐ assure management that you will not lose the flash drive.
- ☐ request that management deliver the flash drive by courier.
- ☐ encrypt the folder containing the data with a strong key.

Question 1912

Which of the following is the MOST effective control in an organization to mitigate the risk of insider misuse of personal devices?

- ☐ Security risk assessments
- ☐ Periodic vulnerability scanning
- ☐ Security awareness training
- ☐ Comprehensive procedures on data security

Question 1913

An IS auditor is reviewing an IT security risk management program. Measures of security risk should:

- ☐ address all of the network risks.
- ☐ be tracked over time against the IT strategic plan.
- ☐ take into account the entire IT environment.
- ☐ result in the identification of vulnerability tolerances.

Licensed to Berend Post berend.post@it-university.nl

Question 1914

Which of the following provides the BEST indication that the information security program is in alignment with enterprise requirements?

- ☐ The security strategy is benchmarked with similar organizations.
- ☐ The information security manager reports to the chief executive officer.
- ☐ An IT governance committee is in place.
- ☐ Security strategy objectives are defined in business terms.

Question 1915

After an IS auditor has identified threats and potential impacts, the auditor should:

- ☐ Identify and evaluate the existing controls
- ☐ Conduct a business impact analysis (BIA)
- ☐ Report on existing controls
- ☐ Propose new controls

Question 1916

An accounting department uses a spreadsheet to calculate sensitive financial transactions. Which of the following is the MOST important control for maintaining the security of data in the spreadsheet?

- ☐ There is a reconciliation process between the spreadsheet and the finance system.
- ☐ The spreadsheet is locked down to avoid inadvertent changes.
- ☐ A separate copy of the spreadsheet is routinely backed up.
- ☐ Access to the spreadsheet is given only to those who require access.

Question 1917

Which of the following controls would BEST detect intrusion?

- ☐ User IDs and user privileges are granted through authorized procedures.
- ☐ Automatic logoff is used when a workstation is inactive for a particular period of time.
- ☐ Automatic logoff of the system occurs after a specified number of unsuccessful attempts.
- ☐ Unsuccessful logon attempts are monitored by the security administrator.

Licensed to Berend Post berend.post@it-university.nl

Question 1918

Host Based ILD&P primarily addresses the issue of:

- ☐ information integrity
- ☐ information accuracy
- ☐ information validity
- ☐ information leakage
- ☐ None of the choices.

Question 1919

What is the MOST important role of an organization's data custodian in support of information security function?

- ☐ Evaluating data security technology vendors
- ☐ Applying approval security policies
- ☐ Approving access rights to departmental data
- ☐ Assessing data security risks to the organization

Question 1920

When planning an audit to assess application controls of a cloud-based system, it is MOST important for the IS auditor to understand the:

- ☐ policies and procedures of the business area being audited.
- ☐ business process supported by the system.
- ☐ availability reports associated with the cloud-based system.
- ☐ architecture and cloud environment of the system.

Question 1921

The BEST method an organization can employ to align its business continuity plan (BCP) and disaster recovery plan (DRP) with core business needs is to:

- ☐ execute periodic walk-throughs of the plans.
- ☐ update the business impact analysis (BIA) for significant business changes.
- ☐ outsource the maintenance of the BCP and disaster recovery plan to a third party.
- ☐ include BCP and disaster recovery plan responsibilities as a part of new employee training.

Licensed to Berend Post berend.post@it-university.nl

Question 1922

When two or more systems are integrated, input/output controls must be reviewed by an IS auditor in the:

- ☐ systems receiving the output of other systems.
- ☐ systems sending output to other systems.
- ☐ systems sending and receiving data.
- ☐ interfaces between the two systems.

Question 1923

Which of the following layer of an OSI model encapsulates packets into frames?

- ☐ Transport Layer
- ☐ Network Layer
- ☐ Data Link Layer
- ☐ Physical Layer
- ☐ .

Question 1924

While reviewing similar issues in an organization's help desk system, an IS auditor finds that they were analyzed independently and resolved differently. This situation MOST likely indicates a deficiency in:

- ☐ IT service level management.
- ☐ change management.
- ☐ configuration management.
- ☐ problem management.

Question 1925

Which of the following provide(s) near-immediate recoverability for time-sensitive systems and transaction processing?

- ☐ Automated electronic journaling and parallel processing
- ☐ Data mirroring and parallel processing
- ☐ Data mirroring
- ☐ Parallel processing

Licensed to Berend Post berend.post@it-university.nl

Question 1926

The BEST way to minimize the risk of communication failures in an e-commerce environment would be to use:

- ☐ compression software to minimize transmission duration.
- ☐ functional or message acknowledgments.
- ☐ a packet-filtering firewall to reroute messages.
- ☐ leased asynchronous transfer mode lines.

Question 1927

To ensure efficient and economic use of limited resources in supporting a local area network (LAN) infrastructure, it is advisable to:

- ☐ periodically rotate vendors to obtain the best price-to-performance ratio.
- ☐ standardize on a limited number of device models and software applications.
- ☐ quickly upgrade to the latest hardware and software versions to take advantage of new features.
- ☐ recommend a variety of products so that user effectiveness and flexibility can be maximized.

Question 1928

Which of the following is the MOST effective way of ensuring that business units comply with an information security governance framework?

- ☐ Conducting information security awareness training
- ☐ Performing security assessments and gap analyses
- ☐ Integrating security requirements with processes
- ☐ Conducting a business impact analysis (BIA)

Question 1929

An IS auditor finds that firewalls are outdated and not supported by vendors. Which of the following should be the auditor's NEXT course of action?

- ☐ Determine the value of the firewall.
- ☐ Report the security posture of the organization.
- ☐ Report the mitigating controls.
- ☐ Determine the risk of not replacing the firewall.

Licensed to Berend Post berend.post@it-university.nl

Question 1930

Which of the following is the MOST appropriate document for granting authority to an external IS auditor in an audit engagement with a client organization?

- ☐ Approved statement of work
- ☐ Formally approved audit charter
- ☐ An internal memo to all concerned parties
- ☐ Request for proposal for audit services

Question 1931

An IS auditor found that a company executive is encouraging employee use of social networking sites for business purposes. Which of the following recommendations would BEST help to reduce the risk of data leakage?

- ☐ Requiring policy acknowledgment and nondisclosure agreements signed by employees
- ☐ Providing education and guidelines to employees on use of social networking sites
- ☐ Establishing strong access controls on confidential data
- ☐ Monitoring employees' social networking usage

Question 1932

Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

- ☐ A substantive test of program library controls
- ☐ A compliance test of program library controls
- ☐ A compliance test of the program compiler controls
- ☐ A substantive test of the program compiler controls

Question 1933

Security administration procedures require read-only access to:

- ☐ access control tables.
- ☐ security log files.
- ☐ logging options.
- ☐ user profiles.

Licensed to Berend Post berend.post@it-university.nl

Question 1934

Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

- ☐ True
- ☐ False

Question 1935

When physical destruction is not practical, which of the following is the MOST effective means of disposing of sensitive data on a hard disk?

- ☐ Recycling the disk
- ☐ Reformatting
- ☐ Deleting files sequentially
- ☐ Overwriting multiple times

Question 1936

If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions. True or false?

- ☐ True
- ☐ False

Question 1937

What benefit does using capacity-monitoring software to monitor usage patterns and trends provide to management?

- ☐ The software can dynamically readjust network traffic capabilities based upon current usage.
- ☐ The software produces nice reports that really impress management.
- ☐ It allows users to properly allocate resources and ensure continuous efficiency of operations.
- ☐ It allows management to properly allocate resources and ensure continuous efficiency of operations.

Licensed to Berend Post berend.post@it-university.nl

Question 1938

As part of an international expansion plan, an organization has acquired a company located in another jurisdiction. Which of the following would be the BEST way to maintain an effective information security program?

- ☐ Determine new factors that could influence the information security strategy.
- ☐ Implement the current information security program in the acquired company.
- ☐ Merge the two information security programs to establish continuity.
- ☐ Ensure information security is included in any change control efforts.

Question 1939

Which of the following type of a computer network are variation of LAN and are dedicated to connecting storage devices to servers and other computing devices?

- ☐ LAN
- ☐ MAN
- ☐ SAN
- ☐ PAN

Question 1940

When reviewing a disaster recovery plan (DRP), an IS auditor should examine the:

- ☐ access to the computer site by backup staff.
- ☐ offsite data file storage.
- ☐ uninterruptible power supply (UPS).
- ☐ fire-fighting equipment.

Question 1941

Which of the following type of an IDS resides on important systems like database, critical servers and monitors various internal resources of an operating system?

- ☐ Signature based IDS
- ☐ Host based IDS
- ☐ Network based IDS
- ☐ Statistical based IDS

Licensed to Berend Post berend.post@it-university.nl

Question 1942

Which of the following is the GREATEST concern when an organization's backup facility is at a warm site?

- ☐ Timely availability of hardware
- ☐ Availability of heat, humidity and air conditioning equipment
- ☐ Adequacy of electrical power connections
- ☐ Effectiveness of the telecommunications network

Question 1943

Which of the following is the BEST practice to ensure that access authorizations are still valid?

- ☐ information owner provides authorization for users to gain access
- ☐ identity management is integrated with human resource processes
- ☐ information owners periodically review the access controls
- ☐ An authorization matrix is used to establish validity of access

Question 1944

What is/are used to measure and ensure proper network capacity management and availability of services?

- ☐ Network performance-monitoring tools
- ☐ Network component redundancy
- ☐ Syslog reporting
- ☐ IT strategic planning

Question 1945

Which of the following is the GREATEST risk resulting from conducting periodic reviews of IT over several years based on the same audit program?

- ☐ The amount of errors will increase because the routine work promotes inattentiveness.
- ☐ Detection risk is increased because auditees already know the audit program.
- ☐ Audit risk is increased because the programs might not be adapted to the organization’s current situation.
- ☐ Staff turnover in the audit department will increase because fieldwork becomes less interesting.

Licensed to Berend Post berend.post@it-university.nl

Question 1946

Which of the following is the GREATEST benefit of implementing an incident management process?

- ☐ Opportunity for frequent reassessment of incidents
- ☐ Reduction in security threats
- ☐ Reduction in the business impact of incidents
- ☐ Reduction of costs by the efficient use of resources

Question 1947

Which of the following would provide the BEST protection against the hacking of a computer connected to the Internet?

- ☐ A remote access server
- ☐ A proxy server
- ☐ A personal firewall
- ☐ A password-generating token

Question 1948

Which of the following potentially blocks hacking attempts?

- ☐ intrusion detection system
- ☐ Honeypot system
- ☐ Intrusion prevention system
- ☐ Network security scanner

Question 1949

Which of the following is the BEST indicator of the effectiveness of signature-based intrusion detection systems?

- ☐ An increase in the number of identified false positives
- ☐ An increase in the number of unfamiliar sources of intruders
- ☐ An increase in the number of detected incidents not previously identified
- ☐ An increase in the number of internally reported critical incidents

Question 1950

Which of the following would be an INAPPROPRIATE activity for a network administrator?

- ☐ Analyzing network security incidents
- ☐ Prioritizing traffic between subnets
- ☐ Modifying a router configuration
- ☐ Modifying router log files

Licensed to Berend Post berend.post@it-university.nl

Question 1951

When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

- ☐ whose sum of activity time is the shortest.
- ☐ that have zero slack time.
- ☐ that give the longest possible completion time.
- ☐ whose sum of slack time is the shortest.

Question 1952

Whenever an application is modified, what should be tested to determine the full impact of the change?

- ☐ Interface systems with other applications or systems
- ☐ The entire program, including any interface systems with other applications or systems
- ☐ All programs, including interface systems with other applications or systems
- ☐ Mission-critical functions and any interface systems with other applications or systems

Question 1953

Involvement of senior management is MOST important in the development of:

- ☐ strategic plans.
- ☐ IS policies.
- ☐ IS procedures.
- ☐ standards and guidelines.

Question 1954

Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?

- ☐ Halon gas
- ☐ Wet-pipe sprinklers
- ☐ Dry-pipe sprinklers
- ☐ Carbon dioxide gas

Licensed to Berend Post berend.post@it-university.nl

Question 1955

IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

- ☐ The outsourcing contract does not cover disaster recovery for the outsourced IT operations.
- ☐ The service provider does not have incident handling procedures.
- ☐ Recently a corrupted database could not be recovered because of library management problems.
- ☐ incident logs are not being reviewed.

Question 1956

Responsibility and reporting lines cannot always be established when auditing automated systems since:

- ☐ diversified control makes ownership irrelevant.
- ☐ staff traditionally changes jobs with greater frequency.
- ☐ ownership is difficult to establish where resources are shared.
- ☐ duties change frequently in the rapid development of technology.

Question 1957

Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

- ☐ Time zone differences could impede communications between IT teams.
- ☐ Telecommunications cost could be much higher in the first year.
- ☐ Privacy laws could prevent cross-border flow of information.
- ☐ Software development may require more detailed specifications.

Question 1958

An objective of capacity management is to ensure that:

- ☐ organizational resources are used efficiently.
- ☐ available resources are fully utilized.
- ☐ new resources are allocated for new applications.
- ☐ resource utilization does not drop below 85%.

Licensed to Berend Post berend.post@it-university.nl

Question 1959

An IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could an IS auditor use to estimate the size of the development effort?

- ☐ Program evaluation review technique (PERT)
- ☐ Counting source lines of code (SLOC)
- ☐ Function point analysis
- ☐ White box testing

Question 1960

An online retailer is receiving customer about receiving different items from what they ordered on the organization's website. The root cause has been traced to poor data quality. Despite efforts to clean erroneous data from the system, multiple data quality issues continue to occur. Which of the following recommendations would be the BEST way to reduce the likelihood of future occurrences?

- ☐ Implement business rules to validate employee data entry.
- ☐ Invest in additional employee training for data entry.
- ☐ Assign responsibility for improving data quality.
- ☐ Outsource data cleansing activities to reliable third parties.

Question 1961

If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

- ☐ Documentation development
- ☐ Comprehensive integration testing
- ☐ Full unit testing
- ☐ Full regression testing

Question 1962

An IS audit of an organization's data classification policies finds some areas of the policies may not be up-to-date with new data privacy regulations. What should management do FIRST to address the risk of noncompliance?

- ☐ Conduct a privacy impact assessment to identify gaps
- ☐ Reclassify information based on revised information classification labels
- ☐ Mandate training on the new privacy regulations
- ☐ Perform a data discovery exercise to identify all personal data

Licensed to Berend Post berend.post@it-university.nl

Question 1963

The MOST important reason that security risk assessment should be conducted frequently throughout an organization is because:

- ☐ threats to the organization may change.
- ☐ controls should be regularly tested.
- ☐ compliance with legal and regulatory standards should be reassessed.
- ☐ control effectiveness may weaken.

Question 1964

Which of the following are examples of tools for launching Distributed DoS Attack (Choose four.):

- ☐ TFN
- ☐ TFN2K
- ☐ Trin00
- ☐ Stacheldracht
- ☐ Tripwire

Question 1965

For mission-critical applications with a low recovery time objective (RTO), which of the following is the BEST backup strategy?

- ☐ Frequent back-ups to tape
- ☐ Mirroring
- ☐ Use of virtual tape libraries
- ☐ Archiving to conventional disk

Question 1966

Which of the following is the MOST important prerequisite to performing an information security assessment?

- ☐ Reviewing the business impact analysis (BIA)
- ☐ Assessing threats and vulnerabilities
- ☐ Determining risk tolerance
- ☐ Classifying assets

Licensed to Berend Post berend.post@it-university.nl

Question 1967

Which of the following is MOST important when planning a network audit?

- ☐ Determination of IP range in use
- ☐ Isolation of rogue access points
- ☐ Identification of existing nodes
- ☐ Analysis of traffic content

Question 1968

Which of the following is the MOST important feature of access control software?

- ☐ Authentication
- ☐ Violation reporting
- ☐ Nonrepudiation
- ☐ Identification

Question 1969

An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus PRIMARILY on defining:

- ☐ security requirements for the process being outsourced
- ☐ security metrics
- ☐ service level agreements (SLAs)
- ☐ risk-reporting methodologies

Question 1970

An organization implements a data loss prevention tool as a control to mitigate the risk of sensitive data leaving the organization via electronic mail. Which of the following would provide the BEST indication of adequate control design?

- ☐ Management has formally approved the control design.
- ☐ Management presents evidence that data loss incidents have decreased.
- ☐ Security administrators can demonstrate the functions of the tool.
- ☐ Rules enforced by the tool were based on the classification of the data.

Question 1971

Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

- ☐ True
- ☐ False

Licensed to Berend Post berend.post@it-university.nl

Question 1972

In RFID technology which of the following risk could represent a threat to non-RFID networked or collocated systems, assets, and people?

- ☐ Business Process Risk
- ☐ Business Intelligence Risk
- ☐ Privacy Risk
- ☐ Externality Risk

Question 1973

Which of the following software tools is often used for stealing money from infected PC owner through taking control of the modem?

- ☐ System patcher
- ☐ Porn dialer
- ☐ War dialer
- ☐ T1 dialer
- ☐ T3 dialer
- ☐ None of the choices.

Question 1974

Which of the following would provide the MOST reliable evidence to indicate whether employee access has been deactivated in a timely manner following termination?

- ☐ Comparing termination forms with dates in the HR system
- ☐ Reviewing hardware return-of-asset forms
- ☐ Interviewing supervisors to verify employee data is being updated immediately
- ☐ Comparing termination forms with system transaction log entries

Question 1975

Which of the following should be the GREATEST concern to an IS auditor reviewing the information security framework of an organization?

- ☐ The information security policy has not been updated in the last two years.
- ☐ A list of critical information assets was not included in the information security policy.
- ☐ Senior management was not involved in the development of the information security policy.
- ☐ The information security policy is not aligned with regulatory requirements.

Licensed to Berend Post berend.post@it-university.nl

Question 1976

Which of the following is necessary to determine what would constitute a disaster for an organization?

- ☐ Backup strategy analysis
- ☐ Threat probability analysis
- ☐ Risk analysis
- ☐ Recovery strategy analysis

Question 1977

Which of the following would be the MOST effective method to identify high risk areas in the business to be included in the audit plan?

- ☐ Validate current risk from prior internal audit findings.
- ☐ Review industry reports to identify common risk areas.
- ☐ Engage with management to understand the business.
- ☐ Review external audit reports of the business.

Question 1978

Gimmes often work through:

- ☐ SMS
- ☐ IRC chat
- ☐ email attachment
- ☐ news
- ☐ file download
- ☐ None of the choices.

Question 1979

Which of the following findings should an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?

- ☐ There are three individuals with a key to enter the area.
- ☐ Paper documents are also stored in the offsite vault.
- ☐ Data files that are stored in the vault are synchronized.
- ☐ The offsite vault is located in a separate facility.

Licensed to Berend Post berend.post@it-university.nl

Question 1980

An effective implementation of security roles and responsibilities is BEST evidenced across an enterprise when:

- ☐ operational activities are aligned with policies.
- ☐ policies are signed off by users.
- ☐ policies are rolled out and disseminated.
- ☐ reviews and updates of policies are regularly performed.

Question 1981

Which of the following should occur EARLIEST in a business continuity management lifecycle?

- ☐ Defining business continuity procedures
- ☐ Identifying critical business processes
- ☐ Developing a training and awareness program
- ☐ Carrying out a threat and risk assessment

Question 1982

An internal audit department recently established a quality assurance (QA) program as part of its overall audit program. Which of the following activities should be included as part of the QA program requirements?

- ☐ Reporting program results to the board
- ☐ Reviewing audit standards periodically
- ☐ Analyzing user satisfaction reports from business lines
- ☐ Conducting long-term planning for internal audit staffing

Question 1983

During the review of a web-based software development project, an IS auditor realizes that coding standards are not enforced and code reviews are rarely carried out. This will MOST likely increase the likelihood of a successful:

- ☐ buffer overflow.
- ☐ brute force attack.
- ☐ distributed denial-of-service attack.
- ☐ war dialing attack.

Licensed to Berend Post berend.post@it-university.nl

Question 1984

Which of the following would be MOST important for an IS auditor to review during an audit of an automated continuous monitoring process being used by the finance department?

- ☐ Resiliency of the monitoring service
- ☐ Dual control and approvals embedded in processes
- ☐ Management sign-off of test documentation
- ☐ Configuration of the monitoring tool

Question 1985

How does the SSL network protocol provide confidentiality?

- ☐ Through symmetric encryption such as RSA
- ☐ Through asymmetric encryption such as Data Encryption Standard, or DES
- ☐ Through asymmetric encryption such as Advanced Encryption Standard, or AES
- ☐ Through symmetric encryption such as Data Encryption Standard, or DES

Question 1986

Effective IT governance will ensure that the IT plan is consistent with the organization's:

- ☐ business plan.
- ☐ audit plan.
- ☐ security plan.
- ☐ investment plan.

Question 1987

Which of the following is the PRIMARY purpose for conducting parallel testing?

- ☐ To determine if the system is cost-effective
- ☐ To enable comprehensive unit and system testing
- ☐ To highlight errors in the program interfaces with files
- ☐ To ensure the new system meets user requirements

Question 1988

Cross-site scripting (XSS) attacks are BEST prevented through:

- ☐ use of common industry frameworks.
- ☐ secure coding practices.
- ☐ application firewall policy settings.
- ☐ a three-tier web architecture.

Licensed to Berend Post berend.post@it-university.nl

Question 1989

Which of the following insurance types provide for a loss arising from fraudulent acts by employees?

- ☐ Business interruption
- ☐ Fidelity coverage
- ☐ Errors and omissions
- ☐ Extra expense

Question 1990

In which phase of penetration testing would host detection and domain name system (DNS) interrogation be performed?

- ☐ Reporting
- ☐ Attacks
- ☐ Discovery
- ☐ Planning

Question 1991

In the context of physical access control, what is known as the process of verifying user identities?

- ☐ Authentication
- ☐ Authorization
- ☐ Accounting
- ☐ Encryption
- ☐ Compression
- ☐ None of the choices.

Question 1992

During the audit of a database server, which of the following would be considered the GREATEST exposure?

- ☐ The password does not expire on the administrator account
- ☐ Default global security settings for the database remain unchanged
- ☐ Old data have not been purged
- ☐ Database activity is not fully logged

Licensed to Berend Post berend.post@it-university.nl

Question 1993

What is the FIRST step an auditor should take when beginning a follow-up audit?

- ☐ Review workpapers from the previous audit.
- ☐ Gather evidence of remediation to conduct tests of controls.
- ☐ Review previous findings and action plans.
- ☐ Meet with the auditee to discuss remediation progress.

Question 1994

A database administrator is responsible for:

- ☐ defining data ownership.
- ☐ establishing operational standards for the data dictionary.
- ☐ creating the logical and physical database.
- ☐ establishing ground rules for ensuring data integrity and security.

Question 1995

Which of the following tools BEST demonstrate the effectiveness of the information security program?

- ☐ A security balanced scorecard
- ☐ Management satisfaction surveys
- ☐ Risk heat map
- ☐ Key risk indicators (KRIs)

Question 1996

Which of the following is the BEST way to increase the effectiveness of security incident detection?

- ☐ Determining containment activities based on the type of incident
- ☐ Establishing service level agreements (SLAs) with appropriate forensic service providers
- ☐ Educating end users on identifying suspicious activity
- ☐ Documenting root cause analysis procedures

Licensed to Berend Post berend.post@it-university.nl

Question 1997

You should keep all computer rooms at reasonable humidity levels, which are in between:

- ☐ 20 - 70 percent.
- ☐ 10 - 70 percent.
- ☐ 10 - 60 percent.
- ☐ 70 - 90 percent.
- ☐ 60 - 80 percent.
- ☐ None of the choices.

Question 1998

Which of the following is the MOST significant risk associated with the use of virtualization?

- ☐ Insufficient network bandwidth
- ☐ Single point of failure
- ☐ Inadequate configuration
- ☐ Performance issues of hosts

Question 1999

Which of the following would be BEST prevented by a raised floor in the computer machine room?

- ☐ Damage of wires around computers and servers
- ☐ A power failure from static electricity
- ☐ Shocks from earthquakes
- ☐ Water flood damage.

Question 2000

A data breach has occurred at a third-party vendor used by an organization to outsource the processing of its customer data. What should be management's FIRST course of action?

- ☐ Activate the disaster recovery plan
- ☐ Notify the insurance company of the potential claim
- ☐ Activate the incident management process
- ☐ Take legal action against the service provider for reputation damage

Licensed to Berend Post berend.post@it-university.nl

Question 2001

An investment advisor e-mails periodic newsletters to clients and wants reasonable assurance that no one has modified the newsletter. This objective can be achieved by:

- ☐ encrypting the hash of the newsletter using the advisor's private key.
- ☐ encrypting the hash of the newsletter using the advisor's public key.
- ☐ digitally signing the document using the advisor's private key.
- ☐ encrypting the newsletter using the advisor's private key.

Question 2002

Requiring that passwords contain a combination of numeric and alphabetic characters is MOST effective against which type of attack?

- ☐ Denial of service
- ☐ Dictionary
- ☐ Social engineering
- ☐ Programmed

Question 2003

A client/server configuration will:

- ☐ optimize system performance by having a server on a front-end and clients on a host
- ☐ enhance system performance through the separation of front-end and back-end processes
- ☐ keep track of all the clients using the IS facilities of a service organization
- ☐ limit the clients and servers' relationship by limiting the IS facilities to a single hardware system

Question 2004

Which of the following function in traditional EDI process is used for transmitting and receiving electronic documents between trading partners via dial up lines, public switched network or VAN?

- ☐ Communication handler
- ☐ EDI Interface
- ☐ Application System
- ☐ EDI Translator

Licensed to Berend Post berend.post@it-university.nl

Question 2005

What should be the PRIMARY objective of conducting interviews with business unit managers when developing an information security strategy?

- ☐ Obtain information on department goals.
- ☐ Classify information assets.
- ☐ Identify data and system ownership.
- ☐ Determine information types.

Question 2006

Which of the following is a benefit of a risk-based approach to audit planning? Audit:

- ☐ scheduling may be performed months in advance.
- ☐ budgets are more likely to be met by the IS audit staff.
- ☐ staff will be exposed to a variety of technologies.
- ☐ resources are allocated to the areas of highest concern

Question 2007

An employee loses a mobile device resulting in loss of sensitive corporate data. Which of the following would have BEST prevented data leakage?

- ☐ Awareness training for mobile device users
- ☐ Data encryption on the mobile device
- ☐ The triggering of remote data wipe capabilities
- ☐ Complex password policy for mobile devices

Question 2008

Which of the following is necessary for the effective risk management in IT governance?

- ☐ Risk evaluation is embedded in management processes
- ☐ Risk management strategy is approved by the audit committee
- ☐ Local managers are solely responsible for risk evaluation
- ☐ IT risk management is separate from corporate risk management

Licensed to Berend Post berend.post@it-university.nl

Question 2009

To help ensure the organization's information assets are adequately protected, which of the following considerations is MOST important when developing an information classification and handling policy?

- ☐ The policy has been mapped against industry frameworks for classifying information assets.
- ☐ The policy is owned by the head of information security, who has the authority to enforce the policy.
- ☐ The policy specifies requirements to safeguard information assets based on their importance to the organization.
- ☐ The policy is subject to periodic reviews to ensure its provisions are up to date.

Question 2010

Which of the following would be the GREATEST concern to an IS auditor reviewing an IT outsourcing arrangement?

- ☐ Several IT personnel perform the same functions as the vendor.
- ☐ The contract does not include a renewal option.
- ☐ Development of KPIs that will be used was assigned to the vendor.
- ☐ Some penalties were waived during contract negotiations.

Question 2011

Which of the following option INCORRECTLY describes PBX feature?

- ☐ Voice mail -Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.
- ☐ Tenanting-Provides for the possibility to break into a busy line to inform another user an important message
- ☐ Automatic Call Distribution - Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available
- ☐ Diagnostics -Allows for bypassing normal call restriction procedures

Question 2012

Which of the following is MOST likely to be prevented by a firewall connected to the Internet?

- ☐ Dial-in penetration attacks
- ☐ Disclosure of public key infrastructure (PKI) keys
- ☐ Alteration of email message content
- ☐ External spoofing of internal addresses

Licensed to Berend Post berend.post@it-university.nl

Question 2013

The security level of a private key system depends on the number of:

- ☐ encryption key bits.
- ☐ messages sent.
- ☐ keys.
- ☐ channels used.

Question 2014

An accuracy measure for a biometric system is:

- ☐ system response time.
- ☐ registration time.
- ☐ input file size.
- ☐ false-acceptance rate.

Question 2015

Who is ultimately accountable for the development of an IS security policy?

- ☐ The board of directors
- ☐ Middle management
- ☐ Security administrators
- ☐ Network administrators

Question 2016

An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long. Which of the following could be caused by the length of the cable?

- ☐ Electromagnetic interference (EMI)
- ☐ Cross-talk
- ☐ Dispersion
- ☐ Attenuation

Question 2017

Which of the following should be of MOST concern to an IS auditor reviewing an organization's disaster recovery plan (DRP)?

- ☐ The responsibility for declaring a disaster is not identified.
- ☐ The disaster recovery steps are not detailed.
- ☐ The CIO has not signed off on the DRP.
- ☐ Copies of the DRP are not kept in a secure offsite location.

Licensed to Berend Post berend.post@it-university.nl

Question 2018

Which of the following is the BEST IS audit strategy?

- ☐ Perform audits based on impact and probability of error and failure.
- ☐ Cycle general control and application audits over a two-year period.
- ☐ Conduct general control audits annually and application audits in alternating years.
- ☐ Limit audits to new application system developments.

Question 2019

Which of the following statement INCORRECTLY describes the traditional audit approach in comparison to the Control self-assessment approach?

- ☐ In traditional approach, Staffs at all level, in all functions, are the primary control analyst.
- ☐ Traditional approach assigns duties/supervises staff
- ☐ Traditional approach is a policy driven approach
- ☐ Traditional approach requires limited employee participations.

Question 2020

Which of the following should be the GREATEST concern to an IS auditor evaluating an organization's policies?

- ☐ Policies are not formally approved by the management.
- ☐ Policies are nor formally acknowledged and signed by employees.
- ☐ Policies do not provide adequate protection to the organization.
- ☐ Policies are not reviewed and updated frequently.

Question 2021

Which of the following may be deployed in a network as lower cost surveillance and early-warning tools?

- ☐ Honeypots
- ☐ Hardware IPSs
- ☐ Hardware IDSs
- ☐ Botnets
- ☐ Stateful inspection firewalls
- ☐ Stateful logging facilities
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 2022

What is the MOST important role of a Certificate Authority (CA) when a private key becomes compromised?

- ☐ Issue a new private key to the user
- ☐ Refresh the key information database in the certificate publishing server
- ☐ Publish the certificate revocation lists (CRL) into the repository
- ☐ Refresh the metadata of the certificates

Question 2023

An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's MAIN concern should be that the:

- ☐ complexity and risks associated with the project have been analyzed.
- ☐ resources needed throughout the project have been determined.
- ☐ project deliverables have been identified.
- ☐ a contract for external parties involved in the project has been completed.

Question 2024

When performing an audit of access rights, an IS auditor should be suspicious of which of the following if allocated to a computer operator?

