



isaca.test-king.cisa.v2020-10-08.by.mason.1457q.vce

CISA

CISA

Score: 800/1000
Version: 1
Time Limit: 120 Minutes

Exam A (1457 questions)

Question 1

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.

Question 2

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.

Question 3

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 4

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 5

When an organization outsources a payroll system to a cloud service provider, the IS auditor's PRIMARY concern should be the:

- ☐ service level