- ☐ Read access to data
- ☐ Delete access to transaction data files
- ☐ Logged read/execute access to programs
- ☐ Update access to job control language/script files

Question 2025

Sophisticated database systems provide many layers and types of security, including (Choose three.):

- ☐ Access control
- ☐ Auditing
- ☐ Encryption
- ☐ Integrity controls
- ☐ Compression controls

Licensed to Berend Post berend.post@it-university.nl

Question 2026

Which of the following forms of evidence for the auditor would be considered the MOST reliable?

- ☐ An oral statement from the auditee
- ☐ The results of a test performed by an IS auditor
- ☐ An internally generated computer accounting report
- ☐ A confirmation letter received from an outside source

Question 2027

When reviewing the configuration of network devices, an IS auditor should FIRST identify:

- ☐ the best practices for the type of network devices deployed.
- ☐ whether components of the network are missing.
- ☐ the importance of the network device in the topology.
- ☐ whether subcomponents of the network are being used appropriately.

Question 2028

An IS auditor should be concerned when a telecommunication analyst:

- ☐ monitors systems performance and tracks problems resulting from program changes.
- ☐ reviews network load requirements in terms of current and future transaction volumes.
- ☐ assesses the impact of the network load on terminal response times and network data transfer rates.
- ☐ recommends network balancing procedures and improvements.

Question 2029

What influences decisions regarding criticality of assets?

- ☐ The business criticality of the data to be protected
- ☐ Internal corporate politics
- ☐ The business criticality of the data to be protected, and the scope of the impact upon the organization as a whole
- ☐ The business impact analysis

Licensed to Berend Post berend.post@it-university.nl

Question 2030

An information security manager learns that a departmental system is out of compliance with the information security policy's authentication requirements. Which of the following should be the information security manager's FIRST course of action?

- ☐ Isolate the noncompliant system from the rest of the network.
- ☐ Submit the issue to the steering committee for escalation.
- ☐ Request risk acceptance from senior management.
- ☐ Conduct an impact analysis to quantify the associated risk.

Question 2031

Which of the following provides the BEST evidence of successfully completed batch uploads?

- ☐ Sign-off on the batch journal
- ☐ Using sequence controls
- ☐ Enforcing batch cut-off times
- ☐ Reviewing process logs

Question 2032

Which of the following protocol is developed jointly by VISA and Master Card to secure payment transactions among all parties involved in credit card transactions on behalf of cardholders and merchants?

- ☐ S/MIME
- ☐ SSH
- ☐ SET
- ☐ S/HTTP

Question 2033

Which of the following is MOST likely to result from compliance testing?

- ☐ Comparison of data with physical counts
- ☐ Confirmation of data with outside sources
- ☐ Identification of errors due to processing mistakes
- ☐ Discovery of controls that have not been applied

Licensed to Berend Post berend.post@it-university.nl

Question 2034

Which type of risk would MOST influence the selection of a sampling methodology?

- ☐ Control
- ☐ Inherent
- ☐ Residual
- ☐ Detection

Question 2035

An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

- ☐ evaluate the record retention plans for off-premises storage.
- ☐ interview programmers about the procedures currently being followed.
- ☐ compare utilization records to operations schedules.
- ☐ review data file access records to test the librarian function.

Question 2036

In which of the following RFID risks competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system?

- ☐ Business Process Risk
- ☐ Business Intelligence Risk
- ☐ Privacy Risk
- ☐ Externality Risk

Question 2037

When developing a security architecture, which of the following steps should be executed FIRST?

- ☐ Developing security procedures
- ☐ Defining a security policy
- ☐ Specifying an access control methodology
- ☐ Defining roles and responsibilities

Licensed to Berend Post berend.post@it-university.nl

Question 2038

The Federal Information Processing Standards (FIPS) were developed by:

- ☐ the United States Federal government
- ☐ ANSI
- ☐ ISO
- ☐ IEEE
- ☐ IANA
- ☐ None of the choices.

Question 2039

What should an organization do before providing an external agency physical access to its information processing facilities (IPFs)?

- ☐ The processes of the external agency should be subjected to an IS audit by an independent agency.
- ☐ Employees of the external agency should be trained on the security procedures of the organization.
- ☐ Any access by an external agency should be limited to the demilitarized zone (DMZ).
- ☐ The organization should conduct a risk assessment and design and implement appropriate controls.

Question 2040

The BEST way to obtain funding from senior management for a security awareness program is to:

- ☐ meet regulatory requirements
- ☐ produce an impact analysis report of potential breaches
- ☐ demonstrate that the program will adequately reduce risk
- ☐ produce a report of organizational risks

Question 2041

Which of the following is the PRIMARY objective of an IT performance measurement process?

- ☐ Minimize errors
- ☐ Gather performance data
- ☐ Establish performance baselines
- ☐ Optimize performance

Licensed to Berend Post berend.post@it-university.nl

Question 2042

Reviewing project plans and status reports throughout the development life cycle will:

- ☐ eliminate the need to perform a risk assessment.
- ☐ postpone documenting the project's progress until the final phase.
- ☐ guarantee that the project will meet its intended deliverables.
- ☐ facilitate the optimal use of resources over the life of the project.

Question 2043

Which of the following should be of GREATEST concern to an IS auditor conducting an audit of an organization's backup processes?

- ☐ A written backup policy is not available.
- ☐ Backup failures are not resolved in a timely manner.
- ☐ The restoration process is slow due to connectivity issues.
- ☐ The service levels are not achieved.

Question 2044

A trojan horse simply cannot operate autonomously.

- ☐ true
- ☐ false

Question 2045

Which of the following type of IDS has self-learning functionality and over a period of time will learned what is the expected behavior of a system?

- ☐ Signature Based IDS
- ☐ Host Based IDS
- ☐ Neural Network based IDS
- ☐ Statistical based IDS

Question 2046

Which of the following should be included in an organization's IS security policy?

- ☐ A list of key IT resources to be secured
- ☐ The basis for access authorization
- ☐ Identity of sensitive security features
- ☐ Relevant software security features

Licensed to Berend Post berend.post@it-university.nl

Question 2047

A virtual private network (VPN) provides data confidentiality by using:

- ☐ Secure Sockets Layer (SSL)
- ☐ Tunneling
- ☐ Digital signatures
- ☐ Phishing

Question 2048

What is the primary objective of a control self-assessment (CSA) program?

- ☐ Enhancement of the audit responsibility
- ☐ Elimination of the audit responsibility
- ☐ Replacement of the audit responsibility
- ☐ Integrity of the audit responsibility

Question 2049

Which of the following is the MOST effective way to maintain network integrity when using mobile devices?

- ☐ Perform network reviews.
- ☐ Implement network access control.
- ☐ Implement outbound firewall rules.
- ☐ Review access control lists.

Question 2050

A data administrator is responsible for:

- ☐ maintaining database system software.
- ☐ defining data elements, data names and their relationship.
- ☐ developing physical database structures.
- ☐ developing data dictionary system software.

Question 2051

Which of the following is the MOST effective control to mitigate unintentional misuse of authorized access?

- ☐ Regular monitoring of user access logs
- ☐ Annual sign-off of acceptable use policy
- ☐ Security awareness training
- ☐ Formalized disciplinary action

Licensed to Berend Post berend.post@it-university.nl

Question 2052

Most trojan horse programs are spread through:

- ☐ e-mails.
- ☐ MP3.
- ☐ MS Office.
- ☐ Word template.
- ☐ None of the choices.

Question 2053

During a follow-up audit, an IS auditor finds that the auditee has updated virus scanner definitions without adopting the original audit recommendation to increase the frequency of using the scanner. The MOST appropriate action for the auditor is to:

- ☐ prepare a follow-up audit report reiterating the recommendation.
- ☐ escalate the issue to senior management.
- ☐ modify the audit opinion based on the new information available.
- ☐ conclude that the residual risk is beyond tolerable levels of risk.

Question 2054

Software quality assurance (QA) reviews are planned as part of system development. At which stage in the development process should the first review be initiated?

- ☐ At pre-implementation planning
- ☐ As a part of the user requirements definition
- ☐ Immediately prior to user acceptance testing
- ☐ During the feasibility study

Question 2055

Rather than simply reviewing the adequacy of access control, appropriateness of access policies, and effectiveness of safeguards and procedures, the IS auditor is more concerned with effectiveness and utilization of assets. True or false?

- ☐ True
- ☐ False

Licensed to Berend Post berend.post@it-university.nl

Question 2056

When preventive controls to appropriately mitigate risk are not feasible, which of the following is the MOST important action for the information security manager to perform?

- ☐ Identity unacceptable risk levels
- ☐ Manage the impact
- ☐ Evaluate potential threats
- ☐ Assess vulnerabilities

Question 2057

Which of the following types of attack often take advantage of curiosity or greed to deliver malware?

- ☐ Gimmes
- ☐ Tripwire
- ☐ Icing
- ☐ Soft coding
- ☐ Pretexting
- ☐ None of the choices.

Question 2058

During a disaster recovery test, an IS auditor observes that the performance of the disaster recovery site's server is slow. To find the root cause of this, the IS auditor should FIRST review the:

- ☐ event error log generated at the disaster recovery site.
- ☐ disaster recovery test plan.
- ☐ disaster recovery plan (DRP).
- ☐ configurations and alignment of the primary and disaster recovery sites.

Question 2059

Which of the following would MOST effectively control the usage of universal storage bus (USB) storage devices?

- ☐ Policies that require instant dismissal if such devices are found
- ☐ Software for tracking and managing USB storage devices
- ☐ Administratively disabling the USB port
- ☐ Searching personnel for USB storage devices at the facility's entrance

Licensed to Berend Post berend.post@it-university.nl

Question 2060

Which of the following step of PDCA establishes the objectives and processes necessary to deliver results in accordance with the expected output?

- ☐ Plan
- ☐ Do
- ☐ Check
- ☐ Act

Question 2061

Which of the following virus prevention techniques can be implemented through hardware?

- ☐ Remote booting
- ☐ Heuristic scanners
- ☐ Behavior blockers
- ☐ Immunizers

Question 2062

Which of the following is the MOST significant risk when an application uses individual end user accounts to access the underlying database?

- ☐ User accounts may remain active after a termination.
- ☐ Multiple connects to the database are used and slow the process.
- ☐ Application may not capture a complete audit trail.
- ☐ Users may be able to circumvent application controls.

Question 2063

Which of the following methods should be used to effectively erase sensitive data from portable storage devices that are to be reused?

- ☐ Formatting the portable device
- ☐ Using media sanitization software
- ☐ Overwriting the sensitive data
- ☐ Exposing the portable device to a magnetic field

Licensed to Berend Post berend.post@it-university.nl

Question 2064

Which of the following is MOST important for an organization to complete prior to developing its disaster recovery plan (DRP)?

- ☐ Support staff skill gap analysis
- ☐ Comprehensive IT inventory
- ☐ Business impact analysis (BIA)
- ☐ Risk assessment

Question 2065

How is the time required for transaction processing review usually affected by properly implemented Electronic Data Interface (EDI)?

- ☐ EDI usually decreases the time necessary for review.
- ☐ EDI usually increases the time necessary for review.
- ☐ Cannot be determined.
- ☐ EDI does not affect the time necessary for review.

Question 2066

Which of the following layer of an enterprise data flow architecture does the scheduling of the tasks necessary to build and maintain the Data Warehouse (DW) and also populates Data Marts?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☐ Warehouse management layer
- ☐ Data access layer

Question 2067

Statistical sampling is NOT based on which of the following audit sample techniques?

- ☐ Haphazard Sampling
- ☐ Random Sampling
- ☐ Cell Sampling
- ☐ Fixed interval sampling

Question 2068

When a new system is to be implemented within a short time frame, it is MOST important to:

- ☐ finish writing user manuals.
- ☐ perform user acceptance testing.
- ☐ add last-minute enhancements to functionalities.
- ☐ ensure that the code has been documented and reviewed.

Licensed to Berend Post berend.post@it-university.nl

Question 2069

In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

- ☐ Diskless workstations
- ☐ Data encryption techniques
- ☐ Network monitoring devices
- ☐ Authentication systems

Question 2070

Overall business risk for a particular threat can be expressed as:

- ☐ a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.
- ☐ the magnitude of the impact should a threat source successfully exploit the vulnerability.
- ☐ the likelihood of a given threat source exploiting a given vulnerability.
- ☐ the collective judgment of the risk assessment team.

Question 2071

A month after a company purchased and implemented system and performance monitoring software, reports were too large and therefore were not reviewed or acted upon. The MOST effective plan of action would be to:

- ☐ use analytical tools to produce exception reports from the system and performance monitoring software
- ☐ re-install the system and performance monitoring software
- ☐ evaluate replacement systems and performance monitoring software
- ☐ restrict functionality of system monitoring software to security-related events

Question 2072

An IS auditor observes that an organization's critical IT systems have experienced several failures throughout the year. Which of the following is the BEST recommendation?

- ☐ Perform a disaster recovery test.
- ☐ Perform a root cause analysis.
- ☐ Contract for a hot site.
- ☐ Implement redundant systems.

Licensed to Berend Post berend.post@it-university.nl

Question 2073

Which of the following PBX feature supports shared extensions among several devices, ensuring that only one device at a time can use an extension?

- ☐ Call forwarding
- ☐ Privacy release
- ☐ Tenanting
- ☐ Voice mail

Question 2074

During a disaster recovery audit, an IS auditor finds that a business impact analysis (BIA) has not been performed. The auditor should FIRST:

- ☐ perform a business impact analysis (BIA).
- ☐ issue an intermediate report to management.
- ☐ evaluate the impact on current disaster recovery capability.
- ☐ ?onduct additional compliance testing.

Question 2075

Which of the following is MOST important to include in a contract with a software development service provider?

- ☐ A list of key performance indicators (KPIs)
- ☐ Ownership of intellectual property
- ☐ Service level agreement (SLA)
- ☐ Explicit contract termination requirements

Question 2076

Which of the following is the BEST way for an information security manager to justify continued investment in the information security program when the organization is facing significant budget cuts?

- ☐ Demonstrate an increase in ransomware attacks targeting peer organizations.
- ☐ Demonstrate the readiness of business continuity plans.
- ☐ Demonstrate that implemented program controls are effective.
- ☐ Demonstrate that the program enables business activities.

Licensed to Berend Post berend.post@it-university.nl

Question 2077

When reviewing system parameters, an IS auditor's PRIMARY concern should be that:

- ☐ they are set to meet security and performance requirements.
- ☐ changes are recorded in an audit trail and periodically reviewed.
- ☐ changes are authorized and supported by appropriate documents.
- ☐ access to parameters in the system is restricted.

Question 2078

Which of the following is MOST important for an IS auditor to consider when reviewing the effectiveness of an incident response program?

- ☐ Incidents are categorized according to industry standards.
- ☐ Lessons learned are incorporated into incident response processes.
- ☐ Incidents are escalated to senior management in a timely manner.
- ☐ The plan is reviewed and updated annually.

Question 2079

As part of a follow-up of a previous year's audit, an IS auditor has increased the expected error rate for a sample. The impact will be:

- ☐ degree of assurance increases.
- ☐ standard deviation decreases.
- ☐ sampling risk decreases.
- ☐ required sample size increases.

Question 2080

A source code repository should be designed to:

- ☐ provide automatic incorporation and distribution of modified code.
- ☐ prevent changes from being incorporated into existing code.
- ☐ provide secure versioning and backup capabilities for existing code.
- ☐ prevent developers from accessing secure source code.

Licensed to Berend Post berend.post@it-university.nl

Question 2081

An IS auditor is performing a network security review of a telecom company that provides Internet connection services to shopping malls for their wireless customers. The company uses Wireless Transport Layer Security (WTLS) and Secure Sockets Layer (SSL) technology for protecting their customer's payment information. The IS auditor should be MOST concerned if a hacker:

- ☐ compromises the Wireless Application Protocol (WAP) gateway.
- ☐ installs a sniffing program in front of the server.
- ☐ steals a customer's PDA.
- ☐ listens to the wireless transmission.

Question 2082

Confidentiality of the data transmitted in a wireless LAN is BEST protected if the session is:

- ☐ restricted to predefined MAC addresses.
- ☐ encrypted using static keys.
- ☐ encrypted using dynamic keys.
- ☐ initiated from devices that have encrypted storage.

Question 2083

Which of the following type of lock uses a numeric keypad or dial to gain entry?

- ☐ Bolting door locks
- ☐ Cipher lock
- ☐ Electronic door lock
- ☐ Biometric door lock

Question 2084

An organization using instant messaging to communicate with customers can prevent legitimate customers from being impersonated by:

- ☐ using call monitoring.
- ☐ using firewalls to limit network traffic to authorized ports.
- ☐ logging conversations.
- ☐ authenticating users before conversations are initiated.

Licensed to Berend Post berend.post@it-university.nl

Question 2085

In a botnet, mailbot logs into a particular type of system for making coordinated attack attempts. What type of system is this?

- ☐ Chat system
- ☐ SMS system
- ☐ Email system
- ☐ Log system
- ☐ Kernel system
- ☐ None of the choices.

Question 2086

As part of business continuity planning, which of the following is MOST important to include in a business impact analysis (BIA)?

- ☐ Define a risk appetite.
- ☐ Assess risk of moving significant applications to the cloud.
- ☐ Assess recovery scenarios.
- ☐ Assess threats to the organization.

Question 2087

Many WEP systems require a key in a relatively insecure format. What format is this?

- ☐ binary format.
- ☐ hexadecimal format.
- ☐ 128 bit format.
- ☐ 256 bit format.
- ☐ None of the choices.

Question 2088

During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

- ☐ Dumping the memory content to a file
- ☐ Generating disk images of the compromised system
- ☐ Rebooting the system
- ☐ Removing the system from the network

Licensed to Berend Post berend.post@it-university.nl

Question 2089

Which of the following types of attack almost always requires physical access to the targets?

- ☐ Direct access attack
- ☐ Wireless attack
- ☐ Port attack
- ☐ Window attack
- ☐ System attack
- ☐ None of the choices.

Question 2090

During a routine check, a system administrator identifies unusual activity indicating an intruder within a firewall. Which of the following controls has MOST likely been compromised?

- ☐ Identification
- ☐ Data integrity
- ☐ Data validation
- ☐ Authentication

Question 2091

Cisco IOS based routers perform basic traffic filtering via which of the following mechanisms?

- ☐ datagram scanning
- ☐ access lists
- ☐ stateful inspection
- ☐ state checking
- ☐ link progressing
- ☐ None of the choices.

Question 2092

What can be used to gather evidence of network attacks?

- ☐ Access control lists (ACL)
- ☐ Intrusion-detection systems (IDS)
- ☐ Syslog reporting
- ☐ Antivirus programs

Licensed to Berend Post berend.post@it-university.nl

Question 2093

To address a maintenance problem, a vendor needs remote access to a critical network. The MOST secure and effective solution is to provide the vendor with a:

- ☐ Secure Shell (SSH-2) tunnel for the duration of the problem.
- ☐ two-factor authentication mechanism for network access.
- ☐ dial-in access.
- ☐ virtual private network (VPN) account for the duration of the vendor support contract.

Question 2094

Which of the following controls will MOST effectively detect inconsistent records resulting from the lack of referential integrity in a database management system?

- ☐ Concurrent access controls
- ☐ Incremental data backups
- ☐ Performance monitoring tools
- ☐ Periodic table link checks

Question 2095

Which of the following is the BEST way to detect software license violations?

- ☐ Implementing a corporate policy on copyright infringements and software use.
- ☐ Requiring that all PCs be diskless workstations.
- ☐ Installing metering software on the LAN so applications can be accessed through the metered software.
- ☐ Regularly scanning PCs in use to ensure that unauthorized copies of software have not been loaded on the PC.

Question 2096

An IS auditor seeks assurance that a new process for purging transactions does not have a detrimental impact on the integrity of a database. This could be achieved BEST by analyzing the:

- ☐ database structure.
- ☐ design of triggers.
- ☐ results of the process in a test environment.
- ☐ entity relationship diagram of the database.

Licensed to Berend Post berend.post@it-university.nl

Question 2097

Which of the following types of testing would determine whether a new or modifies system can operate in its target environment without adversely impacting other existing systems?

- ☐ Parallel testing
- ☐ Pilot testing
- ☐ Interface/integration testing
- ☐ Sociability testing

Question 2098

Which of the following threats is prevented by using token-based authentication?

- ☐ Password sniffing attack on the network
- ☐ Session eavesdropping attack on the network
- ☐ Man-in-the-middle attack on the client
- ☐ Denial of service attack over the network

Question 2099

Sam is the security Manager of a financial institute. Senior management has requested he performs a risk analysis on all critical vulnerabilities reported by an IS auditor. After completing the risk analysis, Sam has observed that for a few of the risks, the cost benefit analysis shows that risk mitigation cost (countermeasures, controls, or safeguard) is more than the potential lost that could be incurred. What kind of a strategy should Sam recommend to the senior management to treat these risks?

- ☐ Risk Mitigation
- ☐ Risk Acceptance
- ☐ Risk Avoidance
- ☐ Risk transfer

Question 2100

Which of the following component of an expert system allows the expert to enter knowledge into the system without the traditional mediation of a software engineer?

- ☐ Decision tree
- ☐ Rules
- ☐ Semantic nets
- ☐ Knowledge interface

Licensed to Berend Post berend.post@it-university.nl

Question 2101

Which of the following methods should be used to purge confidential data from write-once optical media?

- ☐ Degauss the media.
- ☐ Destroy the media.
- ☐ Remove the references to data from the access index.
- ☐ Write over the data with null values.

Question 2102

Human error is being HEAVILY relied upon on by which of the following types of attack?

- ☐ Eavedropping
- ☐ DoS
- ☐ DDoS
- ☐ ATP
- ☐ Social Engineering
- ☐ None of the choices.

Question 2103

Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

- ☐ Discussion with management
- ☐ Review of the organization chart
- ☐ Observation and interviews
- ☐ Testing of user access rights

Question 2104

In regard to moving an application program from the test environment to the production environment, the BEST control would be to have the:

- ☐ application programmer copy the source program and compiled object module to the production libraries
- ☐ application programmer copy the source program to the production libraries and then have the production control group compile the program.
- ☐ production control group compile the object module to the production libraries using the source program in the test environment.
- ☐ production control group copy the source program to the production libraries and then compile the program.

Licensed to Berend Post berend.post@it-university.nl

Question 2105

An organization is considering using production data for testing a new application's functionality. Which of the following data protection techniques would BEST ensure that personal data cannot be inadvertently recovered in test environments while also reducing the need for strict confidentiality of the data?

- ☐ Data anonymization
- ☐ Data minimization
- ☐ Data normalization
- ☐ Data encryption

Question 2106

Which of the following BEST enables staff acceptance of information security policies?

- ☐ Strong senior management support
- ☐ Adequate security funding
- ☐ Computer-based training
- ☐ A robust incident response program

Question 2107

Which of the following would BEST assist an information security manager in gaining strategic support from executive management?

- ☐ Research on trends in global information security breaches
- ☐ Risk analysis specific to the organization
- ☐ Annual report of security incidents within the organization
- ☐ Rating of the organization's security based on international standards

Question 2108

An IS auditor reviewing an accounts payable system discovers that audit logs are not being reviewed. When this issue is raised with management the response is that additional controls are not necessary because effective system access controls are in place. The BEST response the auditor can make is to:

- ☐ review the integrity of system access controls.
- ☐ accept management's statement that effective access controls are in place.
- ☐ stress the importance of having a system control framework in place.
- ☐ review the background checks of the accounts payable staff.

Licensed to Berend Post berend.post@it-university.nl

Question 2109

The FIRST step in data classification is to:

- ☐ establish ownership.
- ☐ perform a criticality analysis.
- ☐ define access rules.
- ☐ create a data dictionary.

Question 2110

What would be an IS auditor's BEST recommendation upon finding that a third-party IT service provider hosts the organization's human resources (HR) system in a foreign country?

- ☐ Conduct a privacy impact analysis.
- ☐ Implement change management review.
- ☐ Review third-party audit reports.
- ☐ Perform background verification checks.

Question 2111

Mitigating the risk and impact of a disaster or business interruption usually takes priority over transference of risk to a third party such as an insurer. True or false?

- ☐ True
- ☐ False

Question 2112

There are several types of penetration tests depending upon the scope, objective and nature of a test. Which of the following describes a penetration test where you attack and attempt to circumvent the controls of the targeted network from the outside, usually the Internet?

- ☐ External Testing
- ☐ Internal Testing
- ☐ Blind Testing
- ☐ Targeted Testing

Licensed to Berend Post berend.post@it-university.nl

Question 2113

A core business unit relies on an effective legacy system that does not meet the current security standards and threatens the enterprise network. Which of the following is the BESTcourse of action to address the situation?

- ☐ Require that new systems that can meet the standards be implemented.
- ☐ Document the deficiencies in the risk register.
- ☐ Develop processes to compensate for the deficiencies.
- ☐ Disconnect the legacy system from the rest of the network.

Question 2114

An IS auditor finds that the process for removing access for terminated employees is not documented. What is the MOST significant risk from this observation?

- ☐ Procedures may not align with best practices.
- ☐ HR records may not match system access.
- ☐ Unauthorized access cannot be identified.
- ☐ Access rights may not be removed in a timely manner.

Question 2115

Which of the following would BEST demonstrate that an effective disaster recovery plan (DRP) is in place?

- ☐ Periodic risk assessment
- ☐ Full operational test
- ☐ Frequent testing of backups
- ☐ Annual walk-through testing

Question 2116

An IS auditor reviewing the threat assessment for a data center would be MOST concerned if:

- ☐ all identified threats relate to external entities
- ☐ some of the identified threats are unlikely to occur
- ☐ neighboring organizations' operations have been included
- ☐ the exercise was completed by local management

Licensed to Berend Post berend.post@it-university.nl

Question 2117

Which of the following statement INCORRECTLY describes the Control self-assessment (CSA) approach?

- ☐ CSA is policy or rule driven
- ☐ CSA Empowered/accountable employees
- ☐ CSA focuses on continuous improvement/learning curve
- ☐ In CSA, Staffs at all level, in all functions, are the primary control analyst.

Question 2118

During the due diligence phase of an acquisition, the MOST important course of action for an information security manager would be to:

- ☐ review the state of security awareness
- ☐ perform a gap analysis
- ☐ perform a risk assessment
- ☐ review information security policies

Question 2119

Identify the INCORRECT statement related to network performance below?

- ☐ Bandwidth - Bandwidth commonly measured in bits/second is the maximum rate that information can be transferred
- ☐ Latency - Latency the actual rate that information is transferred
- ☐ Jitter - Jitter variation in the time of arrival at the receiver of the information
- ☐ Error Rate - Error rate the number of corrupted bits expressed as a percentage or fraction of the total sent

Question 2120

When reviewing the implementation of a LAN, an IS auditor should FIRST review the:

- ☐ node list.
- ☐ acceptance test report.
- ☐ network diagram.
- ☐ user's list.

Licensed to Berend Post berend.post@it-university.nl

Question 2121

Which of the following statement is NOT true about Voice-Over IP (VoIP)?

- ☐ VoIP uses circuit switching technology
- ☐ Lower cost per call or even free calls, especially for long distance call
- ☐ Lower infrastructure cost
- ☐ VoIP is a technology where voice traffic is carried on top of existing data infrastructure

Question 2122

Which of the following should an IS auditor be MOST concerned with when a system uses radio frequency identification (RFID)?

- ☐ Scalability
- ☐ Maintainability
- ☐ Nonrepudiation
- ☐ Privacy

Question 2123

The MAIN criterion for determining the severity level of a service disruption incident is:

- ☐ cost of recovery.
- ☐ negative public opinion.
- ☐ geographic location.
- ☐ downtime.

Question 2124

When auditing a software development project, a review of which of the following will BEST verify that project work is adequately subdivided?

- ☐ Work breakdown structure
- ☐ Statement of work
- ☐ Scope statement
- ☐ Functional and technical design documents

Licensed to Berend Post berend.post@it-university.nl

Question 2125

A hacker could obtain passwords without the use of computer tools or programs through the technique of:

- ☐ social engineering.
- ☐ sniffers.
- ☐ back doors.
- ☐ Trojan horses.

Question 2126

Which of the following provides an IS auditor the MOST assurance that an organization is compliant with legal and regulatory requirements?

- ☐ The IT manager is responsible for the organization's compliance with legal and regulatory requirements.
- ☐ Controls associated with legal and regulatory requirements have been identified and tested.
- ☐ Senior management has provided attestation of legal and regulatory compliance.
- ☐ There is no history of complaints or fines from regulators regarding noncompliance.

Question 2127

Which of the following should be of GREATEST concern to an IS auditor reviewing an organization's information security program?

- ☐ The program was not formally signed off by the sponsor.
- ☐ Key performance indicators (KPIs) are not established.
- ☐ Not all IT staff are aware of the program.
- ☐ The program was last updated five years ago.

Question 2128

An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

- ☐ variable sampling.
- ☐ substantive testing.
- ☐ compliance testing.
- ☐ stop-or-go sampling.

Licensed to Berend Post berend.post@it-university.nl

Question 2129

A disaster recovery plan for an organization should:

- ☐ reduce the length of the recovery time and the cost of recovery.
- ☐ increase the length of the recovery time and the cost of recovery.
- ☐ reduce the duration of the recovery time and increase the cost of recovery.
- ☐ affect neither the recovery time nor the cost of recovery.

Question 2130

Which of the following BEST restricts users to those functions needed to perform their duties?

- ☐ Application level access control
- ☐ Data encryption
- ☐ Disabling floppy disk drives
- ☐ Network monitoring device

Question 2131

Which of the following physical access controls effectively reduces the risk of piggybacking?

- ☐ Biometric door locks
- ☐ Combination door locks
- ☐ Deadman doors
- ☐ Bolting door locks

Question 2132

When developing a business continuity plan (BCP), business unit management's involvement is MOST important during the:

- ☐ performance of a business impact analysis (BIA).
- ☐ development of business recovery procedures.
- ☐ implementation of a document repository.
- ☐ performance of an IT risk assessment.

Question 2133

An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated data. True or false?

- ☐ True
- ☐ False

Licensed to Berend Post berend.post@it-university.nl

Question 2134

Which of the following are valid choices for the Apache/SSL combination (Choose three.):

- ☐ the Apache-SSL project
- ☐ third-party SSL patches
- ☐ the mod_ssl module
- ☐ the mod_css module
- ☐ None of the choices.

Question 2135

An organization's IT security policy requires annual security awareness training for all employees. Which of the following would provide the BEST evidence of the training's effectiveness?

- ☐ Results of a social engineering test
- ☐ Interviews with employees
- ☐ Decreased calls to the incident response team
- ☐ Surveys completed by randomly selected employees

Question 2136

An IS auditor recommends that an initial validation control be programmed into a credit card transaction capture application. The initial validation process would MOST likely:

- ☐ check to ensure that the type of transaction is valid for the card type.
- ☐ verify the format of the number entered then locate it on the database.
- ☐ ensure that the transaction entered is within the cardholder's credit limit.
- ☐ confirm that the card is not shown as lost or stolen on the master file.

Question 2137

Following an unauthorized disclosure of data, an organization needs to implement data loss prevention (DLP) measures. The IS auditor's BEST recommendation should be to:

- ☐ install DLP software on corporate servers to prevent recurrence.
- ☐ monitor and block outgoing emails based on common DLP criteria.
- ☐ restrict removable media access on all computer systems.
- ☐ establish a risk and control framework.

Licensed to Berend Post berend.post@it-university.nl

Question 2138

Responsibility for the governance of IT should rest with the:

- ☐ IT strategy committee.
- ☐ chief information officer (CIO).
- ☐ audit committee.
- ☐ board of directors.

Question 2139

While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's next step?

- ☐ Observe the response mechanism.
- ☐ Clear the virus from the network.
- ☐ Inform appropriate personnel immediately.
- ☐ Ensure deletion of the virus.

Question 2140

The PRIMARY purpose of a precedence diagramming method in managing IT projects is to:

- ☐ monitor project scope creep.
- ☐ identify the critical path.
- ☐ identify key milestones.
- ☐ minimize delays and overruns.

Question 2141

Which audit technique provides the GREATEST assurance that incident management procedures are effective?

- ☐ Determining whether incidents are categorized and addressed
- ☐ Performing comprehensive vulnerability scanning and penetration testing
- ☐ Comparing incident management procedures to best practices
- ☐ Evaluating end-user satisfaction survey results

Question 2142

A firewall has been installed on the company's web server. Which concern does the firewall address?

- ☐ Availability of the information
- ☐ Unauthorized modification of information by internal users
- ☐ Accessing information by the outside world
- ☐ Connectivity to the Internet

Licensed to Berend Post berend.post@it-university.nl

Question 2143

Which of the following devices extends the network and has the capacity to store frames and act as a storage and forward device?

- ☐ Router
- ☐ Bridge
- ☐ Repeater
- ☐ Gateway

Question 2144

An IS auditor notes that IDS log entries related to port scanning are not being analyzed. This lack of analysis will MOST likely increase the risk of success of which of the following attacks?

- ☐ Denial-of-service
- ☐ Replay
- ☐ Social engineering
- ☐ Buffer overflow

Question 2145

An IS auditor finds that conference rooms have active network ports. Which of the following is MOST important to ensure?

- ☐ The corporate network is using an intrusion prevention system (IPS)
- ☐ This part of the network is isolated from the corporate network
- ☐ A single sign-on has been implemented in the corporate network
- ☐ Antivirus software is in place to protect the corporate network

Question 2146

IS management has decided to rewrite a legacy customer relations system using fourth generation languages (4GLs). Which of the following risks is MOST often associated with system development using 4GLs?

- ☐ Inadequate screen/report design facilities
- ☐ Complex programming language subsets
- ☐ Lack of portability across operating systems
- ☐ Inability to perform data intensive operations

Licensed to Berend Post berend.post@it-university.nl

Question 2147

An IS auditor discovers instances where software with the same license key is deployed to multiple workstations, in breach of the licensing agreement. Which of the following is the auditor's BEST recommendation?

- ☐ Evaluate the business case for funding of additional licenses.
- ☐ Require business owner approval before granting software access.
- ☐ Remove embedded keys from offending packages.
- ☐ Implement software licensing monitoring to manage duplications.

Question 2148

Which of the following property of the core date warehouse layer of an enterprise data flow architecture uses common attributes to access a cross section of an information in the warehouse?

- ☐ Drill up
- ☐ Drill down
- ☐ Drill across
- ☐ Historical Analysis

Question 2149

After implementing an information security governance framework, which of the following would provide the BEST information to develop an information security project plan?

- ☐ Balanced scorecard
- ☐ Recent audit results
- ☐ Risk heat map
- ☐ Gap analysis

Question 2150

Which of the following is a substantive test procedure?

- ☐ Using audit software to verify the total of an accounts receivable file
- ☐ Observing that user IDs and passwords are required to sign on to the online system
- ☐ Test of invoice calculation process
- ☐ Verifying that appropriate approvals are documented in a sample of program changes

Licensed to Berend Post berend.post@it-university.nl

Question 2151

An IS auditor performing detailed network assessments and access control reviews should FIRST:

- ☐ determine the points of entry.
- ☐ evaluate users' access authorization.
- ☐ assess users' identification and authorization.
- ☐ evaluate the domain-controlling server configuration.

Question 2152

When performing a data classification project, an information security manager should:

- ☐ assign information critically and sensitivity
- ☐ identify information owners
- ☐ identify information custodians
- ☐ assign information access privileges

Question 2153

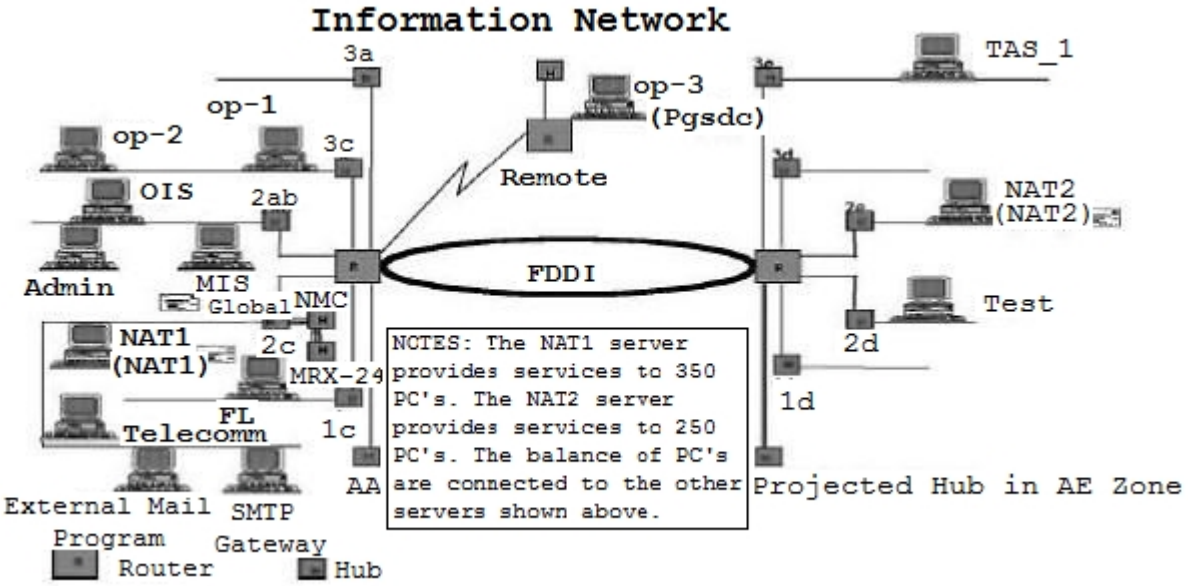
Which of the following will enable a customer to authenticate an online Internet vendor?

- ☐ Vendor signs a reply using a hash function and the customer’s public key.
- ☐ Customer encrypts an order using the vendor’s public key.
- ☐ Customer verifies the vendor’s certificate with a certificate authority (CA).
- ☐ Vendor decrypts incoming orders using its own private key.

Licensed to Berend Post berend.post@it-university.nl

Question 2154

Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?



- ☐ No firewalls are needed
- ☐ Op-3 location only
- ☐ MIS (Global) and NAT2
- ☐ SMTP Gateway and op-3

Question 2155

Which of the following transmission media is LEAST vulnerable to cross talk?

- ☐ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Coaxial cable

Question 2156

When using an integrated test facility (ITF), an IS auditor should ensure that:

- ☐ production data are used for testing.
- ☐ test data are isolated from production data.
- ☐ a test data generator is used.
- ☐ master files are updated with the test data.

Licensed to Berend Post berend.post@it-university.nl

Question 2157

During the requirements definition phase for a database application, performance is listed as a top priority. To access the DBMS files, which of the following technologies should be recommended for optimal I/O performance?

- ☐ Storage area network (SAN)
- ☐ Network Attached Storage (NAS)
- ☐ Network file system (NFS v2)
- ☐ Common Internet File System (CIFS)

Question 2158

During the system testing phase of an application development project the IS auditor should review the:

- ☐ conceptual design specifications.
- ☐ vendor contract.
- ☐ error reports.
- ☐ program change requests.

Question 2159

Which of the following BEST helps to identify errors during data transfer?

- ☐ Decrease the size of data transfer packets.
- ☐ Test the integrity of the data transfer.
- ☐ Review and verify the data transfer sequence numbers.
- ☐ Enable a logging process for data transfer.

Question 2160

An organization's IT security policy states that user IDs must uniquely identify individuals and that users should not disclose their passwords. An IS auditor discovers that several generic user IDs are being used. Which of the following is the MOST appropriate course of action for the auditor?

- ☐ Investigate the noncompliance.
- ☐ Include the finding in the final audit report.
- ☐ Recommend disciplinary action.
- ☐ Recommend a change in security policy.

Licensed to Berend Post berend.post@it-university.nl

Question 2161

An organization's business continuity plan should be:

- ☐ updated based on changes to personnel and environments.
- ☐ updated only after independent audit review by a third party.
- ☐ tested whenever new applications are implemented.
- ☐ tested after successful intrusions into the organization's hot site.

Question 2162

While reviewing the business continuity plan of an organization, an IS auditor observed that the organization's data and software files are backed up on a periodic basis. Which characteristic of an effective plan does this demonstrate?

- ☐ Deterrence
- ☐ Mitigation
- ☐ Recovery
- ☐ Response

Question 2163

Which of the following is NOT an example of preventive control?

- ☐ Physical access control like locks and door
- ☐ User login screen which allows only authorize user to access website
- ☐ Encrypt the data so that only authorize user can view the same
- ☐ Duplicate checking of a calculations

Question 2164

_____ (fill in the blank) is/are ultimately accountable for the functionality, reliability, and security within IT governance.

- ☐ Data custodians
- ☐ The board of directors and executive officers
- ☐ IT security administration
- ☐ Business unit managers

Licensed to Berend Post berend.post@it-university.nl

Question 2165

Which of the following would BEST help ensure information security is effective following the outsourcing of network operations?

- ☐ Test security controls periodically.
- ☐ Review security key performance indicators (KPIs).
- ☐ Establish security service level agreements (SLAs).
- ☐ Appoint a security service delivery monitoring manager.

Question 2166

Reconciliations have identified data discrepancies between an enterprise data warehouse and a revenue system for key financial reports. What is the GREATEST risk to the organization in this situation?

- ☐ The key financial reports may no longer be produced
- ☐ Financial reports may be delayed
- ☐ Undetected fraud may occur
- ☐ Decisions may be made based on incorrect information

Question 2167

Which of the following should be of PRIMARY concern to an IS auditor reviewing the management of external IT service providers?

- ☐ Minimizing costs for the services provided
- ☐ Prohibiting the provider from subcontracting services
- ☐ Evaluating the process for transferring knowledge to the IT department
- ☐ Determining if the services were provided as contracted

Question 2168

A cloud service provider is unable to provide an independent assessment of controls. Which of the following is the BEST way to obtain assurance that the provider can adequately protect the organization's information?

- ☐ Check references supplied by the provider's other customers.
- ☐ Invoke the right to audit per the contract.
- ☐ Review the provider's information security policy.
- ☐ Review the provider's self-assessment.

Licensed to Berend Post berend.post@it-university.nl

Question 2169

Which of the following type of a computer network covers a limited area such as a home, office or campus?

- ☐ LAN
- ☐ WAN
- ☐ SAN
- ☐ PAN

Question 2170

A web organization is developed in-house by an organization. Which of the following would provide the BEST evidence to an IS auditor that the application is secure from external attack?

- ☐ Code review by a third party
- ☐ Web application firewall implementation
- ☐ Penetration test results
- ☐ Database application monitoring logs

Question 2171

Which of the following would be the PRIMARY benefit of replacing physical keys with an electronic badge system for access to a data center?

- ☐ Increasing accountability
- ☐ Maintaining compliance
- ☐ Tracking employee work hours
- ☐ Increasing reliability

Question 2172

A change to the scope of an IT project has been formally submitted to the project manager. What should the project manager do NEXT?

- ☐ Update the project plan to reflect the change in scope
- ☐ Discuss the change with the project team and determine if it should be approved
- ☐ Escalate the change to the change advisory board for approval
- ☐ Determine how the change will affect the schedule and budget

Licensed to Berend Post berend.post@it-university.nl

Question 2173

Which of the following would be best suited to oversee the development of an information security policy?

- ☐ System Administrators
- ☐ End User
- ☐ Security Officers
- ☐ Security administrators

Question 2174

A policy has been established requiring users to install mobile device management (MDM) software on their personal devices. Which of the following would BEST mitigate the risk created by noncompliance with this policy?

- ☐ Issuing warnings and documenting noncompliance
- ☐ Disabling remote access from the mobile device
- ☐ Issuing company-configured mobile devices
- ☐ Requiring users to sign-off on terms and conditions

Question 2175

When removing a financial application system from production, which of the following is MOST important?

- ☐ Media used by the retired system has been sanitized.
- ☐ Data retained for regulatory purposes can be retrieved.
- ☐ End-user requests for changes are recorded and tracked.
- ☐ Software license agreements are retained.

Question 2176

A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

- ☐ what amount of progress against schedule has been achieved.
- ☐ if the project budget can be reduced.
- ☐ if the project could be brought in ahead of schedule.
- ☐ if the budget savings can be applied to increase the project scope.

Licensed to Berend Post berend.post@it-university.nl

Question 2177

Which of the following would an IS auditor consider to be the MOST significant risk associated with a project to reengineer a business process?

- ☐ The negative impact of change may not be documented.
- ☐ The project manager is inexperienced in information systems.
- ☐ Existing controls may be weakened or removed.
- ☐ Existing baseline processes may not be reported to management.

Question 2178

Which of the following is BEST enabled by following a configuration management process for new applications?

- ☐ Deploying approved emergency changes to production
- ☐ Ensuring proper testing of code before deployment
- ☐ Managing successful implementation of acquired software
- ☐ Maintaining adequate control over changes to production

Question 2179

An external security audit risk has reported multiple instances of control noncompliance. Which of the following would be MOSTimportant for the information security manager to communicate to senior management?

- ☐ The impact of noncompliance on the organization's risk profile
- ☐ An accountability report to initiate remediation activities
- ☐ A plan for mitigating the risk due to noncompliance
- ☐ Control owner responses based on a root cause analysis

Question 2180

Which of the following is MOST important for an IS auditor to verify when reviewing an organization's information security practices following the adoption of a bring your own device (BYOD) program?

- ☐ Only applications approved by information security may be installed on devices.
- ☐ The expected benefits of adopting the BYOD program have been realized.
- ☐ Security policies have been updated to include BYOD.
- ☐ Remote wipe is enabled for devices allowed by BYOD.

Licensed to Berend Post berend.post@it-university.nl

Question 2181

Which of the following would create the GREATEST risk when migrating a critical legacy system to a new system?

- ☐ Using agile development methodology
- ☐ Following a phased approach
- ☐ Following a direct cut-over approach
- ☐ Maintaining parallel systems

Question 2182

Which of the following findings should be of MOST concern to an IS auditor when evaluating information security governance within an organization?

- ☐ The data center manager has final sign-off on security projects.
- ☐ The information security oversight committee meets quarterly.
- ☐ The information security department has difficulty filling vacancies.
- ☐ Information security policies were last updated two years ago.

Question 2183

What is the PRIMARY purpose of audit trails?

- ☐ To document auditing efforts
- ☐ To correct data integrity errors
- ☐ To establish accountability and responsibility for processed transactions
- ☐ To prevent unauthorized access to data

Question 2184

Which of the following would be the GREATEST concern to an IS auditor reviewing a critical spreadsheet during a financial audit?

- ☐ Periodic access reviews are manually performed.
- ☐ Changes to the file are not always documented.
- ☐ Access requests are manually processed.
- ☐ A copy current validated file is not available.

Licensed to Berend Post berend.post@it-university.nl

Question 2185

Which of the following actions should an organization's security policy require an employee to take upon finding a security breach?

- ☐ Report the incident to the manager immediately.
- ☐ Inform IS audit management immediately.
- ☐ Confirm the breach can be exploited.
- ☐ Devise appropriate countermeasures.

Question 2186

What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

- ☐ Document existing internal controls
- ☐ Perform compliance testing on internal controls
- ☐ Establish a controls-monitoring steering committee
- ☐ Identify high-risk areas within the organization

Question 2187

Upon receipt of the initial signed digital certificate the user will decrypt the certificate with the public key of the:

- ☐ registration authority (RA).
- ☐ certificate authority (CA).
- ☐ certificate repository.
- ☐ receiver.

Question 2188

Which of the following refers to the proving of mathematical theorems by a computer program?

- ☐ Analytical theorem proving
- ☐ Automated technology proving
- ☐ Automated theorem processing
- ☐ Automated theorem proving
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 2189

What would an IS auditor expect to find in the console log?

- ☐ Evidence of password spoofing
- ☐ System errors
- ☐ Evidence of data copy activities
- ☐ Evidence of password sharing

Question 2190

The most common reason for the failure of information systems to meet the needs of users is that:

- ☐ user needs are constantly changing.
- ☐ the growth of user requirements was forecast inaccurately.
- ☐ the hardware system limits the number of concurrent users.
- ☐ user participation in defining the system's requirements was inadequate.

Question 2191

What is a primary high-level goal for an auditor who is reviewing a system development project?

- ☐ To ensure that programming and processing environments are segregated
- ☐ To ensure that proper approval for the project has been obtained
- ☐ To ensure that business objectives are achieved
- ☐ To ensure that projects are monitored and administrated effectively

Question 2192

An organization plans to deploy Wi-Fi location analytics to count the number of shoppers per day across its various retail outlets. What should the IS auditor recommend as the FIRST course of action by IT management?

- ☐ Conduct a privacy impact assessment
- ☐ Mask media access control (MAC) addresses
- ☐ Survey shoppers for feedback
- ☐ Develop a privacy notice to be displayed to shoppers

Question 2193

Which of the following should be of GREATEST concern to an IS auditor reviewing the controls for a continuous software release process?

- ☐ Release documentation is not updated to reflect successful deployment.
- ☐ Test libraries have not been reviewed in over six months.
- ☐ Developers are able to approve their own releases.
- ☐ Testing documentation is not attached to production releases.

Licensed to Berend Post berend.post@it-university.nl

Question 2194

Senior management has allocated funding to each of the organization's divisions to address information security vulnerabilities. The funding is based on each division's technology budget from the previous fiscal year. Which of the following should be of GREATEST concern to the information security manager?

- ☐ Redundant controls may be implemented across divisions
- ☐ Information security governance could be decentralized by divisions
- ☐ Areas of highest risk may not be adequately prioritized for treatment
- ☐ Return on investment may be inconsistently reported to senior management

Question 2195

The GREATEST benefit in implementing an expert system is the:

- ☐ capturing of the knowledge and experience of individuals in an organization.
- ☐ sharing of knowledge in a central repository.
- ☐ enhancement of personnel productivity and performance.
- ☐ reduction of employee turnover in key departments.

Question 2196

During an audit of an enterprise that is dedicated to e-commerce, the IS manager states that digital signatures are used when receiving communications from customers. To substantiate this, an IS auditor must prove that which of the following is used?

- ☐ A biometric, digitalized and encrypted parameter with the customer's public key
- ☐ A hash of the data that is transmitted and encrypted with the customer's private key
- ☐ A hash of the data that is transmitted and encrypted with the customer's public key
- ☐ The customer's scanned signature encrypted with the customer's public key

Question 2197

If the inherent risk of a business activity is higher than the acceptable risk level, the information security manager should FIRST:

- ☐ transfer risk to a third party to avoid cost of impact
- ☐ implement controls to mitigate the risk to an acceptable level
- ☐ recommend that management avoids the business activity
- ☐ assess the gap between current and acceptable level of risk

Licensed to Berend Post berend.post@it-university.nl

Question 2198

Which of the following is the FIRST step when conducting a business impact analysis?

- ☐ Identifying critical information resources
- ☐ Identifying events impacting continuity of operations
- ☐ Analyzing past transaction volumes
- ☐ Creating a data classification scheme

Question 2199

Which of the following is protocol data unit (PDU) of data at LAN or WAN interface layer in TCP/IP model?

- ☐ Data
- ☐ Segment
- ☐ Packet
- ☐ Frame and bits

Question 2200

Which of the following activities is MOST important to consider when conducting IS audit planning?

- ☐ Results from previous audits are reviewed.
- ☐ Audit scheduling is based on skill set of audit team.
- ☐ Resources are allocated to areas of high risk.
- ☐ The audit committee agrees on risk rankings.

Question 2201

An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

- ☐ this lack of knowledge may lead to unintentional disclosure of sensitive information.
- ☐ information security is not critical to all functions.
- ☐ IS audit should provide security training to the employees.
- ☐ the audit finding will cause management to provide continuous training to staff.

Question 2202

When auditing the IT governance of an organization planning to outsource a critical financial application to a cloud vendor, the MOST important consideration for the auditor should be:

- ☐ the cost of the outsourced system.
- ☐ the inclusion of a service termination clause.
- ☐ alignment with industry standards.
- ☐ alignment with business requirements.

Licensed to Berend Post berend.post@it-university.nl

Question 2203

Which of the following device in Frame Relay WAN technique is generally customer owned device that provides a connectivity between company's own network and the frame relays network?

- ☐ DTE
- ☐ DCE
- ☐ DME
- ☐ DLE

Question 2204

Which of the following is the BEST way to determine the effectiveness of a recently installed intrusion detection system (IDS)?

- ☐ Implement access control.
- ☐ Conduct attack simulation.
- ☐ Review audit logs.
- ☐ Inspect IDS configuration.

Question 2205

Which of the following line media would provide the BEST security for a telecommunication network?

- ☐ broadband network digital transmission
- ☐ Baseband network
- ☐ Dial-up
- ☐ Dedicated lines

Question 2206

Which of the following is the MOST beneficial outcome of testing an incident response plan?

- ☐ The plan is enhanced to reflect the findings of the test.
- ☐ Test plan results are documented.
- ☐ Incident response time is improved.
- ☐ The response includes escalation to senior management.

Licensed to Berend Post berend.post@it-university.nl

Question 2207

Which of the following methods would BEST help detect unauthorized disclosure of confidential documents sent over corporate email?

- ☐ Installing firewalls on the corporate network
- ☐ Requiring all users to encrypt documents before sending
- ☐ Monitoring all emails based on pre-defined criteria
- ☐ Reporting all outgoing emails that are marked as confidential

Question 2208

An IS auditor has observed gaps in the data available to the organization for detecting incidents. Which of the following would be the BEST recommendation to improve the organization's security incident response capability?

- ☐ Document procedures for incident escalation.
- ☐ Document procedures for incident classification.
- ☐ Correlate security logs collected from multiple sources.
- ☐ Centralize alerts and security log information.

Question 2209

What is the most effective means of determining that controls are functioning properly within an operating system?

- ☐ Interview with computer operator
- ☐ Review of software control features and/or parameters
- ☐ Review of operating system manual
- ☐ Interview with product vendor

Question 2210

Which of the following IS audit recommendations would BEST help to ensure appropriate mitigation will occur on control weaknesses identified during an audit?

- ☐ Assign actions to responsible personnel and follow up.
- ☐ Report on progress to the audit committee.
- ☐ Perform a cost-benefit analysis on remediation strategy.
- ☐ Implement software to input the action points from the IS audit.

Licensed to Berend Post berend.post@it-university.nl

Question 2211

Which of the following should be of GREATEST concern to an IS auditor when auditing an organization's information security awareness program?

- ☐ Security awareness training is not included as part of the onboarding process for new hires.
- ☐ The number of security incidents logged by employees to the help desk has increased in the past year.
- ☐ Training quizzes are designed and run by a third-party company under a contract with the organization.
- ☐ Security awareness training is run via the organization's enterprise-wide e-learning portal.

Question 2212

Which of the following refers to any authentication protocol that requires two independent ways to establish identity and privileges?

- ☐ Strong-factor authentication
- ☐ Two-factor authentication
- ☐ Dual-password authentication
- ☐ Two-passphrases authentication
- ☐ Dual-keys authentication
- ☐ Rich-factor authentication

Question 2213

For an organization which uses a VoIP telephony system exclusively, the GREATEST concern associated with leaving a connected telephone in an unmonitored public area is the possibility of:

- ☐ connectivity issues when used with an analog local exchange carrier
- ☐ unauthorized use leading to theft of services and financial loss
- ☐ network compromise due to the introduction of malware
- ☐ theft or destruction of an expensive piece of electronic equipment

Licensed to Berend Post berend.post@it-university.nl

Question 2214

An IS auditor reviewing database controls discovered that changes to the database during normal working hours were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation, which of the following would be considered an adequate set of compensating controls?

- ☐ Allow changes to be made only with the DBA user account.
- ☐ Make changes to the database after granting access to a normal user account.
- ☐ Use the DBA user account to make changes, log the changes and review the change log the following day.
- ☐ Use the normal user account to make changes, log the changes and review the change log the following day.

Question 2215

Capacity management enables organizations to:

- ☐ establish the capacity of network communication links.
- ☐ determine business transaction volumes.
- ☐ forecast technology trends.
- ☐ identify the extent to which components need to be upgraded.

Question 2216

Facilitating telecommunications continuity by providing redundant combinations of local carrier T- 1 lines, microwaves and/or coaxial cables to access the local communication loop:

- ☐ last-mile circuit protection.
- ☐ long-haul network diversity.
- ☐ diverse routing.
- ☐ alternative routing.

Question 2217

Which of the following is the key benefit of control self-assessment (CSA)?

- ☐ Management ownership of the internal controls supporting business objectives is reinforced.
- ☐ Audit expenses are reduced when the assessment results are an input to external audit work.
- ☐ Improved fraud detection since internal business staff are engaged in testing controls
- ☐ Internal auditors can shift to a consultative approach by using the results of the assessment.

Licensed to Berend Post berend.post@it-university.nl

Question 2218

Which of the following is a telecommunication device that translates data from digital to analog form and back to digital?

- ☐ Multiplexer
- ☐ Modem
- ☐ Protocol converter
- ☐ Concentrator

Question 2219

What are often the primary safeguards for systems software and data?

- ☐ Administrative access controls
- ☐ Logical access controls
- ☐ Physical access controls
- ☐ Detective access controls

Question 2220

Of the following alternatives, the FIRST approach to developing a disaster recovery strategy would be to assess whether:

- ☐ all threats can be completely removed.
- ☐ a cost-effective, built-in resilience can be implemented.
- ☐ the recovery time objective can be optimized.
- ☐ the cost of recovery can be minimized.

Question 2221

IS management is considering a Voice-over Internet Protocol (VoIP) network to reduce telecommunication costs and management asked the IS auditor to comment on appropriate security controls. Which of the following security measures is MOST appropriate?

- ☐ Review and, where necessary, upgrade firewall capabilities
- ☐ Install modems to allow remote maintenance support access
- ☐ Create a physically distinct network to handle VoIP traffic
- ☐ Redirect all VoIP traffic to allow clear text logging of authentication credentials

Licensed to Berend Post berend.post@it-university.nl

Question 2222

The GREATEST risk posed by an improperly implemented intrusion prevention system (IPS) is:

- ☐ that there will be too many alerts for system administrators to verify.
- ☐ decreased network performance due to IPS traffic.
- ☐ the blocking of critical systems or services due to false triggers.
- ☐ reliance on specialized expertise within the IT organization.

Question 2223

In an IS audit of several critical servers, the IS auditor wants to analyze audit trails to discover potential anomalies in user or system behavior. Which of the following tools are MOST suitable for performing that task?

- ☐ CASE tools
- ☐ Embedded data collection tools
- ☐ Heuristic scanning tools
- ☐ Trend/variance detection tools

Question 2224

Vendors have released patches fixing security flaws in their software. Which of the following should an IS auditor recommend in this situation?

- ☐ Assess the impact of patches prior to installation.
- ☐ Ask the vendors for a new software version with all fixes included.
- ☐ install the security patch immediately.
- ☐ Decline to deal with these vendors in the future.

Question 2225

Following request for proposal (RFP) responses, a project seeking to acquire a new application system has identified a short list of vendors. At this point, the IS auditor should:

- ☐ encourage contact with current users of the vendor's products
- ☐ perform a detailed cost-benefit exercise on the proposed application
- ☐ require that contract terms include a right-to-audit clause
- ☐ recommend performing system integration tests

Licensed to Berend Post berend.post@it-university.nl

Question 2226

Which of the following is NOT a disadvantage of Single Sign On (SSO)?

- ☐ Support for all major operating system environment is difficult
- ☐ The cost associated with SSO development can be significant
- ☐ SSO could be single point of failure and total compromise of an organization asset
- ☐ SSO improves an administrator's ability to manage user's account and authorization to all associated system

Question 2227

Which of the following is a guiding best practice for implementing logical access controls?

- ☐ Implementing the Biba Integrity Model
- ☐ Access is granted on a least-privilege basis, per the organization's data owners
- ☐ Implementing the Take-Grant access control model
- ☐ Classifying data according to the subject's requirements

Question 2228

The BEST method of proving the accuracy of a system tax calculation is by:

- ☐ detailed visual review and analysis of the source code of the calculation programs
- ☐ recreating program logic using generalized audit software to calculate monthly totals.
- ☐ preparing simulated transactions for processing and comparing the results to predetermined results.
- ☐ automatic flowcharting and analysis of the source code of the calculation programs.

Question 2229

When reviewing an organization's approved software product list, which of the following is the MOST important thing to verify?

- ☐ The risks associated with the use of the products are periodically assessed
- ☐ The latest version of software is listed for each product
- ☐ Due to licensing issues the list does not contain open source software
- ☐ After hours' support is offered

Licensed to Berend Post berend.post@it-university.nl

Question 2230

During a security audit, which of the following is MOST important to review to ensure data confidentiality is managed?

- ☐ Access controls
- ☐ Data flows
- ☐ Access log monitoring
- ☐ Network configuration

Question 2231

Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

- ☐ Test data run
- ☐ Code review
- ☐ Automated code comparison
- ☐ Review of code migration procedures

Question 2232

A top-down approach to the development of operational policies will help ensure:

- ☐ that they are consistent across the organization.
- ☐ that they are implemented as a part of risk assessment.
- ☐ compliance with all policies.
- ☐ that they are reviewed periodically.

Question 2233

The cost of ongoing operations when a disaster recovery plan is in place, compared to not having a disaster recovery plan, will MOST likely:

- ☐ increase.
- ☐ decrease.
- ☐ remain the same.
- ☐ be unpredictable.

Licensed to Berend Post berend.post@it-university.nl

Question 2234

Which of the following is an object-oriented technology characteristic that permits an enhanced degree of security over data?

- ☐ inheritance
- ☐ Dynamic warehousing
- ☐ Encapsulation
- ☐ Polymorphism

Question 2235

Reports to the executive level concerning IT performance should focus on:

- ☐ third-party compliance with organizational practices.
- ☐ IT performance in relation to operational improvements.
- ☐ IT deliverables against organizational strategies.
- ☐ capacity planning effectiveness within the organization.

Question 2236

Which of the following is the MOST important consideration when defining recovery point objectives (RPOs)?

- ☐ Minimum operating requirements
- ☐ Acceptable data loss
- ☐ Mean time between failures
- ☐ Acceptable time for recovery

Question 2237

You are part of a security staff at a highly profitable bank and each day, all traffic on the network is logged for later review. Every Friday when major deposits are made you're seeing a series of bits placed in the "Urgent Pointer" field of a TCP packet. This is only 16 bits which isn't much but it concerns you because:

- ☐ This could be a sign of covert channeling in bank network communications and should be investigated.
- ☐ It could be a sign of a damaged network cable causing the issue.
- ☐ It could be a symptom of malfunctioning network card or drivers and the source system should be checked for the problem.
- ☐ It is normal traffic because sometimes the previous fields 16-bit checksum value can over run into the urgent pointer's 16-bit field causing the condition.

Licensed to Berend Post berend.post@it-university.nl

Question 2238

What is the PRIMARY benefit to executive management when audit, risk, and security functions are aligned?

- ☐ More efficient incident handling
- ☐ Reduced number of assurance reports
- ☐ More effective decision making
- ☐ More timely risk reporting

Question 2239

To prevent unauthorized entry to the data maintained in a dial-up, fast response system, an IS auditor should recommend:

- ☐ online terminals are placed in restricted areas.
- ☐ online terminals are equipped with key locks.
- ☐ ID cards are required to gain access to online terminals.
- ☐ online access is terminated after a specified number of unsuccessful attempts.

Question 2240

Which of the following security control is intended to avoid an incident from occurring?

- ☐ Deterrent
- ☐ Preventive
- ☐ Corrective
- ☐ Recovery

Question 2241

Within a security governance framework, which of the following is the MOST important characteristic of the information security committee? The committee:

- ☐ conducts frequent reviews of the security policy.
- ☐ includes a mix of members from all levels of management.
- ☐ has a clearly defined charter and meeting protocols.
- ☐ has established relationships with external professionals.

Question 2242

Which of the following would normally be the MOST reliable evidence for an auditor?

- ☐ A confirmation letter received from a third party verifying an account balance
- ☐ Assurance from line management that an application is working as designed
- ☐ Trend data obtained from World Wide Web (Internet) sources
- ☐ Ratio analysts developed by the IS auditor from reports supplied by line management

Licensed to Berend Post berend.post@it-university.nl

Question 2243

Which of the following is a directive control?

- ☐ Establishing an information security operations team
- ☐ Updating data loss prevention software
- ☐ Implementing an information security policy
- ☐ Configuring data encryption software

Question 2244

There are many known weaknesses within an Intrusion Detection System (IDS). Which of the following is NOT a limitation of an IDS?

- ☐ Weakness in the identification and authentication scheme.
- ☐ Application level vulnerability.
- ☐ Backdoor into application
- ☐ Detect zero day attack.

Question 2245

Which of the following will MOST effectively help to manage the challenges associated with end user-developed application systems?

- ☐ Developing classifications based on risk
- ☐ Introducing redundant support capacity
- ☐ Prohibiting creation of executable files
- ☐ Applying control practices used by IT

Question 2246

Which of the following can degrade network performance?

- ☐ Superfluous use of redundant load-sharing gateways
- ☐ Increasing traffic collisions due to host congestion by creating new collision domains
- ☐ Inefficient and superfluous use of network devices such as switches
- ☐ Inefficient and superfluous use of network devices such as hubs

Question 2247

An organization has recently incorporated robotic process automation. Which of the following would be of GREATEST concern to an IS auditor?

- ☐ Controls have not been tested
- ☐ A governance structure has not been implemented
- ☐ A risk assessment has not been conducted
- ☐ The adoption rate for the new technology has been low

Licensed to Berend Post berend.post@it-university.nl

Question 2248

Which of the following is the MOST effective control for emergency changes to application programs?

- ☐ Processing the change through change control with review of the change the following day
- ☐ Keeping a sealed envelope containing a password that operators can use to make emergency changes
- ☐ Periodically checking the application program libraries to detect whether unauthorized changes have been made
- ☐ Preparing and approving program change forms before the changes are made

Question 2249

During a review of system access, an IS auditor notes that an employee who has recently changed roles within the organization still has previous access rights. The auditor's NEXT step should be to:

- ☐ determine the reason why access rights have not been revoked.
- ☐ recommend a control to automatically update access rights.
- ☐ direct management to revoke current access rights.
- ☐ determine if access rights are in violation of software licenses.

Question 2250

Which of the following would BEST support a business case to implement a data leakage prevention (DLP) solution?

- ☐ An unusual upward trend in outbound email volume
- ☐ Lack of visibility into previous data leakage incidents
- ☐ Industry benchmark of DLP investments
- ☐ A risk assessment on the threat of data leakage

Question 2251

Which of the following practices associated with capacity planning provides the GREATEST assurance that future incidents related to server performance will be prevented?

- ☐ Anticipating current service level agreements (SLAs) will remain unchanged
- ☐ Prorating the current processing workloads
- ☐ Negotiating agreements to acquire required cloud services
- ☐ Duplicating existing disk drive systems to improve redundancy and data storage

Licensed to Berend Post berend.post@it-university.nl

Question 2252

Screening router inspects traffic through examining:

- ☐ message header.
- ☐ virus payload
- ☐ message content
- ☐ attachment type
- ☐ None of the choices.

Question 2253

The extent to which data will be collected during an IS audit should be determined based on the:

- ☐ availability of critical and required information.
- ☐ auditor's familiarity with the circumstances.
- ☐ auditee's ability to find relevant evidence.
- ☐ purpose and scope of the audit being done.

Question 2254

Over the long term, which of the following has the greatest potential to improve the security incident response process?

- ☐ A walkthrough review of incident response procedures
- ☐ Postevent reviews by the incident response team
- ☐ Ongoing security training for users
- ☐ Documenting responses to an incident

Question 2255

An organization has shifted from a bottom-up approach to a top-down approach in the development of IT policies. This should result in:

- ☐ a synthesis of existing operational policies
- ☐ greater consistency across the organization
- ☐ greater adherence to best practices
- ☐ a more comprehensive risk assessment plan

Licensed to Berend Post berend.post@it-university.nl

Question 2256

Buffer overflow aims primarily at corrupting:

- ☐ system processor
- ☐ network firewall
- ☐ system memory
- ☐ disk storage
- ☐ None of the choices.

Question 2257

Which of the following is the BEST indication that an information security program is effective?

- ☐ The number of reported and confirmed security incidents has increased after awareness training.
- ☐ The security awareness program was developed following industry best practices.
- ☐ The security team has performed a risk assessment to understand the organization's risk appetite.
- ☐ The security team is knowledgeable and uses the best available tools.

Question 2258

Which of the following factor is LEAST important in the measurement of critical success factors of productivity in the SDLC phases?

- ☐ Dollar Spent per use
- ☐ Number of transactions per month
- ☐ Number of transactions per user
- ☐ Number of occurrences of fraud/misuse detection

Question 2259

Which of the following would BEST ensure continuity of a wide area network (WAN) across the organization?

- ☐ Built-in alternative routing
- ☐ Completing full system backup daily
- ☐ A repair contract with a service provider
- ☐ A duplicate machine alongside each server

Licensed to Berend Post berend.post@it-university.nl

Question 2260

Which of the following management decisions presents the GREATEST risk associated with data leakage?

- ☐ Security awareness training is not provided to staff.
- ☐ There is no requirement for desktops to be encrypted.
- ☐ Security policies have not been updated in the past year.
- ☐ Staff are allowed to work remotely.

Question 2261

Which of the following protocol does NOT work at Network interface layer in TCP/IP model?

- ☐ ICMP
- ☐ DNS
- ☐ ARP
- ☐ Internet protocol

Question 2262

What are the different types of Audits?

- ☐ Compliance, financial, operational, forensic and integrated
- ☐ Compliance, financial, operational, G9 and integrated
- ☐ Compliance, financial, SA1, forensic and integrated
- ☐ Compliance, financial, operational, forensic and capability

Question 2263

An IS auditor noted that an organization had adequate business continuity plans (BCPs) for each individual process, but no comprehensive BCP. Which would be the BEST course of action for the IS auditor?

- ☐ Recommend that an additional comprehensive BCP be developed.
- ☐ Determine whether the BCPs are consistent.
- ☐ Accept the BCPs as written.
- ☐ Recommend the creation of a single BCP.

Question 2264

During a business process re-engineering (BPR) program, IT can assist with:

- ☐ total cost of ownership.
- ☐ focusing on value-added tasks.
- ☐ segregation of duties.
- ☐ streamlining of tasks.

Licensed to Berend Post berend.post@it-university.nl

Question 2265

When storing data archives off-site, what must be done with the data to ensure data completeness?

- ☐ The data must be normalized.
- ☐ The data must be validated.
- ☐ The data must be parallel-tested.
- ☐ The data must be synchronized.

Question 2266

Which of the following is MOST important to consider when assessing the scope of privacy concerns for an IT project?

- ☐ Applicable laws and regulations
- ☐ End user access rights
- ☐ Business requirements
- ☐ Classification of data

Question 2267

Which of the following is the BEST method for preventing the leakage of confidential information in a laptop computer?

- ☐ Encrypt the hard disk with the owner's public key.
- ☐ Enable the boot password (hardware-based password).
- ☐ Use a biometric authentication device.
- ☐ Use two-factor authentication to logon to the notebook.

Question 2268

An organization’s current end-user computing practices include the use of a spreadsheet for financial statements. Which of the following is the GREATEST concern?

- ☐ Formulas are not protected against unintended changes.
- ☐ The spreadsheet contains numerous macros.
- ☐ Operational procedures have not been reviewed in the current fiscal year.
- ☐ The spreadsheet is not maintained by IT.

Licensed to Berend Post berend.post@it-university.nl

Question 2269

An IS auditor observes that the CEO has full access to the enterprise resource planning (ERP) system. The IS auditor should FIRST:

- ☐ accept the level of access provided as appropriate
- ☐ recommend that the privilege be removed
- ☐ ignore the observation as not being material to the review
- ☐ document the finding as a potential risk

Question 2270

Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

- ☐ Integrating of assurance efforts
- ☐ Automation of controls
- ☐ Standardization of compliance requirements
- ☐ Documentation of control procedures

Question 2271

Which of the following is the MOST effective mechanism for ensuring that critical IT operational problems are reported to executive management in a timely manner?

- ☐ Regular meetings
- ☐ Escalation procedures
- ☐ Service level monitoring
- ☐ Periodic status reports

Question 2272

Which of the following observations would an IS auditor consider the GREATEST risk when conducting an audit of a virtual server farm for potential software vulnerabilities?

- ☐ The hypervisor is updated quarterly.
- ☐ Guest operating systems are updated monthly.
- ☐ Antivirus software has been implemented on the guest operating system only.
- ☐ A variety of guest operating systems operate on one virtual server.

Licensed to Berend Post berend.post@it-university.nl

Question 2273

For a company that outsources payroll processing, which of the following is the BEST way to ensure that only authorized employees are paid?

- ☐ The company's bank reconciliations should be independently prepared and checked.
- ☐ Employees should receive pay statements showing gross pay, net pay, and deductions.
- ☐ Only payroll employees should be given the password for data entry and report retrieval.
- ☐ Electronic payroll reports should be independently reviewed.

Question 2274

In a complex IS environment, which of the following tasks should be performed by the data owner?

- ☐ Perform technical database maintenance.
- ☐ Perform data restoration when necessary.
- ☐ Review data classifications periodically.
- ☐ Test the validity of backup data.

Question 2275

A database audit reveals an issue with the way data ownership for client data is defined. Which of the following roles should be accountable for this finding?

- ☐ Business management
- ☐ Database administrator
- ☐ Information security management
- ☐ Privacy manager

Question 2276

What is a risk associated with attempting to control physical access to sensitive areas such as computer rooms using card keys or locks?

- ☐ Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.
- ☐ The contingency plan for the organization cannot effectively test controlled access practices.
- ☐ Access cards, keys and pads can be easily duplicated allowing easy compromise of the control.
- ☐ Removing access for those who are no longer authorized is complex.

Licensed to Berend Post berend.post@it-university.nl

Question 2277

A Trojan horse's payload would almost always take damaging effect immediately.

- ☐ True
- ☐ False

Question 2278

Which of the following would BEST enable effective IT resource management?

- ☐ Assessing the risk associated with IT resources
- ☐ Outsourcing IT processes and activities
- ☐ Establishing business priorities
- ☐ Automating business processes

Question 2279

Which of the following should an IS auditor recommend for the protection of specific sensitive information stored in the data warehouse?

- ☐ implement column- and row-level permissions
- ☐ Enhance user authentication via strong passwords
- ☐ Organize the data warehouse into subject matter-specific databases
- ☐ Log user access to the data warehouse

Question 2280

Who is ultimately responsible and accountable for reviewing user access to systems?

- ☐ Systems security administrators
- ☐ Data custodians
- ☐ Data owners
- ☐ Information systems auditors

Question 2281

Which of the following is the MOST likely cause of a successful firewall penetration?

- ☐ Use of a Trojan to bypass the firewall
- ☐ Loophole in firewall vendor’s code
- ☐ Virus infection
- ☐ Firewall misconfiguration by the administrator

Licensed to Berend Post berend.post@it-university.nl

Question 2282

Which of the following is the MOST effective control when granting temporary access to vendors?

- ☐ Vendor access corresponds to the service level agreement (SLA).
- ☐ User accounts are created with expiration dates and are based on services provided.
- ☐ Administrator access is provided for a limited period.
- ☐ User IDs are deleted when the work is completed.

Question 2283

As an IS auditor it is very important to understand software release management process. Which of the following software release normally contains a significant change or addition of new functionality?

- ☐ Major software Release
- ☐ Minor software Release
- ☐ Emergency software release
- ☐ General software Release

Question 2284

When developing metrics to measure the contribution of IT to the achievement of business goals, the MOST important consideration is that the metrics:

- ☐ measure the effectiveness of IT controls in the achievement of IT strategy.
- ☐ provide quantitative measurement of IT initiatives in relation with business targets.
- ☐ are expressed in terms of how IT risk impacts the achievement of business goals.
- ☐ are used by similar industries to measure the effect of IT on business strategy.

Question 2285

An information security manager has discovered a potential security breach in a server that supports a critical business process. Which of the following should be the information security manager's FIRST course of action?

- ☐ Validate that there has been an incident
- ☐ Notify the business process owner
- ☐ Shut down the server in an organized manner
- ☐ Inform senior management of the incident

Licensed to Berend Post berend.post@it-university.nl

Question 2286

During maintenance of a relational database, several values of the foreign key in a transaction table of a relational database have been corrupted. The consequence is that:

- ☐ the detail of involved transactions may no longer be associated with master data, causing errors when these transactions are processed.
- ☐ there is no way of reconstructing the lost information, except by deleting the dangling tuples and reentering the transactions.
- ☐ the database will immediately stop execution and lose more information.
- ☐ the database will no longer accept input data.

Question 2287

The role of the certificate authority (CA) as a third party is to:

- ☐ provide secured communication and networking services based on certificates.
- ☐ host a repository of certificates with the corresponding public and secret keys issued by that CA.
- ☐ act as a trusted intermediary between two communication partners.
- ☐ confirm the identity of the entity owning a certificate issued by that CA.

Question 2288

An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

- ☐ References from other customers
- ☐ Service level agreement (SLA) template
- ☐ Maintenance agreement
- ☐ Conversion plan

Question 2289

To test the integrity of the data in the accounts receivable master file, an IS auditor is particularly interested in reviewing customers with balances over $400,000. The selection technique the IS auditor would use to obtain such a sample is called:

- ☐ random selection.
- ☐ systematic selection.
- ☐ discovery selection.
- ☐ stratification.

Licensed to Berend Post berend.post@it-university.nl

Question 2290

An IS auditor has been asked to audit a complex system with computerized and manual elements. Which of the following should be identified FIRST?

- ☐ Manual controls
- ☐ System risks
- ☐ Programmed controls
- ☐ Input validation

Question 2291

Which of the following is the PRIMARY advantage of the IT portfolio management approach over the balanced scorecard approach when managing IT investments?

- ☐ The influence of qualitative factors on investment decisions.
- ☐ Agility in adjusting investment decisions.
- ☐ Incorporation of organizational strategy in investment decisions.
- ☐ Use of the organization's risk appetite in investment decisions.

Question 2292

An IS auditor has just completed a physical access review of the organization's primary data center. Which of the following weaknesses should be of MOST concern?

- ☐ Metal keys are used for access.
- ☐ Backups of video cameras are corrupt.
- ☐ There is no mantrap at the main door.
- ☐ There is no manual logging for visitors.

Question 2293

Which of the following would prevent accountability for an action performed, thus allowing nonrepudiation?

- ☐ Proper authentication
- ☐ Proper identification AND authentication
- ☐ Proper identification
- ☐ Proper identification, authentication, AND authorization

Licensed to Berend Post berend.post@it-university.nl

Question 2294

Input/output controls should be implemented for which applications in an integrated systems environment?

- ☐ The receiving application
- ☐ The sending application
- ☐ Both the sending and receiving applications
- ☐ Output on the sending application and input on the receiving application

Question 2295

Which of the following communication modes should be of GREATEST concern to an IS auditor evaluating end-user networking?

- ☐ System-to-system
- ☐ Peer-to-peer
- ☐ Host-to-host
- ☐ Client-to-server

Question 2296

An organization is currently replacing its accounting system. Which of the following strategies will BEST minimize risk associated with the loss of data integrity from the upgrade?

- ☐ Pilot implementation
- ☐ Functional integration testing
- ☐ Fallback contingency
- ☐ Parallel implementation

Question 2297

Which of the following aspects of symmetric key encryption influenced the development of asymmetric encryption?

- ☐ Processing power
- ☐ Volume of data
- ☐ Key distribution
- ☐ Complexity of the algorithm

Licensed to Berend Post berend.post@it-university.nl

Question 2298

Which of the following BEST contributes to the successful management of security incidents?

- ☐ Tested controls
- ☐ Established procedures
- ☐ Established policies
- ☐ Current technologies

Question 2299

An operations manager has recently moved to internal audit. Which of the following would be of GREATEST concern when assigning audit projects to this individual?

- ☐ A control within the audit scope was implemented by the operations manager six months ago.
- ☐ A control within the audit scope was downgraded to low risk by the operations manager six months ago.
- ☐ The owner of a process within the audit scope worked for the operations manager six month ago.
- ☐ A system within the audit scope is supported by an emerging technology for which the operations manager lacks experience.

Question 2300

Which of the following satisfies a two-factor user authentication?

- ☐ Iris scanning plus fingerprint scanning
- ☐ Terminal ID plus global positioning system (GPS)
- ☐ A smart card requiring the user's PIN
- ☐ User ID along with password

Question 2301

Which of the following are the PRIMARY considerations when determining the timing of remediation testing?

- ☐ The level of management and business commitment to implementing agreed action plans
- ☐ The difficulty of scheduling resources and availability of management for a follow-up engagement
- ☐ The availability and competencies of control owners for implementing the agreed action
- ☐ The significance of the reported findings and the impact if corrective actions are not taken

Licensed to Berend Post berend.post@it-university.nl

Question 2302

An IS auditor is reviewing a project that is using an Agile software development approach. Which of the following should the IS auditor expect to find?

- ☐ Use a process-based maturity model such as the capability maturity model (CMM)
- ☐ Regular monitoring of task-level progress against schedule
- ☐ Extensive use of software development tools to maximize team productivity
- ☐ Postiteration reviews that identify lessons learned for future use in the project

Question 2303

An organization transmits large amounts of data from one internal system to another. The IS auditor is reviewing the quality of the data at the originating point. Which of the following should the auditor verify FIRST?

- ☐ The data has been encrypted.
- ☐ The data transformation is accurate.
- ☐ The data extraction process is completed.
- ☐ The source data is accurate.

Question 2304

Which of the following is a PRIMARY responsibility of an information security governance committee?

- ☐ Approving the purchase of information security technologies
- ☐ Approving the information security awareness training strategy
- ☐ Reviewing the information security strategy
- ☐ Analyzing information security policy compliance reviews

Question 2305

Which of the following is MOST important for an IS auditor to verify during a disaster recovery audit?

- ☐ Disaster recovery tests are carries out.
- ☐ Regular backups are made and stored offsite.
- ☐ The disaster recovery plan is updated on a regular basis.
- ☐ Media are stored in fireproof cabinets.

Licensed to Berend Post berend.post@it-university.nl

Question 2306

Information for detecting unauthorized input from a terminal would be BEST provided by the:

- ☐ console log printout.
- ☐ transaction journal.
- ☐ automated suspense file listing.
- ☐ user error report.

Question 2307

Which of the following is the BEST way to address potential data privacy concerns associated with inadvertent disclosure of machine identifier information contained within security logs?

- ☐ Only collect logs from servers classified as business critical.
- ☐ Limit the use of logs to only those purposes for which they were collected.
- ☐ Limit log collection to only periods of increased security activity.
- ☐ Restrict the transfer of log files from host machine to online storage.

Question 2308

Which of the following findings should be of GREATEST concern for an IS auditor when auditing the effectiveness of a phishing simulation test administered for staff members?

- ☐ Staff members were not notified about the test beforehand.
- ☐ Test results were not communicated to staff members.
- ☐ Staff members who failed the test did not receive follow-up education.
- ☐ Security awareness training was not provided prior to the test.

Question 2309

During a review of an insurance company's claims system, the IS auditor learns that claims for specific medical procedures are acceptable only from females. This is an example of a:

- ☐ key verification.
- ☐ completeness check.
- ☐ reasonableness check.
- ☐ logical relationship check.

Licensed to Berend Post berend.post@it-university.nl

Question 2310

An IS audit team is evaluating the documentation related to the most recent application user-access review performed by IT and business management. It is determined the user list was not system-generated. Which of the following should be the GREATEST concern?

- ☐ Source of the user list reviewed
- ☐ Availability of the user list reviewed
- ☐ Confidentiality of the user list reviewed
- ☐ Completeness of the user list reviewed

Question 2311

An IS auditor finds that, at certain times of the day, the data warehouse query performance decreases significantly. Which of the following controls would it be relevant for the IS auditor to review?

- ☐ Permanent table-space allocation
- ☐ Commitment and rollback controls
- ☐ User spool and database limit controls
- ☐ Read/write access log controls

Question 2312

An external audit team is deciding whether to rely on internal audit's work for an annual compliance audit. Which of the following is the GREATEST consideration when making this decision?

- ☐ Independence of the internal audit department from management's influence
- ☐ Professional certifications held by the internal audit team members
- ☐ Years of experience each of the internal auditors have in performing compliance audits
- ☐ The level of documentation maintained by internal audit and the methods used to collect evidence

Question 2313

A PRIMARY benefit derived by an organization employing control self-assessment (CSA) techniques is that CSA:

- ☐ can identify high-risk areas for detailed review.
- ☐ allows IS auditors to independently assess risk.
- ☐ can be used as a replacement for traditional audits.
- ☐ allows management to relinquish responsibility for control.

Licensed to Berend Post berend.post@it-university.nl

Question 2314

During an audit of a data center, an IS auditor's BEST way to gain an understanding of physical security controls is to:

- ☐ review the data center's physical security procedures.
- ☐ contact the alarm vendor and identify where alarms are installed in the data center.
- ☐ take a tour of the facility and identify physical security controls.
- ☐ obtain the engineering plans for the building and identify points of entry.

Question 2315

Which of the following statement correctly describes the difference between black box testing and white box testing?

- ☐ Black box testing focuses on functional operative effectiveness where as white box assesses the effectiveness of software program logic
- ☐ White box testing focuses on functional operative effectiveness where as black box assesses the effectiveness of software program logic
- ☐ White box and black box testing focuses on functional operative effectiveness of an information systems without regard to any internal program structure
- ☐ White box and black box testing focuses on the effectiveness of the software program logic

Question 2316

A company has decided to implement an electronic signature scheme based on public key infrastructure. The user's private key will be stored on the computer's hard drive and protected by a password. The MOST significant risk of this approach is:

- ☐ use of the user's electronic signature by another person if the password is compromised.
- ☐ forgery by using another user's private key to sign a message with an electronic signature.
- ☐ impersonation of a user by substitution of the user's public key with another person's public key.
- ☐ forgery by substitution of another person's private key on the computer.

Licensed to Berend Post berend.post@it-university.nl

Question 2317

An IS auditor finds that client requests were processed multiple times when received from different independent departmental databases, which are synchronized weekly. What would be the BEST recommendation?

- ☐ increase the frequency for data replication between the different department systems to ensure timely updates.
- ☐ Centralize all request processing in one department to avoid parallel processing of the same request.
- ☐ Change the application architecture so that common data is held in just one shared database for all departments.
- ☐ implement reconciliation controls to detect duplicates before orders are processed in the systems.

Question 2318

Which of the following testing method examines internal structure or working of an application?

- ☐ White-box testing
- ☐ Parallel Test
- ☐ Regression Testing
- ☐ Pilot Testing

Question 2319

Which of the following processes should an IS auditor recommend to assist in the recording of baselines for software releases?

- ☐ Change management
- ☐ Backup and recovery
- ☐ incident management
- ☐ Configuration management

Question 2320

Which of the following would BEST help to ensure compliance with an organization's information security requirements by an IT service provider?

- ☐ Defining the business recovery plan with the IT service provider
- ☐ Requiring an external security audits of the IT service provider
- ☐ Defining information security requirements with internal IT
- ☐ Requiring regular reporting from the IT service provider

Licensed to Berend Post berend.post@it-university.nl

Question 2321

In addition to the backup considerations for all systems, which of the following is an important consideration in providing backup for online systems?

- ☐ Maintaining system software parameters
- ☐ Ensuring periodic dumps of transaction logs
- ☐ Ensuring grandfather-father-son file backups
- ☐ Maintaining important data at an offsite location

Question 2322

Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

- ☐ ensure the employee maintains a good quality of life, which will lead to greater productivity.
- ☐ reduce the opportunity for an employee to commit an improper or illegal act.
- ☐ provide proper cross-training for another employee.
- ☐ eliminate the potential disruption caused when an employee takes vacation one day at a time.

Question 2323

Which of the following protocol is PRIMARILY used to provide confidentiality in a web based application thus protecting data sent across a client machine and a server?

- ☐ SSL
- ☐ FTP
- ☐ SSH
- ☐ S/MIME

Question 2324

An organization is considering replacing physical backup tapes stored offsite with real-time on-line backup to a storage area network (SAN) located in the primary data center. Which of the following is the GREATEST risk?

- ☐ Archived data may not satisfy data retention requirements
- ☐ A single disaster could cause significant data loss
- ☐ Backups may require excessive storage space
- ☐ Implementation could cause significant cost increases

Licensed to Berend Post berend.post@it-university.nl

Question 2325

Which of the following is the MOST important factor when an organization is developing information security policies and procedures?

- ☐ Cross-references between policies and procedures
- ☐ Inclusion of mission and objectives
- ☐ Compliance with relevant regulations
- ☐ Consultation with management

Question 2326

Which of the following is the GREATEST concern when an organization allows personal devices to connect to its network?

- ☐ It is difficult to enforce the security policy on personal devices
- ☐ Help desk employees will require additional training to support devices.
- ☐ IT infrastructure costs will increase.
- ☐ It is difficult to maintain employee privacy.

Question 2327

The output of the risk management process is an input for making:

- ☐ business plans.
- ☐ audit charters.
- ☐ security policy decisions.
- ☐ software design decisions.

Question 2328

If a database is restored from information backed up before the last system image, which of the following is recommended?

- ☐ The system should be restarted after the last transaction.
- ☐ The system should be restarted before the last transaction.
- ☐ The system should be restarted at the first transaction.
- ☐ The system should be restarted on the last transaction.

Licensed to Berend Post berend.post@it-university.nl

Question 2329

An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

- ☐ Log all table update transactions.
- ☐ implement before-and-after image reporting.
- ☐ Use tracing and tagging.
- ☐ implement integrity constraints in the database.

Question 2330

Which of the following is the GREATEST threat to Voice-over Internet Protocol (VoIP) related to privacy release?

- ☐ Incorrect routing
- ☐ Eavesdropping
- ☐ Call recording
- ☐ Denial of service

Question 2331

During the evaluation of a firm's newly established whistleblower system, an auditor notes several findings. Which of the following should be the auditor's GREATEST concern?

- ☐ New employees have not been informed of the whistleblower policy.
- ☐ The whistleblower's privacy is not protected.
- ☐ The whistleblower system does not track the time and date of submission.
- ☐ The whistleblower system is only available during business hours.

Question 2332

Which of the following is the PRIMARY purpose of red team testing?

- ☐ To determine the organization's preparedness for an attack
- ☐ To confirm the risk profile of the organization
- ☐ To assess the vulnerability of employees to social engineering
- ☐ To establish a baseline incident response program

Question 2333

Which of the following is the PRIMARY objective of the IS audit function?

- ☐ Perform reviews based on standards developed by professional organizations.
- ☐ Reports to management on the functioning of internal controls.
- ☐ Certify the accuracy of financial data.
- ☐ Facilitate extraction of computer-based data for substantive testing.

Licensed to Berend Post berend.post@it-university.nl

Question 2334

When planning an application audit, it is MOST important to evaluate risk factors by interviewing:

- ☐ process owners.
- ☐ application owners.
- ☐ IT management.
- ☐ application users.

Question 2335

An information security risk analysis BEST assists an organization in ensuring that:

- ☐ cost-effective decisions are made with regard to which assets need protection
- ☐ the organization implements appropriate security technologies
- ☐ the infrastructure has the appropriate level of access control
- ☐ an appropriate level of funding is applied to security processes

Question 2336

Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?

- ☐ Parity check
- ☐ Echo check
- ☐ Block sum check
- ☐ Cyclic redundancy check

Question 2337

An IS auditor should know information about different network transmission media. Which of the following transmission media is used for short distance transmission?

- ☐ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Satellite Radio Link

Question 2338

An organization has just completed their annual risk assessment. Regarding the business continuity plan, what should an IS auditor recommend as the next step for the organization?

- ☐ Review and evaluate the business continuity plan for adequacy
- ☐ Perform a full simulation of the business continuity plan
- ☐ Train and educate employees regarding the business continuity plan
- ☐ Notify critical contacts in the business continuity plan

Licensed to Berend Post berend.post@it-university.nl

Question 2339

The MOST important reason for documenting all aspects of a digital forensic investigation is that documentation:

- ☐ provides traceability for independent investigation by third parties.
- ☐ ensures compliance with corporate incident response policies.
- ☐ ensures the process will be repeatable in future investigations.
- ☐ meets IT audit documentation standards.

Question 2340

What is the key distinction between encryption and hashing algorithms?

- ☐ Hashing algorithms ensure data confidentiality.
- ☐ Hashing algorithms are irreversible.
- ☐ Encryption algorithms ensure data integrity.
- ☐ Encryption algorithms are not irreversible.

Question 2341

Which of the following access control situations represents the MOST serious control weakness?

- ☐ Computer operators have access to system level flowcharts.
- ☐ Programmers have access to development hardware.
- ☐ End users have access to program development tools.
- ☐ System developers have access to production data.

Question 2342

Which of the following is the MOST effective way to minimize the risk of a SQL injection attack?

- ☐ Reconfiguring content filtering settings
- ☐ Performing activity monitoring
- ☐ Using secure coding practices
- ☐ Implementing an intrusion detection tool

Licensed to Berend Post berend.post@it-university.nl

Question 2343

A business unit uses an e-commerce application with a strong password policy. Many customers complain that they cannot remember their passwords because they are too long and complex. The business unit states it is imperative to improve the customer experience. The information security manager should FIRST:

- ☐ change the password policy to improve the customer experience.
- ☐ recommend implementing two-factor authentication.
- ☐ research alternative secure methods of identity verification.
- ☐ evaluate the impact of the customer's experience on business revenue.

Question 2344

While planning a security audit, an IS auditor is made aware of a security review carried out by external consultants. It is MOST important for the auditor to:

- ☐ re-perform the security review.
- ☐ accept the findings and conclusions of the consultants.
- ☐ review similar reports issued by the consultants.
- ☐ assess the objectivity and competence of the consultants.

Question 2345

Which of the following types of transmission media provide the BEST security against unauthorized access?

- ☐ Copper wire
- ☐ Twisted pair
- ☐ Fiberoptic cables
- ☐ Coaxial cables

Question 2346

A company has purchased a rival organization and is looking to integrate security strategies. Which of the following is the GREATEST issue to consider?

- ☐ The organizations have different risk appetites
- ☐ Differing security technologies
- ☐ Differing security skills within the organizations
- ☐ Confidential information could be leaked

Licensed to Berend Post berend.post@it-university.nl

Question 2347

There are many types of audit logs analysis tools available in the market. Which of the following audit logs analysis tools will look for anomalies in user or system behavior?

- ☐ Attack Signature detection tool
- ☐ Variance detection tool
- ☐ Audit Reduction tool
- ☐ Heuristic detection tool

Question 2348

Which of the following is the BEST evidence of the maturity of an organization's information security program?

- ☐ The number of reported incidents has increased.
- ☐ The information security department actively monitors security operations.
- ☐ The number of reported incidents has decreased.
- ☐ IT security staff implements strict technical security controls.

Question 2349

Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

- ☐ Function Point Analysis (FPA)
- ☐ GANTT
- ☐ Rapid Application Development (RAD)
- ☐ PERT

Question 2350

Which of the following would BEST protect against web-based cross-domain attacks?

- ☐ Network addressing scheme
- ☐ Database hardening
- ☐ Encryption controls
- ☐ Application controls

Question 2351

Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data- calculation procedures. True or false?

- ☐ True
- ☐ False

Licensed to Berend Post berend.post@it-university.nl

Question 2352

When auditing third-party service providers, an IS auditor should be concerned with which of the following?

- ☐ Ownership of the programs and files
- ☐ A statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster
- ☐ A statement of due care
- ☐ Ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster

Question 2353

To protect information assets, which of the following should be done FIRST?

- ☐ Restrict access to data
- ☐ Encrypt data
- ☐ Classify data
- ☐ Back up data

Question 2354

Relatively speaking, firewalls operated at the application level of the seven layer OSI model are:

- ☐ almost always less efficient.
- ☐ almost always less effective.
- ☐ almost always less secure.
- ☐ almost always less costly to setup.
- ☐ None of the choices.

Question 2355

Which of the following would be the MOST efficient audit approach, given that a compliance-based approach was adopted in the previous year?

- ☐ Validate all applications using test data.
- ☐ Interview systems personnel to evaluate all automated controls.
- ☐ Evaluate the controls surrounding changes to programs.
- ☐ Perform a review of significant transactions posted within the system.

Licensed to Berend Post berend.post@it-university.nl

Question 2356

Which of the following function in traditional EDI translate data between the standard format and trading partner's propriety format?

- ☐ Communication handler
- ☐ Application Interface
- ☐ Application System
- ☐ EDI Translator

Question 2357

Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

- ☐ Deleting database activity logs
- ☐ Implementing database optimization tools
- ☐ Monitoring database usage
- ☐ Defining backup and recovery procedures

Question 2358

An IS auditor observes a system performance monitoring tool which states that a server critical to the organization averages high CPU utilization across a cluster of four virtual servers throughout the audit period. To determine if further investigation is required, an IS auditor should review:

- ☐ the system process activity log
- ☐ system baselines
- ☐ the number of CPUs allocated to each virtual machine
- ☐ organizational objectives

Question 2359

What should be done to determine the appropriate level of audit coverage for an organization's IT environment?

- ☐ determine the company's quarterly budget requirement.
- ☐ define an effective assessment methodology.
- ☐ calculate the company's yearly budget requirement.
- ☐ define an effective system upgrade methodology.
- ☐ define an effective network implementation methodology.

Licensed to Berend Post berend.post@it-university.nl

Question 2360

Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?

- ☐ Allocating resources
- ☐ Keeping current with technology advances
- ☐ Conducting control self-assessment
- ☐ Evaluating hardware needs

Question 2361

Which of the following is the BEST way to control the concurrent use of licensed software?

- ☐ User self-discipline.
- ☐ Monitor by system administrator.
- ☐ Surprise audit conducted by vendors.
- ☐ Metering software

Question 2362

Private Branch Exchange(PBX) environment involves many security risks, one of which is the people both internal and external to an organization. Which of the following risks are NOT associated with Private Branch Exchange?

1. Theft of service
2. Disclosure of information
3. Data Modifications
4. Denial of service
5. Traffic Analysis

- ☐ 3 and 4
- ☐ 4 and 5
- ☐ 1-4
- ☐ They are ALL risks associated with PBX

Question 2363

Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

- ☐ Concurrency controls
- ☐ Reasonableness checks
- ☐ Time stamps
- ☐ Referential integrity controls

Licensed to Berend Post berend.post@it-university.nl

Question 2364

Malicious program code was found in an application and corrected prior to release into production. After the release, the same issue was reported. Which of the following is the IS auditor's BEST recommendation?

- ☐ Ensure the business signs off on end-to-end user acceptance test results.
- ☐ Ensure corrected program code is compiled in a dedicated server.
- ☐ Ensure change management reports are independently reviewed.
- ☐ Ensure programmers cannot access code after the completion of program edits.

Question 2365

Which of the following step of PDCA request a corrective actions on significant differences between the actual versus the planned result?

- ☐ Plan
- ☐ Do
- ☐ Check
- ☐ Act

Question 2366

The purpose of a deadman door controlling access to a computer facility is primarily to:

- ☐ prevent piggybacking.
- ☐ prevent toxic gases from entering the data center.
- ☐ starve a fire of oxygen.
- ☐ prevent an excessively rapid entry to, or exit from, the facility.

Question 2367

A company has implemented an IT segregation of duties policy. In a role-based environment, which of the following roles may be assigned to an approach developer?

- ☐ IT operator
- ☐ Database administration
- ☐ System administration
- ☐ Emergency support

Licensed to Berend Post berend.post@it-university.nl

Question 2368

Which of the following public key infrastructure (PKI) elements provides detailed descriptions for dealing with a compromised private key?

- ☐ Certificate revocation list (CRL)
- ☐ Certification practice statement (CPS)
- ☐ Certificate policy (CP)
- ☐ PKI disclosure statement (PDS)

Question 2369

To prevent IP spoofing attacks, a firewall should be configured to drop a packet if:

- ☐ the source routing field is enabled.
- ☐ it has a broadcast address in the destination field.
- ☐ a reset flag (RST) is turned on for the TCP connection.
- ☐ dynamic routing is used instead of static routing.

Question 2370

To ensure authentication, confidentiality and integrity of a message, the sender should encrypt the hash of the message with the sender's:

- ☐ public key and then encrypt the message with the receiver's private key.
- ☐ private key and then encrypt the message with the receiver's public key.
- ☐ public key and then encrypt the message with the receiver's public key.
- ☐ private key and then encrypt the message with the receiver's private key.

Question 2371

Which of the following is protocol data unit (PDU) of network interface layer in TCP/IP model?

- ☐ Data
- ☐ Segment
- ☐ Packet
- ☐ Frame

Question 2372

Which of the following is a characteristic of timebox management?

- ☐ Not suitable for prototyping or rapid application development (RAD)
- ☐ Eliminates the need for a quality process
- ☐ Prevents cost overruns and delivery delays
- ☐ Separates system and user acceptance testing

Licensed to Berend Post berend.post@it-university.nl

Question 2373

Which of the following is the BEST method to defend against social engineering attacks?

- ☐ Periodically perform antivirus scans to identify malware.
- ☐ Communicate guidelines to limit information posted to public sites.
- ☐ Monitor for unauthorized access attempts and failed logins.
- ☐ Employ the use of a web-content filtering solution.

Question 2374

Which of the following access rights in the production environment should be granted to a developer to maintain segregation of duties?

- ☐ Database administration
- ☐ Emergency support
- ☐ IT operations
- ☐ System administration

Question 2375

The MAJOR advantage of a component-based development approach is the:

- ☐ ability to manage an unrestricted variety of data types.
- ☐ provision for modeling complex relationships.
- ☐ capacity to meet the demands of a changing environment.
- ☐ support of multiple development environments.

Question 2376

Which of the following are often considered as the first defensive line in protecting a typical data and information environment?

- ☐ certificates
- ☐ security token
- ☐ password
- ☐ biometrics
- ☐ None of the choices.

Question 2377

What should be a security manager's PRIMARY objective in the event of a security incident?

- ☐ Identify the source of the breach and how it was perpetrated.
- ☐ Contain the threat and restore operations in a timely manner.
- ☐ Ensure that normal operations are not disrupted.
- ☐ Identify lapses in operational control effectiveness.

Licensed to Berend Post berend.post@it-university.nl

Question 2378

Which of the following statement INCORRECTLY describes circuit switching technique?

- ☐ Packet uses many different dynamic paths to get the same destination
- ☐ Connection oriented virtual links
- ☐ Fixed delays
- ☐ Traffic travels in a predictable and constant manner

Question 2379

An organization wants to test business continuity using a scenario in which there are many remote workers trying to access production data at the same time. Which of the following is the BEST testing method in this situation?

- ☐ Application failover testing.
- ☐ Network stress testing.
- ☐ Alternate site testing.
- ☐ Network penetration testing.

Question 2380

Which of the following is a distinctive feature of the Secure Electronic Transactions (SET) protocol when used for electronic credit card payments?

- ☐ The buyer is assured that neither the merchant nor any other party can misuse their credit card data.
- ☐ All personal SET certificates are stored securely in the buyer's computer.
- ☐ The buyer is liable for any transaction involving his/her personal SET certificates.
- ☐ The payment process is simplified, as the buyer is not required to enter a credit card number and an expiration date.

Question 2381

Which of the following would be MOST important for an IS auditor to verify when conducting a business continuity audit?

- ☐ Data backups are performed on a timely basis
- ☐ A recovery site is contracted for and available as needed
- ☐ Human safety procedures are in place
- ☐ insurance coverage is adequate and premiums are current

Licensed to Berend Post berend.post@it-university.nl

Question 2382

When conducting a post-implementation review, which of the following is the BEST way to determine whether the value from an IT project has been achieved?

- ☐ Calculate the return on investment (ROI).
- ☐ Interview stakeholders.
- ☐ Conduct an earned value analysis (EVA).
- ☐ Survey end users.

Question 2383

A database is denormalized in order to:

- ☐ prevent loss of data.
- ☐ increase processing efficiency.
- ☐ ensure data integrity.
- ☐ save storage space.

Question 2384

Which of the following is the MOST important consideration when designing information security architecture?

- ☐ Risk management parameters for the organization are defined.
- ☐ The existing threat landscape is monitored.
- ☐ The information security architecture is aligned with industry standards.
- ☐ The level of security supported is based on business decisions.

Question 2385

When reviewing the process by which a contract for the outsourcing of various IT functions was completed, an IS auditor would ensure that the successful contractor:

- ☐ has eliminated the risks of outsourcing.
- ☐ maintains an internal audit function.
- ☐ requires a confidentiality agreement to be signed by all employees.
- ☐ was selected according to established business criteria.

Licensed to Berend Post berend.post@it-university.nl

Question 2386

Which of the following is the BEST way to mitigate the risk of unintentional modifications associated with complex calculations in end-user computing (EUC)?

- ☐ Verify EUC results through manual calculations.
- ☐ Operate copies of EUC programs out of a secure library.
- ☐ Implement data integrity checks.
- ☐ Utilize an independent party to review the source calculations.

Question 2387

An IS auditor is evaluating the access controls at a multinational company with a shared network infrastructure. Which of the following is MOST important?

- ☐ Simplicity of end-to-end communication paths
- ☐ Remote network administration
- ☐ Common security policies
- ☐ Logging of network information at user level

Question 2388

When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:

- ☐ allow changes, which will be completed using after-the-fact follow-up.
- ☐ allow undocumented changes directly to the production library.
- ☐ do not allow any emergency changes.
- ☐ allow programmers permanent access to production programs.

Question 2389

As an IS auditor it is very important to understand software release management process. Which of the following software release normally contains small enhancements and fixes?

- ☐ Major software Release
- ☐ Minor software Release
- ☐ Emergency software release
- ☐ General software Release

Licensed to Berend Post berend.post@it-university.nl

Question 2390

What should an IS auditor do when informed that some recommendations cannot be implemented due to financial constraints?

- ☐ Document management's response in the working papers.
- ☐ Insist the recommendations be implemented.
- ☐ Agree to waive the recommendations.
- ☐ Suggest management identify cost-effective alternatives.

Question 2391

The PRIMARY objective of implementing corporate governance by an organization's management is to:

- ☐ provide strategic direction.
- ☐ control business operations.
- ☐ align IT with business.
- ☐ implement best practices.

Question 2392

The purpose of code signing is to provide assurance that:

- ☐ the software has not been subsequently modified.
- ☐ the application can safely interface with another signed application.
- ☐ the signer of the application is trusted.
- ☐ the private key of the signer has not been compromised.

Question 2393

An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

- ☐ the controls already in place.
- ☐ the effectiveness of the controls in place.
- ☐ the mechanism for monitoring the risks related to the assets.
- ☐ the threats/vulnerabilities affecting the assets.

Licensed to Berend Post berend.post@it-university.nl

Question 2394

A company uses a standard form to document and approve all changes in production programs. To ensure that the forms are properly authorized, which of the following is the MOST effective sampling method?

- ☐ Attribute
- ☐ Variable
- ☐ Discovery
- ☐ Monetary

Question 2395

Which of the following components of a scheduling tool BEST prevents job failures due to insufficient system resources?

- ☐ Job dependencies
- ☐ Delayed job starts
- ☐ Exception handling
- ☐ Error alerts

Question 2396

Which of the following BEST minimizes performance degradation of servers used to authenticate users of an e-commerce website?

- ☐ Configure each authentication server and ensure that the disks of each server form part of a duplex.
- ☐ Configure each authentication server as belonging to a cluster of authentication servers.
- ☐ Configure a single server as a primary authentication server and a second server as a secondary authentication server.
- ☐ Configure each authentication server and ensure that each disk of its RAID is attached to the primary controller.

Question 2397

Which of the following methods of providing telecommunications continuity involves the use of an alternative media?

- ☐ Alternative routing
- ☐ Diverse routing
- ☐ Long haul network diversity
- ☐ Last mile circuit protection

Licensed to Berend Post berend.post@it-university.nl

Question 2398

A bank is selecting a server for its retail accounts application. To ensure that the server can handle a high volume of transactions with the required response times, which test should the IS auditor recommend?

- ☐ Regression
- ☐ Acceptance
- ☐ Benchmark
- ☐ Integration

Question 2399

An IS auditor is assigned to audit a software development project which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

- ☐ Report that the organization does not have effective project management.
- ☐ Recommend the project manager be changed.
- ☐ Review the IT governance structure.
- ☐ Review the conduct of the project and the business case.

Question 2400

Processing controls ensure that data is accurate and complete, and is processed only through which of the following?

- ☐ Documented routines
- ☐ Authorized routines
- ☐ Accepted routines
- ☐ Approved routines

Question 2401

Which of the following is MOST important to include in an organization's incident response plan to help prevent similar incidents from happening in the future?

- ☐ Documentation of incident details
- ☐ Incident closure procedures
- ☐ Containment and neutralization actions
- ☐ Post-incident review

Licensed to Berend Post berend.post@it-university.nl

Question 2402

Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource?

- ☐ Systems logs
- ☐ Access control lists (ACL)
- ☐ Application logs
- ☐ Error logs

Question 2403

The MAIN purpose of a transaction audit trail is to:

- ☐ reduce the use of storage media.
- ☐ determine accountability and responsibility for processed transactions.
- ☐ help an IS auditor trace transactions.
- ☐ provide useful information for capacity planning.

Question 2404

Which of the following is a passive attack to a network?

- ☐ Message modification
- ☐ Masquerading
- ☐ Denial of service
- ☐ Traffic analysis

Question 2405

An organization's software develops need access to personally identifiable information (PII) stored in a particular data format. Which of the following would be the BEST way to protect this sensitive information while allowing the developers to use it in development and test environments?

- ☐ Data masking
- ☐ Data encryption
- ☐ Data tokenization
- ☐ Data abstraction

Licensed to Berend Post berend.post@it-university.nl

Question 2406

Which of the following is the MOST effective method of destroying sensitive data stored on electronic media?

- ☐ Physical destruction
- ☐ Degaussing
- ☐ Random character overwrite
- ☐ Low-level formatting

Question 2407

In which of the following database model is the data organized into a tree-like structure, implying a single parent for each record?

- ☐ Hierarchical database model
- ☐ Network database model
- ☐ Relational database model
- ☐ Object-relational database model

Question 2408

When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator to ensure that the:

- ☐ hardware is protected against power surges.
- ☐ integrity is maintained if the main power is interrupted.
- ☐ immediate power will be available if the main power is lost.
- ☐ hardware is protected against long-term power fluctuations.

Question 2409

Which of the following provides for the GREATEST cost reduction in a large data center?

- ☐ Server consolidation
- ☐ Staff rotation
- ☐ Power conditioning
- ☐ Job-scheduling software

Licensed to Berend Post berend.post@it-university.nl

Question 2410

An organization is developing data classification standards and has asked internal audit for advice on aligning the standards with best practices. Internal audit would MOST likely recommend the standards should be:

- ☐ based on the results of an organization-wide risk assessment.
- ☐ based on the business requirements for confidentiality of the information.
- ☐ aligned with the organization's segregation of duties requirements.
- ☐ based on the business requirements for authentication of the information.

Question 2411

An information systems security officer's PRIMARY responsibility for business process applications is to:

- ☐ create role-based rules for each business process.
- ☐ ensure access rules agree with policies.
- ☐ authorize secured emergency access.
- ☐ approve the organization's security policy.

Question 2412

Which of the following would BEST describe an audit risk?

- ☐ The company is being sued for false accusations.
- ☐ The financial report may contain undetected material errors.
- ☐ Key employees have not taken vacation for 2 years.
- ☐ Employees have been misappropriating funds.

Question 2413

During the requirements definition phase of a software development project, the aspects of software testing that should be addressed are developing:

- ☐ test data covering critical applications.
- ☐ detailed test plans.
- ☐ quality assurance test specifications.
- ☐ user acceptance testing specifications

Licensed to Berend Post berend.post@it-university.nl

Question 2414

Which of the following is the GREATEST concern associated with control self-assessments?

- ☐ Employees may have insufficient awareness of controls
- ☐ Controls may not be assessed objectively
- ☐ Communication between operational management and senior management may not be effective
- ☐ The assessment may not provide sufficient assurance to stakeholders

Question 2415

Which of the following outsourced services has the GREATEST need for security monitoring?

- ☐ Web site hosting
- ☐ Application development
- ☐ Virtual private network (VPN) services
- ☐ Enterprise infrastructure

Question 2416

An organization is considering moving one of its critical business applications to a cloud hosting service. The cloud provider may not provide the same level of security for this application as the organization. Which of the following will provide the BEST information to help maintain the security posture?

- ☐ Risk assessment
- ☐ Cloud security strategy
- ☐ Vulnerability assessment
- ☐ Risk governance framework

Question 2417

When auditing the proposed acquisition of a new computer system, an IS auditor should FIRST establish that:

- ☐ a clear business case has been approved by management.
- ☐ corporate security standards will be met.
- ☐ users will be involved in the implementation plan.
- ☐ the new system will meet all required user functionality.

Licensed to Berend Post berend.post@it-university.nl

Question 2418

Which of the following fourth generation language is a development tools to generate lower level programming languages?

- ☐ Query and report generator
- ☐ Embedded database 4GLs
- ☐ Relational database 4GL
- ☐ Application generators

Question 2419

Which of the following is the BEST way to demonstrate to senior management that organizational security practices comply with industry standards?

- ☐ A report on the maturity of controls
- ☐ Up-to-date policy and procedures documentation
- ☐ Existence of an industry-accepted framework
- ☐ Results of an independent assessment

Question 2420

Which of the following is the MOST important criterion when selecting a location for an offsite storage facility for IS backup files? The offsite facility must be:

- ☐ physically separated from the data center and not subject to the same risks.
- ☐ given the same level of protection as that of the computer data center.
- ☐ outsourced to a reliable third party.
- ☐ equipped with surveillance capabilities.

Question 2421

Which of the following software development methodology is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems?

- ☐ Agile Developments
- ☐ Software prototyping
- ☐ Rapid application development
- ☐ Component based development

Licensed to Berend Post berend.post@it-university.nl

Question 2422

Which of the following is the GREATEST advantage of elliptic curve encryption over RSA encryption?

- ☐ Computation speed
- ☐ Ability to support digital signatures
- ☐ Simpler key distribution
- ☐ Greater strength for a given key length

Question 2423

When auditing a disaster recovery plan for a critical business area, an IS auditor finds that it does not cover all the systems. Which of the following is the MOST appropriate action for the IS auditor?

- ☐ Alert management and evaluate the impact of not covering all systems.
- ☐ Cancel the audit.
- ☐ Complete the audit of the systems covered by the existing disaster recovery plan.
- ☐ Postpone the audit until the systems are added to the disaster recovery plan.

Question 2424

Batch control reconciliation is a _____ (fill the blank) control for mitigating risk of inadequate segregation of duties.

- ☐ Detective
- ☐ Corrective
- ☐ Preventative
- ☐ Compensatory

Question 2425

Which of the following is the BEST approach to make strategic information security decisions?

- ☐ Establish regular information security status reporting
- ☐ Establish business unit security working groups
- ☐ Establish periodic senior management meetings
- ☐ Establish an information security steering committee

Question 2426

The MOST effective biometric control system is the one:

- ☐ which has the highest equal-error rate (EER).
- ☐ which has the lowest EER.
- ☐ for which the false-rejection rate (FRR) is equal to the false-acceptance rate (FAR).
- ☐ for which the FRR is equal to the failure-to-enroll rate (FER).

Licensed to Berend Post berend.post@it-university.nl

Question 2427

A start-up company acquiring servers for its order-taking system is unable to predict the volume of transactions. Which of the following is MOST important for the company to consider?

- ☐ Scalability
- ☐ Configuration
- ☐ Optimization
- ☐ Compatibility

Question 2428

Which of the following is NOT an example of corrective control?

- ☐ OS Upgrade
- ☐ Backup and restore
- ☐ Contingency planning
- ☐ System Monitoring

Question 2429

Which of the following IS audit findings should be of GREATEST concern when preparing to migrate to a new core system using a direct cut-over?

- ☐ Incomplete test cases for some critical reports
- ☐ Informal management approval to go live
- ☐ Lack of a rollback strategy for the system go-live
- ☐ Plans to use some workarounds for an extended period after go-live

Question 2430

When an intrusion into an organization's network is detected, which of the following should be performed FIRST?

- ☐ Block all compromised network nodes.
- ☐ Protect information in the compromised systems.
- ☐ Develop a response to the incident.
- ☐ Identify nodes that have been compromised.

Licensed to Berend Post berend.post@it-university.nl

Question 2431

In large corporate networks having supply partners across the globe, network traffic may continue to rise. The infrastructure components in such environments should be scalable. Which of the following firewall architectures limits future scalability?

- ☐ Appliances
- ☐ Operating system-based
- ☐ Host-based
- ☐ Demilitarized

Question 2432

Which of the following is NOT a component of IPSec?

- ☐ Authentication Header
- ☐ Encapsulating Security Payload
- ☐ Key Distribution Center
- ☐ Internet Key Exchange

Question 2433

Which of the following component of an expert system enables the expert system to collect data from nonhuman sources, such as measurement instruments in a power plant?

- ☐ Decision tree
- ☐ Rules
- ☐ Semantic nets
- ☐ Data interface

Question 2434

During an IS audit, auditor has observed that authentication and authorization steps are split into two functions and there is a possibility to force the authorization step to be completed before the authentication step. Which of the following technique an attacker could user to force authorization step before authentication?

- ☐ Eavesdropping
- ☐ Traffic analysis
- ☐ Masquerading
- ☐ Race Condition

Licensed to Berend Post berend.post@it-university.nl

Question 2435

Which of the following refers to the collection of policies and procedures for implementing controls capable of restricting access to computer software and data files?

- ☐ Binary access control
- ☐ System-level access control
- ☐ Logical access control
- ☐ Physical access control
- ☐ Component access control
- ☐ None of the choices.

Question 2436

Which of the following is the MOST effective control for a utility program?

- ☐ Renaming the versions in the programmers' libraries
- ☐ Installing the program on a separate server
- ☐ Storing the program in a production library
- ☐ Allowing only authorized personnel to use the program

Question 2437

An IS auditor has been asked to perform a post-implementation assessment of a new corporate human resources (HR) system. Which of the following control areas would be MOST important to review for the protection of employee information?

- ☐ Logging capabilities
- ☐ Authentication mechanisms
- ☐ Data retention practices
- ☐ System architecture

Question 2438

Which of the following is the BEST way to address ongoing concerns with the quality and accuracy of internal audits?

- ☐ Engage an independent review of the audit function.
- ☐ Require peer reviews of audit workpapers.
- ☐ Implement performance management for IS auditors.
- ☐ Require IS audit management to lead exit meetings.

Licensed to Berend Post berend.post@it-university.nl

Question 2439

Which of the following audit risk is related to material error exist that would not be prevented or detected on timely basis by the system of internal controls?

- ☐ Inherent Risk
- ☐ Control Risk
- ☐ Detection Risk
- ☐ Overall Audit Risk

Question 2440

To gain a clear understanding of the impact that a new regulatory requirement will have on an organization's information security controls, an information security manager should FIRST:

- ☐ conduct a risk assessment.
- ☐ perform a gap analysis.
- ☐ conduct a cost-benefit analysis.
- ☐ interview senior management.

Question 2441

Which of the following BEST demonstrates effective information security management within an organization?

- ☐ Employees support decisions made by information security management.
- ☐ Excessive risk exposure in one department can be absorbed by other departments.
- ☐ Information security governance is incorporated into organizational governance.
- ☐ Control ownership is assigned to parties who can accept losses related to control failure.

Question 2442

An IS auditor observes that routine backups of operational databases are taking longer than before. Which of the following would MOST effectively help to reduce backup and recovery times for operational databases?

- ☐ Utilizing database technologies to achieve efficiencies
- ☐ Using solid storage device (SSD) media
- ☐ Requiring a combination of weekly full backups and daily differential backups
- ☐ Archiving historical data in accordance with the data retention policy

Licensed to Berend Post berend.post@it-university.nl

Question 2443

A recent audit identified duplicate software licenses and technologies. Which of the following would be MOST helpful to prevent this type of duplication in the future?

- ☐ Centralizing IT procurement and approval practices
- ☐ Updating IT procurement policies and procedures
- ☐ Conducting periodic inventory reviews
- ☐ Establishing a project management office

Question 2444

What is an effective control for granting temporary access to vendors and external support personnel?

- ☐ Creating user accounts that automatically expire by a predetermined date
- ☐ Creating permanent guest accounts for temporary use
- ☐ Creating user accounts that restrict logon access to certain hours of the day
- ☐ Creating a single shared vendor administrator account on the basis of least-privileged access

Question 2445

Which of the following is the BEST reason for an organization to develop a business continuity plan?

- ☐ To develop a detailed description of information systems and processes
- ☐ To identify the users of information systems and processes
- ☐ To avoid the costs resulting from the failure of key systems and processes
- ☐ To establish business unit prioritization of systems, projects, and strategies

Question 2446

When should plans for testing for user acceptance be prepared?

- ☐ In the requirements definition phase of the systems-development project
- ☐ In the feasibility phase of the systems-development project
- ☐ In the design phase of the systems-development project
- ☐ In the development phase of the systems-development project

Licensed to Berend Post berend.post@it-university.nl

Question 2447

Which of the following is MOST important for an IS auditor to determine when reviewing how the organization's incident response team handles devices that may be involved in criminal activity?

- ☐ Whether devices are checked for malicious applications
- ☐ Whether the access logs are checked before seizing the devices
- ☐ Whether users have knowledge of their devices being examined
- ☐ Whether there is a chain of custody for the devices

Question 2448

The Trojan.Linux.JBellz Trojan horse runs as a malformed file of what format?

- ☐ e-mails.
- ☐ MP3.
- ☐ MS Office.
- ☐ Word template.
- ☐ None of the choices.

Question 2449

The recovery point objective (RPO) is required in which of the following?

- ☐ Information security plan
- ☐ Incident response plan
- ☐ Disaster recovery plan
- ☐ Business continuity plan

Question 2450

Why would a database be renormalized?

- ☐ To ensure data integrity
- ☐ To increase processing efficiency
- ☐ To prevent duplication of data
- ☐ To save storage space

Question 2451

Which of the following would be the MOST important information to include in a business case for an information security project in a highly regulated industry?

- ☐ Industry comparison analysis
- ☐ Critical audit findings
- ☐ Compliance risk assessment
- ☐ Number of reported security incidents

Licensed to Berend Post berend.post@it-university.nl

Question 2452

An IS auditor analyzing the audit log of a database management system (DBMS) finds that some transactions were partially executed as a result of an error, and are not rolled back. Which of the following transaction processing features has been violated?

- ☐ Consistency
- ☐ Isolation
- ☐ Durability
- ☐ Atomicity

Question 2453

During the testing of the business continuity plan (BCP), which of the following methods of results analysis provides the BEST assurance that the plan is workable?

- ☐ Measurement of accuracy
- ☐ Elapsed time for completion of critical tasks
- ☐ Quantitatively measuring the results of the test
- ☐ Evaluation of the observed test results

Question 2454

Failure in which of the following testing stages would have the GREATEST impact on the implementation of new application software?

- ☐ System testing
- ☐ Acceptance testing
- ☐ Integration testing
- ☐ Unit testing

Licensed to Berend Post berend.post@it-university.nl

Question 2455

While evaluating logical access control the IS auditor should follow all of the steps mentioned below EXCEPT one?

1. Obtain general understanding of security risk facing information processing, through a review of relevant documentation, inquiry and observation,etc
2. Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness
3. Test Control over access paths to determine whether they are functioning and effective by applying appropriate audit technique
4. Evaluate the access control environment to determine if the control objective is achieved by analyzing test result and other audit evidence
5. Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures, and comparing them with appropriate security standard or practice and procedures used by other organization.
6. Evaluate and deploy technical controls to mitigate all identified risks during audit.

- ☐ 2
- ☐ 3
- ☐ 1
- ☐ 6

Question 2456

When planning an audit, it is acceptable for an IS auditor to rely on a third-party provider's external audit report on service level management when the:

- ☐ report was released within the last 12 months.
- ☐ scope and methodology meet audit requirements.
- ☐ service provider is independently certified and accredited.
- ☐ report confirms that service levels were not violated.

Question 2457

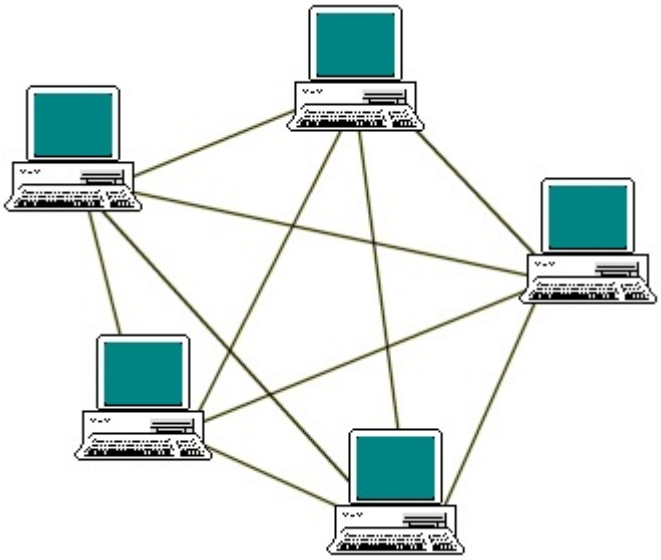
A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:

- ☐ Identify high-risk areas that might need a detailed review later
- ☐ Reduce audit costs
- ☐ Reduce audit time
- ☐ Increase audit accuracy

Licensed to Berend Post berend.post@it-university.nl

Question 2458

Identify the network topology from below diagram presented below:



Network Topology

- ☐ Bus
- ☐ Star
- ☐ Ring
- ☐ Mesh

Question 2459

Which of the following is the MOST effective way to identify anomalous transactions when performing a payroll fraud audit?

- ☐ Substantive testing of payroll files
- ☐ Data analytics on payroll data
- ☐ Observation of payment processing
- ☐ Sample-based review of pay stubs

Question 2460

An IT steering committee assists the board of directors to fulfill IT governance duties by:

- ☐ developing IT policies and procedures for project tracking.
- ☐ focusing on the supply of IT services and products.
- ☐ overseeing major projects and IT resource allocation.
- ☐ implementing the IT strategy.

Licensed to Berend Post berend.post@it-university.nl

Question 2461

The implementation of access controls FIRST requires:

- ☐ a classification of IS resources.
- ☐ the labeling of IS resources.
- ☐ the creation of an access control list.
- ☐ an inventory of IS resources.

Question 2462

What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

- ☐ Assigning copyright to the organization
- ☐ Program back doors
- ☐ Source code escrow
- ☐ Internal programming expertise

Question 2463

Which of the following statement correctly describes the difference between QAT and UAT?

- ☐ QAT focuses on technical aspect of the application and UAT focuses on functional aspect of the application
- ☐ UAT focuses on technical aspect of the application and QAT focuses on functional aspect of the application
- ☐ UAT and QAT both focuses on functional aspect of the application
- ☐ UAT and QAT both focuses on technical aspect of the application

Question 2464

Which of the following is the MOST effective way to prevent unauthorized changes from being moved into production?

- ☐ Conduct periodic review of change tickets to ensure all change documentation is attached.
- ☐ Enforce segregation of duties between developers and migrators.
- ☐ Perform thorough testing of changes in the test environment.
- ☐ Require approval of changes by the appropriate business process owners.

Licensed to Berend Post berend.post@it-university.nl

Question 2465

Which of the following message services provides the strongest evidence that a specific action has occurred?

- ☐ Proof of delivery
- ☐ Nonrepudiation
- ☐ Proof of submission
- ☐ Message origin authentication

Question 2466

When choosing the best controls to mitigate risk to acceptable levels, the information security manager's decision should be MAINLY driven by:

- ☐ cost-benefit analysis
- ☐ regulatory requirements
- ☐ best practices
- ☐ control framework

Question 2467

An organization has a number of branches across a wide geographical area. To ensure that all aspects of the disaster recovery plan are evaluated in a cost effective manner, an IS auditor should recommend the use of a:

- ☐ data recovery test.
- ☐ full operational test.
- ☐ posttest.
- ☐ preparedness test.

Question 2468

As an outcome of information security governance, strategic alignment provides:

- ☐ security requirements driven by enterprise requirements.
- ☐ baseline security following best practices.
- ☐ institutionalized and commoditized solutions.
- ☐ an understanding of risk exposure.

Licensed to Berend Post berend.post@it-university.nl

Question 2469

An IS auditor reviews change control tickets and finds an emergency change request where an IT manager approved the change modified the code on the production platform, and resolved the ticket. Which of the following should be the auditor's GREATEST concern?

- ☐ There was no follow-up approval from the business.
- ☐ The change was made less than an hour after the request.
- ☐ There was no testing prior to making the change in production.
- ☐ The IT manager performed the change and resolved the ticket.

Question 2470

The database administrator (DBA) suggests that DB efficiency can be improved by denormalizing some tables. This would result in:

- ☐ loss of confidentiality.
- ☐ increased redundancy.
- ☐ unauthorized accesses.
- ☐ application malfunctions.

Question 2471

An IS auditor reviewing the use of encryption finds that the symmetric key is sent by an email message between the parties. Which of the following audit responses is correct in this situation?

- ☐ An audit finding is recorded, as the key should be asymmetric and therefore changed.
- ☐ No audit finding is recorded, as it is normal to distribute a key of this nature in this manner.
- ☐ No audit finding is recorded, as the key can only be used once.
- ☐ An audit finding is recorded as the key should be distributed in a secure manner.

Question 2472

A CEO requests access to corporate documents from a mobile device that does not comply with organizational policy. The information security manager should FIRST:

- ☐ evaluate the business risk
- ☐ evaluate a third-party solution
- ☐ initiate an exception approval process
- ☐ deploy additional security controls

Licensed to Berend Post berend.post@it-university.nl

Question 2473

An IS auditor has discovered that unauthorized customer management software was installed on a workstation. The auditor determines the software has been uploading customer data to an external party. Which of the following is the IS auditor's BEST course of action?

- ☐ Review other workstations to determine the extent of the incident.
- ☐ Determine the number of customer records that were uploaded.
- ☐ Notify the incident response team.
- ☐ Present the issue at the next audit progress meeting.

Question 2474

Which of the following is the BEST guidance from an IS auditor to an organization planning an initiative to improve the effectiveness of its IT processes?

- ☐ IT staff should be surveyed to identify current IT process weaknesses and suggest improvements.
- ☐ The organization should use a capability maturity model to identify current maturity levels for each IT process.
- ☐ IT management should include process improvements in staff performance
- ☐ The organization should refer to prior audit reports to identify the specific IT processes to be improved.

Question 2475

What is an IS auditor's BEST recommendation to management if a review of the incident management process finds multiple instances of incident tickets remaining open for an unusually long time?

- ☐ Implement reporting of key performance indicators (KPIs) for ticket closure.
- ☐ Increase the number of help desk staff to enable faster ticket closure.
- ☐ Manually review the identified tickets and mark as closed in the system.
- ☐ Configure the system to automatically close tickets after a defined period.

Question 2476

Which of the following is the PRIMARY purpose of data classification?

- ☐ To determine access rights to data
- ☐ To provide a basis for protecting data
- ☐ To select encryption technologies
- ☐ To ensure integrity of data

Licensed to Berend Post berend.post@it-university.nl

Question 2477

An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. What would be the next task?

- ☐ Report the risks to the CIO and CEO immediately
- ☐ Examine e-business application in development
- ☐ Identify threats and likelihood of occurrence
- ☐ Check the budget available for risk management

Question 2478

Who is responsible for authorizing access level of a data user?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☐ Security Administrator

Question 2479

Which of the following audit mainly focuses on discovering and disclosing on frauds and crimes?

- ☐ Compliance Audit
- ☐ Financial Audit
- ☐ Integrated Audit
- ☐ Forensic audit

Question 2480

An IS auditor is asked to identify risk within an organization’s software development project. The project manager tells the auditor that an agile development methodology is being used to minimize the lengthy development process. Which of the following would be of GREATEST concern to the auditor?

- ☐ Each team does its own testing.
- ☐ The needed work has not yet been fully identified.
- ☐ Some of the developers have not attended recent training.
- ☐ Elements of the project have not been documented.

Licensed to Berend Post berend.post@it-university.nl

Question 2481

Which of the following PBX feature allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available?

- ☐ Automatic Call distribution
- ☐ Call forwarding
- ☐ Tenanting
- ☐ Voice mail

Question 2482

During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

- ☐ create the procedures document.
- ☐ terminate the audit.
- ☐ conduct compliance testing.
- ☐ identify and evaluate existing practices.

Question 2483

The MOST effective control to detect fraud inside an organization's network, is to:

- ☐ implement an intrusion detection system (IDS)
- ☐ apply two-factor authentication
- ☐ review access logs
- ☐ segregate duties

Question 2484

Which of the following is an oft-cited cause of vulnerability of networks?

- ☐ software monoculture
- ☐ software diversification
- ☐ single line of defense
- ☐ multiple DMZ
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 2485

An IS auditor finds that corporate mobile devices used by employees have varying levels of password settings. Which of the following would be the BEST recommendation?

- ☐ Update the acceptable use policy for mobile devices.
- ☐ Notify employees to set passwords to a specified length.
- ☐ Encrypt data between corporate gateway and devices.
- ☐ Apply a security policy to the mobile devices.

Question 2486

Why is the WAP gateway a component warranting critical concern and review for the IS auditor when auditing and testing controls enforcing message confidentiality?

- ☐ WAP is often configured by default settings and is thus insecure.
- ☐ WAP provides weak encryption for wireless traffic.
- ☐ WAP functions as a protocol-conversion gateway for wireless TLS to Internet SSL.
- ☐ WAP often interfaces critical IT systems.

Question 2487

Which of the following methods of encryption has been proven to be almost unbreakable when correctly used?

- ☐ key pair
- ☐ Oakley
- ☐ certificate
- ☐ 3-DES
- ☐ one-time pad
- ☐ None of the choices.

Question 2488

Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

- ☐ Redundancy check
- ☐ Completeness check
- ☐ Accuracy check
- ☐ Parity check

Licensed to Berend Post berend.post@it-university.nl

Question 2489

When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

- ☐ has all the personnel and equipment it needs.
- ☐ plans are consistent with management strategy.
- ☐ uses its equipment and personnel efficiently and effectively.
- ☐ has sufficient excess capacity to respond to changing directions.

Question 2490

IT service engineers at a large organization are unable to effectively prioritize system-generated alerts from hundreds of applications running across multiple servers and databases. As a result, many alerts are often ignored, leading to major problems including downtime. Which of the following is the BEST IS audit recommendation to address this situation?

- ☐ Prioritize alerts from legacy applications that may require remote support from external vendors.
- ☐ Implement a threshold management system that prioritizes alerts over a certain age.
- ☐ Develop a classification scheme that prioritizes alerts according to potential business impact.
- ☐ Group alerts from related systems and immediately escalate to the application owner.

Question 2491

Management has decided to include a compliance manager in the approval process for a new business that may require changes to the IT infrastructure. Which of the following is the GREATEST benefit of this approach?

- ☐ Security breach incidents can be identified in early stages.
- ☐ Regulatory risk exposures can be identified before they materialize.
- ☐ Fewer reviews are needed when updating the IT compliance process.
- ☐ Process accountabilities to external stakeholders are improved.

Question 2492

To ensure confidentiality through the use of asymmetric encryption, a message is encrypted with which of the following?

- ☐ Sender's private key
- ☐ Recipient's private key
- ☐ Sender's public key
- ☐ Recipient's public key

Licensed to Berend Post berend.post@it-university.nl

Question 2493

An IS auditor notes that a loan servicing group retains customer personally identifiable information (PII) on a shared drive. Which of the following is MOST important to ensure compliance with privacy principles?

- ☐ Backups are performed in accordance with organizational policy.
- ☐ Access to the shared drive must be approved by the manager of the group.
- ☐ The data is maintained in accordance with the business's retention policy.
- ☐ All key customer data elements are captured on the shared drive.

Question 2494

The most common problem in the operation of an intrusion detection system (IDS) is:

- ☐ the detection of false positives.
- ☐ receiving trap messages.
- ☐ reject-error rates.
- ☐ denial-of-service attacks.

Question 2495

Which of the following is the BEST approach for performing a business impact analysis (BIA) of a supply-chain management application?

- ☐ Circulating questionnaires to key internal stakeholders
- ☐ Interviewing groups of key stakeholders
- ☐ Accepting IT personnel's view of business issues
- ☐ Reviewing the organization's policies and procedures

Question 2496

What is the BEST indicator of successful implementation of an organization's information security policy?

- ☐ Reduced number of successful phishing incidents
- ☐ Reduced number of help desk calls
- ☐ Reduced number of noncompliance penalties incurred
- ☐ Reduced number of false-positive security events

Licensed to Berend Post berend.post@it-university.nl

Question 2497

Which of the following is an example of a change to the external threat landscape?

- ☐ Organizational security standards have been modified.
- ☐ A commonly used encryption algorithm has been compromised.
- ☐ New legislation has been enacted in a region where the organization does business.
- ☐ Infrastructure changes to the organization have been implemented.

Question 2498

The editing/validation of data entered at a remote site would be performed MOST effectively at the:

- ☐ central processing site after running the application system.
- ☐ central processing sire during the running of the application system.
- ☐ remote processing site after transmission of the data to the central processing site.
- ☐ remote processing site prior to transmission of the data to the central processing site.

Question 2499

Which of the following is best suited for searching for address field duplications?

- ☐ Text search forensic utility software
- ☐ Generalized audit software
- ☐ Productivity audit software
- ☐ Manual review

Question 2500

Which of the following projects would be MOST important to review in an audit of an organization's financial statements?

- ☐ Resource optimization of the enterprise resource planning (ERP) system
- ☐ Security enhancements to the customer relationship database
- ☐ Automation of operational risk management processes
- ☐ Outsourcing of the payroll system to an external service provider

Question 2501

Which of the following is an advantage of asymmetric crypto system over symmetric key crypto system?

- ☐ Performance and Speed
- ☐ Key Management is built in
- ☐ Adequate for Bulk encryption
- ☐ Number of keys grows very quickly

Licensed to Berend Post berend.post@it-university.nl

Question 2502

Which of the following should an IS auditor recommend to reduce the likelihood of potential intruders using social engineering?

- ☐ Perform simulated attacks.
- ☐ Prohibit the use of social networking platforms.
- ☐ Implement an intrusion detection system (IDS).
- ☐ Deploy a security awareness program.

Question 2503

The use of risk assessment tools for classifying risk factors should be formalized in your IT audit effort through:

- ☐ the use of risk controls.
- ☐ the use of computer assisted functions.
- ☐ using computer assisted audit technology tools.
- ☐ the development of written guidelines.
- ☐ None of the choices.

Question 2504

Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:

- ☐ include the statement of management in the audit report.
- ☐ identify whether such software is, indeed, being used by the organization.
- ☐ reconfirm with management the usage of the software.
- ☐ discuss the issue with senior management since reporting this could have a negative impact on the organization.

Question 2505

Company.com has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

- ☐ Acceptance testing is to be managed by users.
- ☐ A quality plan is not part of the contracted deliverables.
- ☐ Not all business functions will be available on initial implementation.
- ☐ Prototyping is being used to confirm that the system meets business requirements.

Licensed to Berend Post berend.post@it-university.nl

Question 2506

Which is MOST important when contracting an external party to perform a penetration test?

- ☐ Obtain approval from IT management.
- ☐ Define the project scope.
- ☐ Increase the frequency of log reviews.
- ☐ Provide network documentation.

Question 2507

Which of the following would effectively verify the originator of a transaction?

- ☐ Using a secret password between the originator and the receiver
- ☐ Encrypting the transaction with the receiver's public key
- ☐ Using a portable document format (PDF) to encapsulate transaction content
- ☐ Digitally signing the transaction with the source's private key

Question 2508

Which of the following would be the BEST way to address segregation of duties issues in an organization with budget constraints?

- ☐ Perform an independent audit.
- ☐ Rotate job duties periodically.
- ☐ Implement compensating controls.
- ☐ Hire temporary staff.

Question 2509

An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

- ☐ A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewall.
- ☐ Firewall policies are updated on the basis of changing requirements.
- ☐ inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
- ☐ The firewall is placed on top of the commercial operating system with all installation options.

Licensed to Berend Post berend.post@it-university.nl

Question 2510

What is an initial step in creating a proper firewall policy?

- ☐ Assigning access to users according to the principle of least privilege
- ☐ Determining appropriate firewall hardware and software
- ☐ Identifying network applications such as mail, web, or FTP servers
- ☐ Configuring firewall access rules

Question 2511

When segregation of duties concerns exists between IT support staff and end users, what would be suitable compensating control?

- ☐ Restricting physical access to computing equipment
- ☐ Reviewing transaction and application logs
- ☐ Performing background checks prior to hiring IT staff
- ☐ Locking user sessions after a specified period of inactivity

Question 2512

Attack amplifier is often being HEAVILY relied upon on by which of the following types of attack?

- ☐ Packet dropping
- ☐ ToS
- ☐ DDoS
- ☐ ATP
- ☐ Wiretapping
- ☐ None of the choices.

Question 2513

To protect a VoIP infrastructure against a denial-of-service (DoS) attack, it is MOST important to secure the:

- ☐ access control servers.
- ☐ session border controllers.
- ☐ backbone gateways.
- ☐ intrusion detection system (IDS).

Licensed to Berend Post berend.post@it-university.nl

Question 2514

An organization has made a strategic decision to split into separate operating entities to improve profitability. However, the IT infrastructure remains shared between the entities. Which of the following would BEST help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan?

- ☐ Increasing the frequency of risk-based IS audits for each business entity
- ☐ Revising IS audit plans to focus on IT changes introduced after the split
- ☐ Conducting an audit of newly introduced IT policies and procedures
- ☐ Developing a risk-based plan considering each entity's business processes

Question 2515

IT best practices for the availability and continuity of IT services should:

- ☐ minimize costs associated with disaster-resilient components.
- ☐ provide for sufficient capacity to meet the agreed upon demands of the business.
- ☐ provide reasonable assurance that agreed upon obligations to customers can be met.
- ☐ produce timely performance metric reports.

Question 2516

Which of the following would contribute MOST to an effective business continuity plan (BCP)?

- ☐ Document is circulated to all interested parties
- ☐ Planning involves all user departments
- ☐ Approval by senior management
- ☐ Audit by an external IS auditor

Question 2517

Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

- ☐ Overlapping controls
- ☐ Boundary controls
- ☐ Access controls
- ☐ Compensating controls

Licensed to Berend Post berend.post@it-university.nl

Question 2518

When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

- ☐ analysis.
- ☐ evaluation.
- ☐ preservation.
- ☐ disclosure.

Question 2519

If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do?

- ☐ Lack of IT documentation is not usually material to the controls tested in an IT audit.
- ☐ The auditor should at least document the informal standards and policies. Furthermore, the IS auditor should create formal documented policies to be implemented.
- ☐ The auditor should at least document the informal standards and policies, and test for a compliance. Furthermore, the IS auditor should recommend management that formal documented policies be developed and implemented.
- ☐ The auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should create formal documented policies to be implemented.

Question 2520

Which of the following hardware upgrades would BEST enhance the capability of a web server to accommodate a significant increase in web traffic?

- ☐ Multicore CPUs
- ☐ Solid state drives
- ☐ Additional flash memory
- ☐ Cloud architecture

Question 2521

John is the product manager for an information system. His product has undergone under security review by an IS auditor. John has decided to apply appropriate security controls to reduce the security risks suggested by an IS auditor. Which of the following technique is used by John to treat the identified risk provided by an IS auditor?

- ☐ Risk Mitigation
- ☐ Risk Acceptance
- ☐ Risk Avoidance
- ☐ Risk transfer

Licensed to Berend Post berend.post@it-university.nl

Question 2522

A decision support system (DSS):

- ☐ is aimed at solving highly structured problems.
- ☐ combines the use of models with nontraditional data access and retrieval functions.
- ☐ emphasizes flexibility in the decision making approach of users.
- ☐ supports only structured decision making tasks.

Question 2523

A large number of exceptions to an organization's information security standards have been granted after senior management approved a bring your own device (BYOD) program. To address this situation, it is MOSTimportant for the information security manage to:

- ☐ introduce strong authentication on devices
- ☐ reject new exception requests
- ☐ require authorization to wipe lost devices
- ☐ update the information security policy

Question 2524

IS audits should be selected through a risk analysis process to concentrate on:

- ☐ those areas of greatest risk and opportunity for improvements.
- ☐ those areas of least risk and opportunity for improvements.
- ☐ those areas of the greatest financial value.
- ☐ areas led by the key people of the organization.
- ☐ random events.
- ☐ irregular events.

Question 2525

During a database audit, an IS auditor noted frequent problems due to the growing size of the order tables. Which of the following is the BEST recommendation in this situation?

- ☐ Develop an archiving approach.
- ☐ Periodically delete completed orders.
- ☐ Build more table indices.
- ☐ Migrate to a different database management system.

Licensed to Berend Post berend.post@it-university.nl

Question 2526

Ideally, stress testing should be carried out in a:

- ☐ test environment using test data.
- ☐ production environment using live workloads.
- ☐ test environment using live workloads.
- ☐ production environment using test data.

Question 2527

Which of the following statements regarding an off-site information processing facility is TRUE?

- ☐ It should have the same amount of physical access restrictions as the primary processing site.
- ☐ It should be located in proximity to the originating site so that it can quickly be made operational.
- ☐ It should be easily identified from the outside so in the event of an emergency it can be easily found.
- ☐ Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

Question 2528

An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:

- ☐ EDI trading partner agreements.
- ☐ physical controls for terminals.
- ☐ authentication techniques for sending and receiving messages.
- ☐ program change control procedures.

Question 2529

Which of the following is the BEST physical security solution for granting and restricting access to individuals based on their unique access needs?

- ☐ Bolting door locks
- ☐ Cipher locks
- ☐ Closed-circuit television (CCTV)
- ☐ Electronic badge system

Licensed to Berend Post berend.post@it-university.nl

Question 2530

The technique used to ensure security in virtual private networks (VPNs) is:

- ☐ encapsulation.
- ☐ wrapping.
- ☐ transform.
- ☐ encryption

Question 2531

In determining the acceptable time period for the resumption of critical business processes:

- ☐ only downtime costs need to be considered.
- ☐ recovery operations should be analyzed.
- ☐ both downtime costs and recovery costs need to be evaluated.
- ☐ indirect downtime costs should be ignored.

Question 2532

An IS auditor selects a server for a penetration test that will be carried out by a technical specialist. Which of the following is MOST important?

- ☐ The tools used to conduct the test
- ☐ Certifications held by the IS auditor
- ☐ Permission from the data owner of the server
- ☐ An intrusion detection system (IDS) is enabled

Question 2533

Which of the following could provide an organization with the fastest resumption of processing following a disk failure?

- ☐ Server load balancing
- ☐ Mirroring
- ☐ Open database connectivity (ODBC) of the backup server
- ☐ Replication

Question 2534

To support an organization's goals, an IS department should have:

- ☐ a low-cost philosophy.
- ☐ long- and short-range plans.
- ☐ leading-edge technology.
- ☐ plans to acquire new hardware and software.

Licensed to Berend Post berend.post@it-university.nl

Question 2535

During an implementation review of a multiuser distributed application, an IS auditor finds minor weaknesses in three areas-the initial setting of parameters is improperly installed, weak passwords are being used and some vital reports are not being checked properly. While preparing the audit report, the IS auditor should:

- ☐ record the observations separately with the impact of each of them marked against each respective finding.
- ☐ advise the manager of probable risks without recording the observations, as the control weaknesses are minor ones.
- ☐ record the observations and the risk arising from the collective weaknesses.
- ☐ apprise the departmental heads concerned with each observation and properly document it in the report.

Question 2536

Which of the following append themselves to files as a protection against viruses?

- ☐ Behavior blockers
- ☐ Cyclical redundancy checkers (CRCs)
- ☐ Immunizers
- ☐ Active monitors

Question 2537

When implementing an application software package, which of the following presents the GREATEST risk?

- ☐ Uncontrolled multiple software versions
- ☐ Source programs that are not synchronized with object code
- ☐ incorrectly set parameters
- ☐ Programming errors.

Question 2538

Which of the following is the MOST important activity to undertake to avoid rework later in a project?

- ☐ Control review
- ☐ Risk assessment
- ☐ Acceptance testing
- ☐ Phase review

Licensed to Berend Post berend.post@it-university.nl

Question 2539

Which of the following method is recommended by security professional to PERMANENTLY erase sensitive data on magnetic media?

- ☐ Degaussing
- ☐ Overwrite every sector of magnetic media with pattern of 1's and 0's
- ☐ Format magnetic media
- ☐ Delete File allocation table

Question 2540

Which of the following should an IS auditor determine FIRST when evaluating additional hardware required to support the acquisition of a new accounting system?

- ☐ A training program has been developed to support the new accounting system.
- ☐ The supplier has experience supporting accounting systems.
- ☐ The hardware specified will be compliant with the current IT strategy.
- ☐ The hardware will be installed in a secure and environmentally controlled area.

Question 2541

Which of the following term related to network performance refers to the maximum rate that information can be transferred over a network?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Jitter

Question 2542

Which of the following is MOST likely to result from a business process reengineering (BPR) Project?

- ☐ An increased number of people using technology
- ☐ Significant cost saving, through a reduction the complexity of information technology
- ☐ A weaker organizational structures and less accountability
- ☐ Increased information protection (IP) risk will increase

Licensed to Berend Post berend.post@it-university.nl

Question 2543

Which of the following is a detective control?

- ☐ Procedures for authorizing transactions
- ☐ Echo checks in telecommunications
- ☐ A router rule restricting a service
- ☐ Programmed edit checks

Question 2544

What is the BEST action to prevent loss of data integrity or confidentiality in the case of an e-commerce application running on a LAN, processing electronic fund transfers (EFT) and orders?

- ☐ Using virtual private network (VPN) tunnels for data transfer
- ☐ Enabling data encryption within the application
- ☐ Auditing the access control to the network
- ☐ Logging all changes to access lists

Question 2545

Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?

- ☐ Overwriting the tapes
- ☐ initializing the tape labels
- ☐ Degaussing the tapes
- ☐ Erasing the tapes

Question 2546

The PRIMARY objective of Secure Sockets Layer (SSL) is to ensure:

- ☐ only the sender and receiver are able to encrypt/decrypt the data.
- ☐ the sender and receiver can authenticate their respective identities.
- ☐ the alteration of transmitted data can be detected.
- ☐ the ability to identify the sender by generating a one-time session key.

Question 2547

The reason a certification and accreditation process is performed on critical systems is to ensure that:

- ☐ security compliance has been technically evaluated.
- ☐ data have been encrypted and are ready to be stored.
- ☐ the systems have been tested to run on different platforms.
- ☐ the systems have followed the phases of a waterfall model.

Licensed to Berend Post berend.post@it-university.nl

Question 2548

Which of the following is the GREATEST risk associated with the lack of an effective data privacy program?

- ☐ Failure to prevent fraudulent transactions
- ☐ Inability to manage access to private or sensitive data
- ☐ Inability to obtain customer confidence
- ☐ Failure to comply with data-related regulations

Question 2549

When reviewing an implementation of a VoIP system over a corporate WAN, an IS auditor should expect to find:

- ☐ an integrated services digital network (ISDN) data link.
- ☐ traffic engineering.
- ☐ wired equivalent privacy (WEP) encryption of data.
- ☐ analog phone terminals.

Question 2550

Which of the following is the MOST significant risk an IS auditor should consider when reviewing a credit card company's application system?

- ☐ Data privacy
- ☐ Processing times
- ☐ System availability
- ☐ Credit ratings

Question 2551

Which of the following is the PRIMARY benefit of implementing configuration management for IT?

- ☐ It helps audit in verifying IT conformance to business requirements.
- ☐ It establishes the dependency of application systems with various IT assets.
- ☐ It provides visibility to the overall function and technical attributes of IT assets.
- ☐ It helps automate change and release management processes in IT.

Licensed to Berend Post berend.post@it-university.nl

Question 2552

The risk that the IS auditor will not find an error that has occurred is identified by which of the following terms?

- ☐ Control
- ☐ Prevention
- ☐ Inherent
- ☐ Detection

Question 2553

Which of the following security control is intended to bring environment back to regular operation?

- ☐ Deterrent
- ☐ Preventive
- ☐ Corrective
- ☐ Recovery

Question 2554

Which of the following layer from an enterprise data flow architecture captures all data of interest to an organization and organize it to assist in reporting and analysis?

- ☐ Desktop access layer
- ☐ Data preparation layer
- ☐ Core data warehouse
- ☐ Data access layer

Question 2555

Which of the following is the MOST important incident management consideration for an organization subscribing to a cloud service?

- ☐ Decision on the classification of cloud-hosted data
- ☐ Expertise of personnel providing incident response
- ☐ Implementation of a SIEM in the organization
- ☐ An agreement on the definition of a security incident

Licensed to Berend Post berend.post@it-university.nl

Question 2556

Which of the following is MOST important for an IS auditor to verify after finding repeated unauthorized access attempts were recorded on a security report?

- ☐ Password reset requests have been confirmed as legitimate
- ☐ There is evidence that the incident was investigated
- ☐ System configuration changes are properly tracked
- ☐ A comprehensive access policy has been established

Question 2557

An organization is implementing the use of mobile devices that will connect to sensitive corporate applications. Which of the following is the BEST recommendation to mitigate risk of data leakage?

- ☐ Remote data wipe
- ☐ GPS tracking software
- ☐ Encrypted RFID tags
- ☐ Data encryption

Question 2558

Neural networks are effective in detecting fraud because they can:

- ☐ discover new trends since they are inherently linear.
- ☐ solve problems where large and general sets of training data are not obtainable.
- ☐ attack problems that require consideration of a large number of input variables.
- ☐ make assumptions about the shape of any curve relating variables to the output.

Question 2559

The PRIMARY reason an IS department should analyze past incidents and problems is to:

- ☐ determine if all incidents and problems are reported.
- ☐ assign responsibility for problems.
- ☐ assess help desk performance.
- ☐ identify the causes of recurring incidents and problems.

Question 2560

Which of the following would be considered the BEST compensating control to use when an emergency process, rather than the established control procedures, is used for database changes?

- ☐ Using an emergency user account with the access to make changes to the database
- ☐ Using the administrator's own account to make out-of-hours changes
- ☐ Logging detailed before-and-after images for later review by the administrator
- ☐ Logging user's ID and change details for later review by the administrator

Licensed to Berend Post berend.post@it-university.nl

Question 2561

Which of the following would an IS auditor consider a weakness when performing an audit of an organization that uses a public key infrastructure with digital certificates for its business-to-consumer transactions via the internet?

- ☐ Customers are widely dispersed geographically, but the certificate authorities are not.
- ☐ Customers can make their transactions from any computer or mobile device.
- ☐ The certificate authority has several data processing subcenters to administer certificates.
- ☐ The organization is the owner of the certificate authority.

Question 2562

Which of the following is a good time frame for making changes to passwords?

- ☐ every 180 to 365 days
- ☐ every 30 to 45 days
- ☐ every 10 to 20 days
- ☐ every 90 to 120 days
- ☐ None of the choices.

Question 2563

The potential for unauthorized system access by way of terminals or workstations within an organization's facility is increased when:

- ☐ connecting points are available in the facility to connect laptops to the network.
- ☐ users take precautions to keep their passwords confidential.
- ☐ terminals with password protection are located in insecure locations.
- ☐ terminals are located within the facility in small clusters under the supervision of an administrator.

Question 2564

Which of the following would MOST effectively aid executive management in achieving IT and business alignment?

- ☐ Risk assessment
- ☐ Value delivery assessment
- ☐ Balanced scorecard
- ☐ Performance measurement

Licensed to Berend Post berend.post@it-university.nl

Question 2565

Which of the following BEST enables effective closure of noncompliance issues?

- ☐ Insuring against the risk
- ☐ Performing control self-assessments
- ☐ Capturing issues in a risk register
- ☐ Executing an approved mitigation plan

Question 2566

When assessing the design of network monitoring controls, an IS auditor should FIRST review network:

- ☐ topology diagrams.
- ☐ bandwidth usage.
- ☐ traffic analysis reports.
- ☐ bottleneck locations.

Question 2567

Adding security requirements late in the software development life cycle would MOST likely result in:

- ☐ cost savings
- ☐ clearer understanding of requirements
- ☐ operational efficiency
- ☐ compensating controls

Question 2568

At a hospital, medical personal carry handheld computers which contain patient health data. These handheld computers are synchronized with PCs which transfer data from a hospital database. Which of the following would be of the most importance?

- ☐ The handheld computers are properly protected to prevent loss of data confidentiality, in case of theft or loss.
- ☐ The employee who deletes temporary files from the local PC, after usage, is authorized to maintain PCs.
- ☐ Timely synchronization is ensured by policies and procedures.
- ☐ The usage of the handheld computers is allowed by the hospital policy.

Licensed to Berend Post berend.post@it-university.nl

Question 2569

Who is ultimately responsible for providing requirement specifications to the software- development team?

- ☐ The project sponsor
- ☐ The project members
- ☐ The project leader
- ☐ The project steering committee

Question 2570

Which key is used by the sender of a message to create a digital signature for the message being sent?

- ☐ Sender's public key
- ☐ Sender's private key
- ☐ Receiver's public key
- ☐ Receiver's private key

Question 2571

In a multinational organization, local security regulations should be implemented over global security policy because:

- ☐ global security policies include unnecessary controls for local businesses
- ☐ business objectives are defined by local business unit managers
- ☐ requirements of local regulations take precedence
- ☐ deploying awareness of local regulations is more practical than of global policy

Question 2572

What increases encryption overhead and cost the most?

- ☐ A long symmetric encryption key
- ☐ A long asymmetric encryption key
- ☐ A long Advance Encryption Standard (AES) key
- ☐ A long Data Encryption Standard (DES) key

Licensed to Berend Post berend.post@it-university.nl

Question 2573

An IS auditor inspected a windowless room containing phone switching and networking equipment and documentation binders. The room was equipped with two handheld fire extinguishers-one filled with CO2, the other filled with halon. Which of the following should be given the HIGHEST priority in the auditor's report?

- ☐ The halon extinguisher should be removed because halon has a negative impact on the atmospheric ozone layer.
- ☐ Both fire suppression systems present a risk of suffocation when used in a closed room.
- ☐ The CO2 extinguisher should be removed, because CO2 is ineffective for suppressing fires involving solid combustibles (paper).
- ☐ The documentation binders should be removed from the equipment room to reduce potential risks.

Question 2574

Implementing which of the following would BEST address issues relating to the aging of IT systems?

- ☐ IT project management
- ☐ Release management
- ☐ Application portfolio management
- ☐ Configuration management

Question 2575

During a security audit, an IS auditor is tasked with reviewing log entries obtained from an enterprise intrusion prevention system (IPS). Which type of risk would be associated with the potential for the auditor to miss a sequence of logged events that could indicate an error in the IPS configuration?

- ☐ Inherent risk
- ☐ Sampling risk
- ☐ Control risk
- ☐ Detection risk

Question 2576

Which of the following audit procedures would be MOST conclusive in evaluating the effectiveness of an e-commerce application system's edit routine?

- ☐ Interviews with knowledgeable users
- ☐ Use of test transactions
- ☐ Review of source code
- ☐ Review of program documentation

Licensed to Berend Post berend.post@it-university.nl

Question 2577

Which of the following device in Frame Relay WAN technique is a service provider device that does the actual data transmission and switching in the frame relay cloud?

- ☐ DTE
- ☐ DCE
- ☐ DME
- ☐ DLE

Question 2578

Key verification is one of the best controls for ensuring that:

- ☐ Data is entered correctly
- ☐ Only authorized cryptographic keys are used
- ☐ Input is authorized
- ☐ Database indexing is performed properly

Question 2579

Which of the following is the MAIN purpose of an information security management system?

- ☐ To enhance the impact of reports used to monitor information security incidents
- ☐ To reduce the frequency and impact of information security incidents
- ☐ To identify and eliminate the root causes of information security incidents
- ☐ To keep information security policies and procedures up-to-date

Question 2580

When replacing a critical software application, which of the following provides for the LOWEST risk of interruption to business processes?

- ☐ Parallel implementation
- ☐ Pilot implementation
- ☐ Incremental implementation
- ☐ Big-bang implementation

Licensed to Berend Post berend.post@it-university.nl

Question 2581

An IS auditor is reviewing the physical security measures of an organization. Regarding the access card system, the IS auditor should be MOST concerned that:

- ☐ nonpersonalized access cards are given to the cleaning staff, who use a sign-in sheet but show no proof of identity.
- ☐ access cards are not labeled with the organization's name and address to facilitate easy return of a lost card.
- ☐ card issuance and rights administration for the cards are done by different departments, causing unnecessary lead time for new cards.
- ☐ the computer system used for programming the cards can only be replaced after three weeks in the event of a system failure.

Question 2582

A small organization is experiencing rapid growth and plans to create a new information security policy. Which of the following is MOST relevant to creating the policy?

- ☐ Industry standards
- ☐ The business impact analysis
- ☐ The business objectives
- ☐ Previous audit recommendations

Question 2583

A lower recovery time objective (RTO) results in:

- ☐ higher disaster tolerance.
- ☐ higher cost.
- ☐ wider interruption windows.
- ☐ more permissive data loss.

Question 2584

Which of the following would be an information security manager's PRIMARY challenge when deploying a bring your own device (BYOD) mobile program in an enterprise?

- ☐ End user acceptance
- ☐ Mobile application control
- ☐ Configuration management
- ☐ Disparate device security

Licensed to Berend Post berend.post@it-university.nl

Question 2585

Which of the following technique is NOT used by a preacher against a Private Branch Exchange (PBX)?

- ☐ Eavesdropping
- ☐ Illegal call forwarding
- ☐ Forwarding a user to an unused or disabled number
- ☐ SYN Flood

Question 2586

"Under the concept of ""defense in depth"", subsystems should be designed to:"

- ☐ """fail insecure"""
- ☐ """fail secure"""
- ☐ """react to attack"""
- ☐ """react to failure"""
- ☐ None of the choices.

Question 2587

An IS audit manager has been asked to perform a quality review on an audit that the same manager also supervised. Which of the following is the manager's BEST response to this situation?

- ☐ Notify the audit committee of the situation.
- ☐ Escalate the situation to senior audit leadership.
- ☐ Determine whether audit evidence supports audit conclusions.
- ☐ Discuss with the audit team to understand how conclusions were reached.

Question 2588

A retirement system verifies that the field for employee status has either a value of A (for active) or R (for retired). This is an example of which type of check?

- ☐ Validity
- ☐ Existence
- ☐ Limit
- ☐ Completeness

Licensed to Berend Post berend.post@it-university.nl

Question 2589

A company requires that all program change requests (PCRs) be approved and all modifications be automatically logged. Which of the following IS audit procedures will BEST determine whether unauthorized changes have been made to production programs?

- ☐ Review a sample of PCRs for proper approval throughout the program change process.
- ☐ Trace a sample of program changes from the log to completed PCR forms.
- ☐ Use source code comparison software to determine whether any changes have been made to a sample of programs since the last audit date.
- ☐ Trace a sample of complete PCR forms to the log of all program changes.

Question 2590

The network of an organization has been the victim of several intruders' attacks. Which of the following measures would allow for the early detection of such incidents?

- ☐ Antivirus software
- ☐ Hardening the servers
- ☐ Screening routers
- ☐ Honeypots

Question 2591

When reviewing a newly implemented quality management system (QMS), which of the following should be the IS auditor's PRIMARY concern?

- ☐ The QMS benefit measures were not included in the business case.
- ☐ The QMS testing methodology is not clearly documented.
- ☐ The QMS post-implementation review (PIR) has not been finalized.
- ☐ The QMS is not mapped to some core business processes.

Question 2592

Codes from exploit programs are frequently reused in:

- ☐ trojan horses only.
- ☐ computer viruses only.
- ☐ OS patchers.
- ☐ eavedroppers.
- ☐ trojan horses and computer viruses.
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 2593

An organization that has suffered a cyber attack is performing a forensic analysis of the affected users' computers. Which of the following should be of GREATEST concern for the IS auditor reviewing this process?

- ☐ The chain of custody has not been documented.
- ☐ The legal department has not been engaged.
- ☐ An imagining process was used to obtain a copy of the data from each computer.
- ☐ Audit was only involved during extraction of the information.

Question 2594

Which of the following metrics would BEST measure the agility of an organization's IT function?

- ☐ Average time to turn strategic IT objectives into an agreed upon and approved initiative
- ☐ Average number of learning and training hours per IT staff member
- ☐ Frequency of security assessments against the most recent standards and guidelines
- ☐ Percentage of staff with sufficient IT-related skills for the competency required of their roles.

Question 2595

Which of the following cloud deployment model operates solely for an organization?

- ☐ Private Cloud
- ☐ Community Cloud
- ☐ Public Cloud
- ☐ Hybrid Cloud

Question 2596

Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

- ☐ Failing to perform user acceptance testing
- ☐ Lack of user training for the new system
- ☐ Lack of software documentation and run manuals
- ☐ Insufficient unit, module, and systems testing

Licensed to Berend Post berend.post@it-university.nl

Question 2597

Which of the following would be the PRIMARY benefit of replacing physical keys with an electronic entry system for a data center?

- ☐ Creates an audit trail
- ☐ Enables data mining
- ☐ Ensures compliance
- ☐ Reduces cost

Question 2598

Which of the following firewall technologies involves examining the header of every packet of data traveling between the Internet and the corporate network without examining the previous packets?

- ☐ Proxy servers
- ☐ Bastion host
- ☐ Stateful filtering
- ☐ Stateless filtering

Question 2599

Which of the following exposures could be caused by a line grabbing technique?

- ☐ Unauthorized data access
- ☐ Excessive CPU cycle usage
- ☐ Lockout of terminal polling
- ☐ Multiplexor control dysfunction

Question 2600

Which of the following is the BEST key performance indicator (KPI) for determining how well the IT policy is aligned to the business requirements?

- ☐ Number of approved exceptions to the policy
- ☐ Total cost of policy breaches
- ☐ Total cost to support the policy
- ☐ Number of inquiries regarding the policy

Licensed to Berend Post berend.post@it-university.nl

Question 2601

Since data storage of a critical business application is on a redundant array of inexpensive disks (RAID), backups are not considered essential. The IS auditor should recommend proper backups because RAID:

- ☐ relies on proper maintenance.
- ☐ cannot offer protection against disk corruption.
- ☐ cannot recover from a natural disaster.
- ☐ disks cannot be hot-swapped for quick recovery.

Question 2602

An organization is MOST at risk from a new worm being introduced through the intranet when:

- ☐ executable code is run from inside the firewall
- ☐ system software does not undergo integrity checks
- ☐ hosts have static IP addresses
- ☐ desktop virus definition files are not up to date

Question 2603

To ensure compliance with a security policy requiring that passwords be a combination of letters and numbers, an IS auditor should recommend that:

- ☐ the company policy be changed.
- ☐ passwords are periodically changed.
- ☐ an automated password management tool be used.
- ☐ security awareness training is delivered.

Question 2604

Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?

- ☐ Spool
- ☐ Cluster controller
- ☐ Protocol converter
- ☐ Front end processor

Licensed to Berend Post berend.post@it-university.nl

Question 2605

To address the issue that performance pressures on IT may conflict with information security controls, it is MOST important that:

- ☐ the security policy is changed to accommodate IT performance pressure
- ☐ noncompliance issues are reported senior management
- ☐ senior management provides guidance and dispute resolution
- ☐ information security management understands business performance issues

Question 2606

IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?

- ☐ True
- ☐ False

Question 2607

An organization has developed mature risk management practices that are followed across all departments. What is the MOST effective way for the audit team to leverage this risk management maturity?

- ☐ Facilitating audit risk identification and evaluation workshops
- ☐ Implementing risk responses on management's behalf
- ☐ Providing assurances to management regarding risk
- ☐ Integrating the risk register for audit planning purposes

Question 2608

Which of the following would provide the STRONGEST indication that senior management commitment to information security is lacking within an organization?

- ☐ Inconsistent enforcement of information security policies
- ☐ A reduction in information security investment
- ☐ A high of information security risk acceptance
- ☐ The information security manager reports to the chief risk officer

Licensed to Berend Post berend.post@it-university.nl

Question 2609

Which of the following approaches would utilize data analytics to facilitate the testing of a new account creation process?

- ☐ Review the business requirements document for date of birth field requirements.
- ☐ Review new account applications submitted in the past month for invalid dates of birth.
- ☐ Evaluate configuration settings for the date of birth field requirements.
- ☐ Attempt to submit new account applications with invalid dates of birth.

Question 2610

An organization has implemented a control to help ensure databases containing personal information will not be updated with online transactions that are incomplete due to connectivity issues. Which of the following information attributes is PRIMARILY addressed by this control?

- ☐ Integrity
- ☐ Confidentiality
- ☐ Availability
- ☐ Compliance

Question 2611

Which of the following should be done FIRSTwhen handling multiple confirmed incidents raised at the same time?

- ☐ Categorize incidents by the value of the affected asset.
- ☐ Inform senior management.
- ☐ Update the business impact assessment.
- ☐ Activate the business continuity plan.

Question 2612

When reviewing backup policies, an IS auditor MUST verify that backup intervals of critical systems do not exceed which of the following?

- ☐ Recovery point objective (RPO)
- ☐ Recovery time objective (RTO)
- ☐ Service level objective (SLO)
- ☐ Maximum acceptable outage (MAO)

Licensed to Berend Post berend.post@it-university.nl

Question 2613

What is the PRIMARY benefit of prototyping as a method of system development?

- ☐ Reduces the need for testing.
- ☐ Minimizes the time the IS auditor has to review the system.
- ☐ Increases the likelihood of user satisfaction.
- ☐ Eliminates the need for documentation.

Question 2614

Which of the following audit assess accuracy of financial reporting?

- ☐ Compliance Audit
- ☐ Financial Audit
- ☐ Operational Audit
- ☐ Forensic audit

Question 2615

During a network security review, the system log indicates an unusually high number of unsuccessful login attempts. Which of the following sampling techniques is MOST appropriate for selecting a sample of user IDs for further investigation?

- ☐ Stratified
- ☐ Attribute
- ☐ Monetary unit
- ☐ Variable

Question 2616

Which of the following is the MOST effective control over visitor access to a data center?

- ☐ Visitors are escorted.
- ☐ Visitor badges are required.
- ☐ Visitors sign in.
- ☐ Visitors are spot-checked by operators.

Question 2617

An IS auditor finds that one employee has unauthorized access to confidential data. The IS auditor's BEST recommendation should be to:

- ☐ reclassify the data to a lower level of confidentiality.
- ☐ recommend corrective actions to be taken by the security administrator.
- ☐ implement a strong password schema for users.
- ☐ require the business owner to conduct regular access reviews.

Licensed to Berend Post berend.post@it-university.nl

Question 2618

Following a risk assessment, new countermeasures have been approved by management. Which of the following should be performed NEXT?

- ☐ Schedule the target end date for implementation activities.
- ☐ Budget the total cost of implementation activities.
- ☐ Develop an implementation strategy.
- ☐ Calculate the residual risk for each countermeasure.

Question 2619

The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

- ☐ Inherent
- ☐ Detection
- ☐ Control
- ☐ Business

Question 2620

Which of the following best characterizes “worms”?

- ☐ Malicious programs that can run independently and can propagate without the aid of a carrier program such as email.
- ☐ Programming code errors that cause a program to repeatedly dump data
- ☐ Malicious programs that require the aid of a carrier program such as email
- ☐ Malicious programs that masquerade as common applications such as screensavers or macro- enabled Word documents

Question 2621

What are used as the framework for developing logical access controls?

- ☐ Information systems security policies
- ☐ Organizational security policies
- ☐ Access Control Lists (ACL)
- ☐ Organizational charts for identifying roles and responsibilities

Question 2622

Which of the following security risks can be reduced by a properly configured network firewall?

- ☐ Insider attacks
- ☐ SQL injection attacks
- ☐ Denial of service (DoS) attacks
- ☐ Phishing attacks

Licensed to Berend Post berend.post@it-university.nl

Question 2623

As part of a mergers and acquisitions activity, an acquiring organization wants to consolidate data and system from the organization being acquired into existing systems. To ensure the data is relevant, the acquiring organization should:

- ☐ obtain data quality software.
- ☐ define data quality requirements based on business needs.
- ☐ automate the process of data collection and cleaning.
- ☐ implement a data warehouse solution.

Question 2624

Which of the following recovery strategies is MOST appropriate for a business having multiple offices within a region and a limited recovery budget?

- ☐ A hot site maintained by the business
- ☐ A commercial cold site
- ☐ A reciprocal arrangement between its offices
- ☐ A third-party hot site

Question 2625

Which of the following are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem?

- ☐ Expert systems
- ☐ Neural networks
- ☐ Integrated synchronized systems
- ☐ Multitasking applications

Question 2626

When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:

- ☐ not be concerned since there may be other compensating controls to mitigate the risks.
- ☐ ensure that overrides are automatically logged and subject to review.
- ☐ verify whether all such overrides are referred to senior management for approval.
- ☐ recommend that overrides not be permitted.

Licensed to Berend Post berend.post@it-university.nl

Question 2627

Which of the following is the PRIMARY advantage of having an established information security governance framework in place when an organization is adopting emerging technologies?

- ☐ An emerging technologies strategy would be in place
- ☐ A cost-benefit analysis process would be easier to perform
- ☐ An effective security risk management process is established
- ☐ End-user acceptance of emerging technologies has been established

Question 2628

Assessing IT risks is BEST achieved by:

- ☐ evaluating threats associated with existing IT assets and IT projects.
- ☐ using the firm's past actual loss experience to determine current exposure.
- ☐ reviewing published loss statistics from comparable organizations.
- ☐ reviewing IT control weaknesses identified in audit reports.

Question 2629

The operations team of an organization has reported an IS security attack. Which of the following should be the NEXT step for the security incident response team?

- ☐ Document lessons learned.
- ☐ Prioritize resources for corrective action.
- ☐ Perform a damage assessment.
- ☐ Report results to management.

Question 2630

Which of the following techniques would BEST help an IS auditor gain reasonable assurance that a project can meet its target date?

- ☐ Estimation of the actual end date based on the completion percentages and estimated time to complete, taken from status reports
- ☐ Confirmation of the target date based on interviews with experienced managers and staff involved in the completion of the project deliverables.
- ☐ Extrapolation of the overall end date based on completed work packages and current resources
- ☐ Calculation of the expected end date based on current resources and remaining available project budget

Licensed to Berend Post berend.post@it-university.nl

Question 2631

Following best practices, formal plans for implementation of new information systems are developed during the:

- ☐ development phase.
- ☐ design phase.
- ☐ testing phase.
- ☐ deployment phase.

Question 2632

An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:

- ☐ report that the control is operating effectively since deactivation happens within the time frame stated in the IS policy.
- ☐ verify that user access rights have been granted on a need-to-have basis.
- ☐ recommend changes to the IS policy to ensure deactivation of user IDs upon termination.
- ☐ recommend that activity logs of terminated users be reviewed on a regular basis.

Question 2633

During which phase of an incident response process should corrective actions to the response procedure be considered and implemented?

- ☐ Eradication
- ☐ Identification
- ☐ Review
- ☐ Containment

Question 2634

While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern should be that the:

- ☐ requirement for protecting confidentiality of information could be compromised.
- ☐ contract may be terminated because prior permission from the outsourcer was not obtained.
- ☐ other service provider to whom work has been outsourced is not subject to audit.
- ☐ outsourcer will approach the other service provider directly for further work.

Licensed to Berend Post berend.post@it-university.nl

Question 2635

Which of the following should be a concern to an IS auditor reviewing a wireless network?

- ☐ 128-bit static-key WEP (Wired Equivalent Privacy) encryption is enabled.
- ☐ SSID (Service Set IDentifier) broadcasting has been enabled.
- ☐ Antivirus software has been installed in all wireless clients.
- ☐ MAC (Media Access Control) access control filtering has been deployed.

Question 2636

An organization currently using tape backups takes one full backup weekly and incremental backups daily. They recently augmented their tape backup procedures with a backup-to- disk solution. This is appropriate because:

- ☐ fast synthetic backups for offsite storage are supported.
- ☐ backup to disk is always significantly faster than backup to tape.
- ☐ tape libraries are no longer needed.
- ☐ data storage on disks is more reliable than on tapes.

Question 2637

A user of a telephone banking system has forgotten his personal identification number (PIN). After the user has been authenticated, the BEST method of issuing a new PIN is to have:

- ☐ the user enter a new PIN twice.
- ☐ banking personnel verbally assign a new PIN.
- ☐ a randomly generated PIN communicated by banking personnel.
- ☐ banking personnel assign the user a new PIN via email.

Question 2638

The development of an IS security policy is ultimately the responsibility of the:

- ☐ IS department.
- ☐ security committee.
- ☐ security administrator.
- ☐ board of directors.

Licensed to Berend Post berend.post@it-university.nl

Question 2639

During an external assessment of network vulnerability, which of the following activities should be performed FIRST?

- ☐ Collect network information
- ☐ Implement an intrusion detection system (IDS)
- ☐ Monitor the network
- ☐ Review policies

Question 2640

Is it appropriate for an IS auditor from a company that is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?

- ☐ Yes, because an IS auditor will evaluate the adequacy of the service bureau's plan and assist their company in implementing a complementary plan.
- ☐ Yes, because based on the plan, an IS auditor will evaluate the financial stability of the service bureau and its ability to fulfill the contract.
- ☐ No, because the backup to be provided should be specified adequately in the contract.
- ☐ No, because the service bureau's business continuity plan is proprietary information.

Question 2641

What should regression testing use to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors?

- ☐ Contrived data
- ☐ Independently created data
- ☐ Live data
- ☐ Data from previous tests

Question 2642

Which of the following transmission media is MOST difficult to tap?

- ☐ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Radio System

Licensed to Berend Post berend.post@it-university.nl

Question 2643

Which of the following would be of MOST concern to an IS auditor reviewing a virtual private network (VPN) implementation? Computers on the network that are located:

- ☐ on the enterprise's internal network.
- ☐ at the backup site.
- ☐ in employees' homes.
- ☐ at the enterprise's remote offices.

Question 2644

In an organization where IT is critical to its business strategy and where there is a high level of operational dependence on IT, senior management commitment to security is BEST demonstrated by the:

- ☐ reporting line of the chief information security officer (CISO).
- ☐ segregation of duties policy.
- ☐ existence of an IT steering committee.
- ☐ size of the IT security function.

Question 2645

To enable the alignment of IT staff development plans with IT strategy, which of the following should be done FIRST?

- ☐ Include strategic objectives in IT staff performance objectives.
- ☐ Review IT staff job descriptions for alignment.
- ☐ Identify required IT skill sets that support key business processes.
- ☐ Develop quarterly training for each IT staff member.

Question 2646

An organization is in the process of deciding whether to allow a bring your own device (BYOD) program. If approved, which of the following should be the FIRST control required before implementation?

- ☐ Device baseline configurations
- ☐ Device registration
- ☐ An acceptable use policy
- ☐ An awareness program

Licensed to Berend Post berend.post@it-university.nl

Question 2647

An organization's disposal policy emphasizes obtaining maximum value for surplus IT media. The IS auditor should obtain assurance that:

- ☐ the media is returned to the vendor for credit
- ☐ any existing data is removed before disposal
- ☐ identification labels are removed
- ☐ the media is recycled to other groups within the organization

Question 2648

Which of the following control is intended to discourage a potential attacker?

- ☐ Deterrent
- ☐ Preventive
- ☐ Corrective
- ☐ Recovery

Question 2649

Which of the following malware technical fool's malware by appending section of themselves to files – somewhat in the same way that file malware appends themselves?

- ☐ Scanners
- ☐ Active Monitors
- ☐ Immunizer
- ☐ Behavior blocker

Question 2650

The advantage of a bottom-up approach to the development of organizational policies is that the policies:

- ☐ are developed for the organization as a whole
- ☐ are more likely to be derived as a result of a risk assessment.
- ☐ will not conflict with overall corporate policy.
- ☐ ensure consistency across the organization.

Licensed to Berend Post berend.post@it-university.nl

Question 2651

A company is implementing a dynamic host configuration protocol (DHCP). Given that the following conditions exist, which represents the GREATEST concern?

- ☐ Most employees use laptops.
- ☐ A packet filtering firewall is used.
- ☐ The IP address space is smaller than the number of PCs.
- ☐ Access to a network port is not restricted.

Question 2652

Which of the following functionality is NOT supported by SSL protocol?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Authentication
- ☐ Availability

Question 2653

An IS auditor performing an independent classification of systems should consider a situation where functions could be performed manually at a tolerable cost for an extended period of time as:

- ☐ critical
- ☐ vital.
- ☐ sensitive.
- ☐ noncritical.

Question 2654

While executing follow-up activities, an IS auditor is concerned that management has implemented corrective actions that are different from those originally discussed and agreed with the audit function. In order to resolve the situation, the IS auditor's BEST course of action would be to:

- ☐ determine whether the alternative controls sufficiently mitigate the risk and record the results.
- ☐ reject the alternative controls and re-prioritize the original issue as high risk.
- ☐ postpone follow-up activities and escalate the alternative controls to senior audit management.
- ☐ schedule another audit due to the implementation of alternative controls.

Licensed to Berend Post berend.post@it-university.nl

Question 2655

Users are issued security tokens to be used in combination with a PIN to access the corporate virtual private network (VPN). Regarding the PIN, what is the MOST important rule to be included in a security policy?

- ☐ Users should not leave tokens where they could be stolen
- ☐ Users must never keep the token in the same bag as their laptop computer
- ☐ Users should select a PIN that is completely random, with no repeating digits
- ☐ Users should never write down their PIN

Question 2656

_____ should be implemented as early as data preparation to support data integrity at the earliest point possible.

- ☐ Control totals
- ☐ Authentication controls
- ☐ Parity bits
- ☐ Authorization controls

Question 2657

Which of the following controls would BEST decrease the exposure if a password is compromised?

- ☐ Passwords are masked.
- ☐ Passwords are encrypted.
- ☐ Passwords have format restrictions.
- ☐ Password changes are forced periodically.

Question 2658

Which of the following components is responsible for the collection of data in an intrusion detection system (IDS)?

- ☐ Analyzer
- ☐ Administration console
- ☐ User interface
- ☐ Sensor

Licensed to Berend Post berend.post@it-university.nl

Question 2659

Based on the guidance of internal audit, an IT steering committee is considering the use of a balanced scorecard to evaluate its project management process. Which of the following is the GREATEST advantage to using this approach?

- ☐ Project schedule and budget management will improve.
- ☐ Performance is measured from different perspectives.
- ☐ Information is provided in a consistent and timely manner.
- ☐ Project will be prioritized based on value.

Question 2660

Which of the following functions is performed by a virtual private network (VPN)?

- ☐ Hiding information from sniffers on the net
- ☐ Enforcing security policies
- ☐ Detecting misuse or mistakes
- ☐ Regulating access

Question 2661

A company is using a software developer for a project. At which of the following points should the software quality assurance (QA) plan be developed?

- ☐ As part of software definition
- ☐ During the feasibility phase
- ☐ Prior to acceptance testing
- ☐ As part of the design phase

Question 2662

To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

- ☐ avoidance
- ☐ transference
- ☐ mitigation
- ☐ acceptance

Licensed to Berend Post berend.post@it-university.nl

Question 2663

An organization is using symmetric encryption. Which of the following would be a valid reason for moving to asymmetric encryption? Symmetric encryption:

- ☐ provides authenticity.
- ☐ is faster than asymmetric encryption.
- ☐ can cause key management to be difficult.
- ☐ requires a relatively simple algorithm.

Question 2664

Which of the following should be reviewed FIRST when planning an IS audit?

- ☐ Recent financial information
- ☐ Annual business unit budget
- ☐ IS audit standards
- ☐ The business environment

Question 2665

Which of the following is the MOST effective means of helping management and the IT strategy committee to monitor IT performance?

- ☐ End-user satisfaction surveys
- ☐ Gap analysis
- ☐ Measurement of service levels against metrics
- ☐ Infrastructure monitoring reports

Question 2666

During an audit of identity and access management, an IS auditor finds that the engagement audit plan does not include the testing of controls that regulate access by third parties. Which of the following would be the auditor's BEST course of action?

- ☐ Plan to test these controls in another audit.
- ☐ Escalate the deficiency to audit management.
- ☐ Add testing of third-party access controls to the scope of the audit.
- ☐ Determine whether the risk has been identified in the planning documents.

Licensed to Berend Post berend.post@it-university.nl

Question 2667

What is the MOST important business concern when an organization is about to migrate a mission-critical application to a virtual environment?

- ☐ The organization's experience with virtual applications
- ☐ Adequacy of the fallback procedures
- ☐ Confidentiality of network traffic
- ☐ Adequacy of the virtual architecture

Question 2668

Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

- ☐ User management coordination does not exist.
- ☐ Specific user accountability cannot be established.
- ☐ Unauthorized users may have access to originate, modify or delete data.
- ☐ Audit recommendations may not be implemented.

Question 2669

Which of the following ACID property in DBMS ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other?

- ☐ Atomicity
- ☐ Consistency
- ☐ Isolation
- ☐ Durability

Question 2670

Establishing data ownership is an important first step for which of the following processes?

- ☐ Assigning user access privileges
- ☐ Developing organizational security policies
- ☐ Creating roles and responsibilities
- ☐ Classifying data

Licensed to Berend Post berend.post@it-university.nl

Question 2671

While conducting a test of a business continuity plan, which of the following is the MOST important consideration?

- ☐ The test simulates actual prime-time processing conditions.
- ☐ The test is scheduled to reduce operational impact.
- ☐ The test involves IT members in the test process.
- ☐ The test addresses the critical components.

Question 2672

Which of the following audit techniques is MOST appropriate for verifying application program controls?

- ☐ Statistical sampling
- ☐ Code review
- ☐ Confirmation of accounts
- ☐ Use of test data

Question 2673

Which of the following types of spyware was originally designed for determining the sources of error or for measuring staff productivity?

- ☐ Keywords logging
- ☐ Keystroke logging
- ☐ Directory logging
- ☐ Password logging
- ☐ None of the choices.

Question 2674

Which of the following would BEST detect that a distributed-denial-of-service attack (DDoS) is occurring?

- ☐ Server crashes
- ☐ Automated monitoring of logs
- ☐ Penetration testing
- ☐ Customer service complaints

Licensed to Berend Post berend.post@it-university.nl

Question 2675

The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

- ☐ confirm that the auditors did not overlook any important issues.
- ☐ gain agreement on the findings.
- ☐ receive feedback on the adequacy of the audit procedures.
- ☐ test the structure of the final presentation.

Question 2676

An organization is considering whether to allow employees to use personal computing devices for business purposes. To BEST facilitate senior management's decision, the information security manager should:

- ☐ perform a cost-benefit analysis
- ☐ map the strategy to business objectives
- ☐ conduct a risk assessment
- ☐ develop a business case

Question 2677

An application development team is also promoting changes to production for a critical financial application. Which of the following would be the BEST control to reduce the associated risk?

- ☐ Implementing a change management code review
- ☐ Implementing a peer review process
- ☐ Performing periodic audits
- ☐ Submitting change logs to the business manager for review

Question 2678

The feature of a digital signature that ensures the sender cannot later deny generating and sending the message is called:

- ☐ data integrity.
- ☐ authentication.
- ☐ non repudiation.
- ☐ replay protection.

Licensed to Berend Post berend.post@it-university.nl

Question 2679

The GREATEST risk when end users have access to a database at its system level, instead of through the application, is that the users can:

- ☐ make unauthorized changes to the database directly, without an audit trail.
- ☐ make use of a system query language (SQL) to access information.
- ☐ remotely access the database.
- ☐ update data without authentication.

Question 2680

What is the PRIMARY reason for hardening new devices before introducing into a corporate network?

- ☐ To comply with organizational rules
- ☐ To ease maintenance of devices
- ☐ To reduce exposure to attacks
- ☐ To avoid software licensing conflicts

Question 2681

The control that MOST effectively addresses the risk of piggybacking/tailgating into a restricted area without a dead man door is:

- ☐ using biometric door locks.
- ☐ security awareness training.
- ☐ requiring employees to wear ID badges.
- ☐ using two-factor authentication.

Question 2682

What supports data transmission through split cable facilities or duplicate cable facilities?

- ☐ Diverse routing
- ☐ Dual routing
- ☐ Alternate routing
- ☐ Redundant routing

Licensed to Berend Post berend.post@it-university.nl

Question 2683

A data center has a badge-entry system. Which of the following is MOST important to protect the computing assets in the center?

- ☐ Badge readers are installed in locations where tampering would be noticed
- ☐ The computer that controls the badge system is backed up frequently
- ☐ A process for promptly deactivating lost or stolen badges exists
- ☐ All badge entry attempts are logged

Question 2684

Which of the following is MOST important when an organization contracts for the long-term use of a custom-developed application?

- ☐ Documented coding standards
- ☐ Error correction management
- ☐ Contract renewal provisions
- ☐ Escrow clause

Question 2685

Which of the following type of computer has highest processing speed?

- ☐ Supercomputers
- ☐ Midrange servers
- ☐ Personal computers
- ☐ Thin client computers

Question 2686

In the IT department where segregation of duties is not feasible due to a limited number of resources, a team member is performing the functions of computer operator and reviewer of application logs. Which of the following would be the IS auditor's BEST recommendation?

- ☐ Develop procedures to verify that the application logs are not modified.
- ☐ Prevent the operator from performing application development activities.
- ☐ Assign an independent second reviewer to verify the application logs.
- ☐ Restrict the computer operator's access to the production environment.

Licensed to Berend Post berend.post@it-university.nl

Question 2687

Which of the following presents an inherent risk with no distinct identifiable preventive controls?

- ☐ Piggybacking
- ☐ Viruses
- ☐ Data diddling
- ☐ Unauthorized application shutdown

Question 2688

Which of the following fourth generation language depends on self-contained database management systems?

- ☐ Query and report generator
- ☐ Embedded database 4GLs
- ☐ Relational database 4GL
- ☐ Application generators

Question 2689

An organization has recently installed a security patch, which crashed the production server. To minimize the probability of this occurring again, an IS auditor should:

- ☐ apply the patch according to the patch's release notes.
- ☐ ensure that a good change management process is in place.
- ☐ thoroughly test the patch before sending it to production.
- ☐ approve the patch after doing a risk assessment.

Question 2690

The use of a GANTT chart can:

- ☐ aid in scheduling project tasks.
- ☐ determine project checkpoints.
- ☐ ensure documentation standards.
- ☐ direct the post-implementation review.

Question 2691

What kind of testing should programmers perform following any changes to an application or system?

- ☐ Unit, module, and full regression testing
- ☐ Module testing
- ☐ Unit testing
- ☐ Regression testing

Licensed to Berend Post berend.post@it-university.nl

Question 2692

Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:

- ☐ include the finding in the final report, because the IS auditor is responsible for an accurate report of all findings.
- ☐ not include the finding in the final report, because the audit report should include only unresolved findings.
- ☐ not include the finding in the final report, because corrective action can be verified by the IS auditor during the audit.
- ☐ include the finding in the closing meeting for discussion purposes only.

Question 2693

Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

- ☐ Multiple cycles of backup files remain available.
- ☐ Access controls establish accountability for e-mail activity.
- ☐ Data classification regulates what information should be communicated via e-mail.
- ☐ Within the enterprise, a clear policy for using e-mail ensures that evidence is available.

Question 2694

Common implementations of strong authentication may use which of the following factors in their authentication efforts (Choose three.):

- ☐ 'something you know'
- ☐ 'something you have'
- ☐ 'something you are'
- ☐ 'something you have done in the past on this same system'
- ☐ 'something you have installed on this same system'
- ☐ None of the choices.

Question 2695

Which of the following is MOST effective against system intrusions?

- ☐ Continuous monitoring
- ☐ Layered protection
- ☐ Penetration testing
- ☐ Two-factor authentication

Licensed to Berend Post berend.post@it-university.nl

Question 2696

Which of the following is BEST addressed when using a timestamp within a digital signature to deliver sensitive financial information?

- ☐ Replay protection
- ☐ Authentication
- ☐ Nonrepudiation
- ☐ Data integrity

Question 2697

Which of the following will BEST ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure?

- ☐ Maintaining system console logs in electronic format
- ☐ Ensuring bisynchronous capabilities on all transmission lines
- ☐ Using a database management system (DBMS) to dynamically back-out partially processed transactions
- ☐ Rotating backup copies of transaction files offsite

Question 2698

Which of the following term related to network performance refers to the actual rate that information is transferred over a network?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Jitter

Question 2699

Which of the following roles should be PRIMARILY responsible for assigning sensitivity levels to an organization's financial and payroll databases?

- ☐ Information security manager
- ☐ Data owner
- ☐ Systems administrator
- ☐ Database administrator

Licensed to Berend Post berend.post@it-university.nl

Question 2700

An organization allows employees to use personally owned mobile devices to access customers' personal information. An IS auditor's GREATEST concern should be whether:

- ☐ mobile devices are compatible with company infrastructure.
- ☐ devices have the capability to segregate business and personal data.
- ☐ mobile device security policies have been implemented.
- ☐ devices have adequate storage and backup capabilities.

Question 2701

Which of the following is NOT a true statement about public key infrastructure (PKI)?

- ☐ The Registration authority role is to validate and issue digital certificates to end users
- ☐ The Certificate authority role is to issue digital certificates to end users
- ☐ The Registration authority (RA) acts as a verifier for Certificate Authority (CA)
- ☐ Root certificate authority's certificate is always self-signed

Question 2702

The quality of the metadata produced from a data warehouse is _____ in the warehouse's design.

- ☐ Often hard to determine because the data is derived from a heterogeneous data environment
- ☐ The most important consideration
- ☐ Independent of the quality of the warehoused databases
- ☐ Of secondary importance to data warehouse content

Question 2703

To assist an organization in planning for IT investments, an IS auditor should recommend the use of:

- ☐ project management tools.
- ☐ an object-oriented architecture.
- ☐ tactical planning.
- ☐ enterprise architecture (EA).

Licensed to Berend Post berend.post@it-university.nl

Question 2704

Which of the following is the MOST effective approach for integrating security into application development?

- ☐ Including security in user acceptance testing sign-off
- ☐ Performing vulnerability scans
- ☐ Developing security models in parallel
- ☐ Defining security requirements

Question 2705

An IS auditor has been asked to participate in the creation of an organization's formal business continuity program. Which of the following would impair auditor independence?

- ☐ Developing disaster recovery test scenarios
- ☐ Determining system criticality
- ☐ Facilitating the business impact analysis (BIA)
- ☐ Participating on the business continuity committee

Question 2706

Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs. True or false?

- ☐ True
- ☐ False

Question 2707

Which of the following is MOST critical when creating data for testing the logic in a new or modified application system?

- ☐ A sufficient quantity of data for each test case
- ☐ Data representing conditions that are expected in actual processing
- ☐ Completing the test on schedule
- ☐ A random sample of actual data

Question 2708

An organization is replacing its financial processing system. To help ensure that transactions in the new system are processed accurately, which of the following is MOST appropriate?

- ☐ Compare year-to-date balances between the systems.
- ☐ Reconcile results of parallel processing.
- ☐ Document and test internal controls over the conversion.
- ☐ Review data file conversion procedures.

Licensed to Berend Post berend.post@it-university.nl

Question 2709

Which of the following protocol uses serial interface for communication between two computers in WAN technology?

- ☐ Point-to-point protocol
- ☐ X.25
- ☐ Frame Relay
- ☐ ISDN

Question 2710

Parity bits are a control used to validate:

- ☐ Data authentication
- ☐ Data completeness
- ☐ Data source
- ☐ Data accuracy

Question 2711

Which of the following is a distinguishing feature at the highest level of a maturity model?

- ☐ There are formal standards and procedures.
- ☐ Projects are controlled with management supervision.
- ☐ A continuous improvement process is applied.
- ☐ Processes are monitored continuously.

Question 2712

Which of the following can be thought of as the simplest and almost cheapest type of firewall?

- ☐ stateful firewall
- ☐ hardware firewall
- ☐ PIX firewall
- ☐ packet filter
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 2713

A computer system is no more secure than the human systems responsible for its operation. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them. zombie computers are being HEAVILY relied upon on by which of the following types of attack?

- ☐ Eavedropping
- ☐ DoS
- ☐ DDoS
- ☐ ATP
- ☐ Social Engineering
- ☐ None of the choices.

Question 2714

The use of a business case to obtain funding for an information security investment is MOST effective when the business case:

- ☐ translates information security policies and standards into business requirements.
- ☐ articulates management's intent and information security directives in clear language.
- ☐ relates the investment to the organization's strategic plan.
- ☐ realigns information security objectives to organizational strategy.

Question 2715

An organization is running servers with critical business applications that are in an area subject to frequent but brief power outages. Knowledge of which of the following would allow the organization's management to monitor the ongoing adequacy of the uninterrupted power supply (UPS)?

- ☐ Duration and interval of the power outages
- ☐ Business impact of server downtime
- ☐ Number of servers supported by the UPS
- ☐ Mean time to recover servers after failure

Question 2716

Which of the following level in CMMI model focuses on process definition and process deployment?

- ☐ Level 4
- ☐ Level 5
- ☐ Level 3
- ☐ Level 2

Licensed to Berend Post berend.post@it-university.nl

Question 2717

Which of the following would be the BEST access control procedure?

- ☐ The data owner formally authorizes access and an administrator implements the user authorization tables.
- ☐ Authorized staff implements the user authorization tables and the data owner sanctions them.
- ☐ The data owner and an IS manager jointly create and update the user authorization tables.
- ☐ The data owner creates and updates the user authorization tables.

Question 2718

How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?

- ☐ Modems convert analog transmissions to digital, and digital transmission to analog.
- ☐ Modems encapsulate analog transmissions within digital, and digital transmissions within analog.
- ☐ Modems convert digital transmissions to analog, and analog transmissions to digital.
- ☐ Modems encapsulate digital transmissions within analog, and analog transmissions within digital.

Question 2719

The PRIMARY benefit to using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry-pipe system:

- ☐ has a decreased risk of leakage.
- ☐ is more effective at suppressing flames.
- ☐ allows more time to abort release of the suppressant.
- ☐ disperses dry chemical suppressants exclusively.

Question 2720

Which of the following provides the GREATEST assurance that an organization allocates appropriate resources to respond to information security events?

- ☐ Incident classification procedures
- ☐ Threat analysis and intelligence reports
- ☐ An approved IT staffing plan
- ☐ Information security policies and standards.

Licensed to Berend Post berend.post@it-university.nl

Question 2721

Reorganization of databases is undertaken PRIMARILY to:

- ☐ reduce backout and recovery times.
- ☐ eliminate duplicates and perform data backup.
- ☐ reduce simultaneous update time and index validation.
- ☐ improve data access and retrieval times.

Question 2722

Which of the following would a digital signature MOST likely prevent?

- ☐ Corruption
- ☐ Unauthorized change
- ☐ Repudiation
- ☐ Disclosure

Question 2723

Which of the following would be the MOST appropriate reason for an organization to purchase fault-tolerant hardware?

- ☐ Reducing hardware maintenance costs.
- ☐ Improving system performance.
- ☐ Minimizing business loss.
- ☐ Compensating for the lack of contingency planning

Question 2724

To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:

- ☐ enterprise data model.
- ☐ IT balanced scorecard (BSC).
- ☐ IT organizational structure.
- ☐ historical financial statements.

Licensed to Berend Post berend.post@it-university.nl

Question 2725

An organization has outsourced many application development activities to a third party that uses contract programmers extensively. Which of the following would provide the BESTassurance that the third party's contract programmers comply with the organization's security policies?

- ☐ Perform periodic security assessments of the contractors' activities.
- ☐ Conduct periodic vulnerability scans of the application.
- ☐ Include penalties for noncompliance in the contracting agreement.
- ☐ Require annual signed agreements of adherence to security policies.

Question 2726

Which of the following is the PRIMARY reason for an IS auditor to issue an interim audit report?

- ☐ To avoid issuing a final audit report
- ☐ To enable the auditor to complete the engagement in a timely manner
- ☐ To provide feedback to the auditee for timely remediation
- ☐ To provide follow-up opportunity during the audit

Question 2727

Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

- ☐ A monitored double-doorway entry system
- ☐ A monitored turnstile entry system
- ☐ A monitored doorway entry system
- ☐ A one-way door that does not allow exit after entry

Question 2728

An organization allows employee use of personal mobile devices for corporate email. Which of the following should be the GREATEST IS audit concern?

- ☐ Email forwarding to private devices requires excessive network bandwidth
- ☐ There is no corporate policy for the acceptable use of private devices
- ☐ There is no adequate tracking of the working time spent out-of-hours
- ☐ The help desk is not able to fully support different kinds of private devices

Licensed to Berend Post berend.post@it-university.nl

Question 2729

A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?

- ☐ Key verification
- ☐ One-for-one checking
- ☐ Manual recalculations
- ☐ Functional acknowledgements

Question 2730

An organization is planning to replace its wired networks with wireless networks. Which of the following would BEST secure the wireless network from unauthorized access?

- ☐ Implement Wired Equivalent Privacy (WEP)
- ☐ Permit access to only authorized Media Access Control (MAC) addresses
- ☐ Disable open broadcast of service set identifiers (SSID)
- ☐ Implement Wi-Fi Protected Access (WPA) 2

Question 2731

An IS auditor would MOST likely recommend that IT management use a balanced scorecard to:

- ☐ ensure that IT staff meet performance requirements.
- ☐ train and educate IT staff.
- ☐ indicate whether the organization meets quality standards.
- ☐ assess IT functions and processes.

Question 2732

A large organization is considering a policy that would allow employees to bring their own smartphones into the organizational environment. The MOST important concern to the information security manager should be the:

- ☐ lack of a device management solution.
- ☐ decrease in end user productivity.
- ☐ impact on network capacity.
- ☐ higher costs in supporting end users.

Licensed to Berend Post berend.post@it-university.nl

Question 2733

Which of the following should an IS auditor review FIRST when planning a customer data privacy audit?

- ☐ Legal and compliance requirements
- ☐ Customer agreements
- ☐ Organizational policies and procedures
- ☐ Data classification

Question 2734

Which of the following is the GREATEST risk when storage growth in a critical file server is not managed properly?

- ☐ Backup time would steadily increase
- ☐ Backup operational cost would significantly increase
- ☐ Storage operational cost would significantly increase
- ☐ Server recovery work may not meet the recovery time objective (RTO)

Question 2735

The phases and deliverables of a system development life cycle (SDLC) project should be determined:

- ☐ during the initial planning stages of the project.
- ☐ after early planning has been completed, but before work has begun.
- ☐ throughout the work stages, based on risks and exposures.
- ☐ only after all risks and exposures have been identified and the IS auditor has recommended appropriate controls.

Question 2736

A sender of an e-mail message applies a digital signature to the digest of the message. This action provides assurance of the:

- ☐ date and time stamp of the message.
- ☐ identity of the originating computer.
- ☐ confidentiality of the message's content.
- ☐ authenticity of the sender.

Licensed to Berend Post berend.post@it-university.nl

Question 2737

Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following?

- ☐ IT strategic plan
- ☐ Business continuity plan
- ☐ Business impact analysis
- ☐ Incident response plan

Question 2738

Which of the following is MOST important when selecting an information security metric?

- ☐ Defining the metric in quantitative terms
- ☐ Aligning the metric to the IT strategy
- ☐ Defining the metric in qualitative terms
- ☐ Ensuring the metric is repeatable

Question 2739

What type of fire-suppression system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities?

- ☐ A dry-pipe sprinkler system
- ☐ A deluge sprinkler system
- ☐ A wet-pipe system
- ☐ A halon sprinkler system

Question 2740

Which of the following provides the MOST comprehensive description of IT's role in an organization?

- ☐ IT organizational chart
- ☐ IT project portfolio
- ☐ IT charter
- ☐ IT job description

Licensed to Berend Post berend.post@it-university.nl

Question 2741

An external penetration test identified a serious security vulnerability in a critical business application. Before reporting the vulnerability to senior management, the information security manager's BEST course of action should be to:

- ☐ determine the potential impact with the business owner
- ☐ initiate the incident response process
- ☐ block access to the vulnerable business application
- ☐ report the vulnerability to IT for remediation

Question 2742

Which of the following implementation modes would provide the GREATEST amount of security for outbound data connecting to the internet?

- ☐ Transport mode with authentication header (AH) plus encapsulating security payload (ESP)
- ☐ Secure Sockets Layer (SSL) mode
- ☐ Tunnel mode with AH plus ESP
- ☐ Triple-DES encryption mode

Question 2743

A business application system accesses a corporate database using a single ID and password embedded in a program. Which of the following would provide efficient access control over the organization's data?

- ☐ Introduce a secondary authentication method such as card swipe
- ☐ Apply role-based permissions within the application system
- ☐ Have users input the ID and password for each database transaction
- ☐ Set an expiration period for the database password embedded in the program

Question 2744

During an IS audit, it is discovered that security configurations differ across the organization's virtual server farm. Which of the following is the IS auditor's BEST recommendation for improving the control environment?

- ☐ Conduct an independent review of each server's security configuration
- ☐ Implement a security configuration baseline for virtual servers
- ☐ Implement security monitoring controls for high-risk virtual servers
- ☐ Conduct a standard patch management review across the virtual server farm

Licensed to Berend Post berend.post@it-university.nl

Question 2745

Which of the following should be an information security manager's PRIMARY role when an organization initiates a data classification process?

- ☐ Assign the asset classification level.
- ☐ Define the classification structure to be implemented.
- ☐ Verify that assets have been appropriately classified.
- ☐ Apply security in accordance with specific classification.

Question 2746

If an IS auditor finds evidence of risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function, what is the auditor's primary responsibility?

- ☐ To advise senior management.
- ☐ To reassign job functions to eliminate potential fraud.
- ☐ To implement compensator controls.
- ☐ Segregation of duties is an administrative control not considered by an IS auditor.

Question 2747

Online banking transactions are being posted to the database when processing suddenly comes to a halt. The integrity of the transaction processing is BEST ensured by:

- ☐ database integrity checks.
- ☐ validation checks.
- ☐ input controls.
- ☐ database commits and rollbacks.

Question 2748

Which of the following is the most important benefit of control self-assessment (CSA)?

- ☐ CSA is a policy/rule driven
- ☐ In CSA approach, risk is identified sooner
- ☐ CSA requires limited employee participations
- ☐ In CSA, resources are being used in an effective manner.

Licensed to Berend Post berend.post@it-university.nl

Question 2749

Which of the following BEST provides continuous availability of network bandwidth for critical application services?

- ☐ Configuration management
- ☐ Cloud computing
- ☐ Problem management
- ☐ Quality of service (QoS)

Question 2750

Which of the following is the PRIMARY benefit of using an integrated audit approach?

- ☐ Higher acceptance of the findings from the audited business areas
- ☐ The avoidance of duplicated work and redundant recommendations
- ☐ Enhanced allocation of resources and reduced audit costs
- ☐ A holistic perspective of overall risk and a better understanding of controls

Question 2751

Which of the following terms refers to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders?

- ☐ ILD&P
- ☐ ICT&P
- ☐ ILP&C
- ☐ ILR&D
- ☐ None of the choices.

Question 2752

When developing a disaster recovery plan, the criteria for determining the acceptable downtime should be the:

- ☐ annualized loss expectancy (ALE).
- ☐ service delivery objective.
- ☐ quantity of orphan data.
- ☐ maximum tolerable outage.

Licensed to Berend Post berend.post@it-university.nl

Question 2753

The MOST significant reason for using key performance indicators (KPIs) to track the progress of IT projects against initial targets is that they:

- ☐ influence management decisions to outsource IT projects
- ☐ identify which projects may require additional funding
- ☐ provide timely indication of when corrective actions need to be taken
- ☐ identify instances where increased stakeholder engagement is required

Question 2754

An organization with many desktop PCs is considering moving to a thin client architecture. Which of the following is the MAJOR advantage?

- ☐ Administrative security can be provided for the client.
- ☐ System administration can be better managed.
- ☐ The security of the desktop PC is enhanced.
- ☐ Desktop application software will never have to be upgraded.

Question 2755

Run-to-run totals can verify data through which stage(s) of application processing?

- ☐ Initial
- ☐ Various
- ☐ Final
- ☐ Output

Question 2756

Which of the following would prevent unauthorized changes to information stored in a server's log?

- ☐ Write-protecting the directory containing the system log
- ☐ Writing a duplicate log to another server
- ☐ Daily printing of the system log
- ☐ Storing the system log in write-once media

Question 2757

In an audit of an inventory application, which approach would provide the BEST evidence that purchase orders are valid?

- ☐ Testing whether inappropriate personnel can change application parameters
- ☐ Tracing purchase orders to a computer listing
- ☐ Comparing receiving reports to purchase order details
- ☐ Reviewing the application documentation

Licensed to Berend Post berend.post@it-university.nl

Question 2758

Passwords should be:

- ☐ assigned by the security administrator for first time logon.
- ☐ changed every 30 days at the discretion of the user.
- ☐ reused often to ensure the user does not forget the password.
- ☐ displayed on the screen so that the user can ensure that it has been entered properly.

Question 2759

A certificate authority (CA) can delegate the processes of:

- ☐ revocation and suspension of a subscriber's certificate.
- ☐ generation and distribution of the CA public key.
- ☐ establishing a link between the requesting entity and its public key.
- ☐ issuing and distributing subscriber certificates.,

Question 2760

Which of the following is the GREATEST risk of single sign-on?

- ☐ Password carelessness by one user may render the entire infrastructure vulnerable
- ☐ Integration of single sign-on with the rest of the infrastructure is complicated
- ☐ It is a single point of failure for an enterprise access control process
- ☐ One administrator maintains the single sign-on solutions without segregation of duty

Question 2761

Which of the following control helps to identify an incident's activities and potentially an intruder?

- ☐ Deterrent
- ☐ Preventive
- ☐ Detective
- ☐ Compensating

Question 2762

The PRIMARY reason an organization would require that users sign an acknowledgment of their system access responsibilities is to:

- ☐ maintain compliance with industry best practices.
- ☐ serve as evidence of security awareness training.
- ☐ assign accountability for transactions made with the user's ID.
- ☐ maintain an accurate record of users' access rights.

Licensed to Berend Post berend.post@it-university.nl

Question 2763

An IS auditor reviewing an organization's IS disaster recovery plan should verify that it is:

- ☐ tested every six months.
- ☐ regularly reviewed and updated.
- ☐ approved by the chief executive officer (CEO).
- ☐ communicated to every department head in the organization.

Question 2764

An IS auditor submitted audit reports and scheduled a follow-up audit engagement with a client. The client has requested to engage the services of the same auditor to develop enhanced controls. What is the GREATEST concern with this request?

- ☐ It would require the approval of the audit manager.
- ☐ It would be beyond the original audit scope.
- ☐ It would a possible conflict of interest.
- ☐ It would require a change to the audit plan.

Question 2765

During an audit of the organization’s data privacy policy, the IS auditor identified that only some IT application databases have encryption in place. What should be the auditor’s FIRST action?

- ☐ Assess the resources required to implement encryption to unencrypted databases.
- ☐ Review the most recent database penetration testing results.
- ☐ Determine whether compensating controls are in place.
- ☐ Review a comprehensive list of databases with the information they contain.

Question 2766

An organization is considering allowing users to connect personal devices to the corporate network. Which of the following should be done FIRST?

- ☐ Configure users on the mobile device management solution.
- ☐ Create inventory records of personal devices.
- ☐ Implement an acceptable use policy.
- ☐ Conduct security awareness training.

Licensed to Berend Post berend.post@it-university.nl

Question 2767

Which of the following is BEST for providing uninterrupted services?

- ☐ Snapshots
- ☐ Differential backup
- ☐ Televaulting
- ☐ Mirroring

Question 2768

Properly planned risk-based audit programs are often capable of offering which of the following benefits?

- ☐ audit efficiency and effectiveness.
- ☐ audit efficiency only.
- ☐ audit effectiveness only.
- ☐ audit transparency only.
- ☐ audit transparency and effectiveness.
- ☐ None of the choices.

Question 2769

What is the most common purpose of a virtual private network implementation?

- ☐ A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over an otherwise unsecured channel such as the Internet.
- ☐ A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a dedicated T1 connection.
- ☐ A virtual private network (VPN) helps to secure access within an enterprise when communicating over a dedicated T1 connection between network segments within the same facility.
- ☐ A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a wireless connection.

Question 2770

Data edits are implemented before processing and are considered which of the following?

- ☐ Deterrent integrity controls
- ☐ Detective integrity controls
- ☐ Corrective integrity controls
- ☐ Preventative integrity controls

Licensed to Berend Post berend.post@it-university.nl

Question 2771

Which of the following is the GREATEST risk to the effectiveness of application system controls?

- ☐ Removal of manual processing steps
- ☐ inadequate procedure manuals
- ☐ Collusion between employees
- ☐ Unresolved regulatory compliance issues

Question 2772

As an IS auditor, it is very important to make sure all storage media are well protected. Which of the following is the LEAST important factor for protecting CDs and DVDs?

- ☐ Handle by edges or by the hole in the middle
- ☐ Store in anti-static bag
- ☐ Avoid long term exposure to bright light
- ☐ Store in a hard jewel case, not in soft sleeves

Question 2773

Which of the following layer of an OSI model responsible for routing and forwarding of a network packets?

- ☐ Transport Layer
- ☐ Network Layer
- ☐ Data Link Layer
- ☐ Physical Layer

Question 2774

A proposed transaction processing application will have many data capture sources and outputs in paper and electronic form. To ensure that transactions are not lost during processing, an IS auditor should recommend the inclusion of:

- ☐ validation controls.
- ☐ internal credibility checks.
- ☐ clerical control procedures.
- ☐ automated systems balancing.

Licensed to Berend Post berend.post@it-university.nl

Question 2775

Determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as:

- ☐ the likelihood of a given threat attempting to exploit a vulnerability
- ☐ a function of the cost and effectiveness of controls over a vulnerability
- ☐ the magnitude of the impact should a threat exploit a vulnerability
- ☐ a function of the likelihood and impact, should a threat exploit a vulnerability

Question 2776

Which of the following software development methodology uses minimal planning and in favor of rapid prototyping?

- ☐ Agile Developments
- ☐ Software prototyping
- ☐ Rapid application development
- ☐ Component based development

Question 2777

Which of the following would be the MOST effective control to reduce the risk of information leakage through social media?

- ☐ Use of keystroke loggers
- ☐ Periodic review of the data classification policy
- ☐ Limited access to social media sites in the workplace
- ☐ Security awareness training

Question 2778

The success of an IT projects is measured PRIMARILY by the:

- ☐ translation of business vision to function vision
- ☐ implementation of current technology
- ☐ benefit that the business derives from the outcome
- ☐ efficient use of resources

Licensed to Berend Post berend.post@it-university.nl

Question 2779

Which of the following should be the PRIMARY reason to establish a social media policy for all employees?

- ☐ To publish acceptable messages to be used by employees when posting
- ☐ To raise awareness and provide guidance about social media risks
- ☐ To restrict access to social media during business hours to maintain productivity
- ☐ To prevent negative public social media postings and comments

Question 2780

Which of the following is the MOST important element for the successful implementation of IT governance?

- ☐ Implementing an IT scorecard
- ☐ Identifying organizational strategies
- ☐ Performing a risk assessment
- ☐ Creating a formal security policy

Question 2781

Which of the following audit is mainly designed to evaluate the internal control structure in a given process or area?

- ☐ Compliance Audit
- ☐ Financial Audit
- ☐ Operational Audit
- ☐ Forensic audit

Question 2782

Which of the following groups is MOST likely responsible for the implementation of IT projects?

- ☐ IT steering committee
- ☐ IT compliance committee
- ☐ IT strategy committee
- ☐ IT governance committee

Licensed to Berend Post berend.post@it-university.nl

Question 2783

An IS auditor learns a server administration team regularly applies workarounds to address repeated failures of critical data processing services. Which of the following would BEST enable the organization to resolve this issue?

- ☐ Service level management
- ☐ Change management
- ☐ Problem management
- ☐ Incident management

Question 2784

Which of the following BEST reduces the ability of one device to capture the packets that are meant for another device?

- ☐ Filters
- ☐ Switches
- ☐ Routers
- ☐ Firewalls

Question 2785

Which of the following fire-suppression methods is considered to be the most environmentally friendly?

- ☐ Halon gas
- ☐ Deluge sprinklers
- ☐ Dry-pipe sprinklers
- ☐ Wet-pipe sprinklers

Question 2786

Which of the following can provide assurance that an IT project has delivered its planned benefits?

- ☐ User acceptance testing (UAT)
- ☐ Steering committee approval
- ☐ Post-implementation review
- ☐ Quality assurance evaluation

Licensed to Berend Post berend.post@it-university.nl

Question 2787

Due to the cost restrains, a company defers the replacement of hardware supporting core application. Which of the following represents the GREATEST risk?

- ☐ Maintenance costs may rise.
- ☐ Future upgrades may not be possible.
- ☐ Systems availability may suffer.
- ☐ Eventual replacement may be more expensive.

Question 2788

In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as:

- ☐ wormnets
- ☐ trojannets
- ☐ spynets
- ☐ botnets
- ☐ rootnets
- ☐ backdoor

Question 2789

A check digit is an effective edit check to:

- ☐ Detect data-transcription errors
- ☐ Detect data-transposition and transcription errors
- ☐ Detect data-transposition, transcription, and substitution errors
- ☐ Detect data-transposition errors

Question 2790

What is the recommended minimum length of a good password?

- ☐ 6 characters
- ☐ 8 characters
- ☐ 12 characters
- ☐ 18 characters
- ☐ 22 characters
- ☐ None of the choices.

Licensed to Berend Post berend.post@it-university.nl

Question 2791

When installing an intrusion detection system (IDS), which of the following is MOST important?

- ☐ Properly locating it in the network architecture
- ☐ Preventing denial-of-service (DoS) attacks
- ☐ Identifying messages that need to be quarantined
- ☐ Minimizing the rejection errors

Licensed to Berend Post berend.post@it-university.nl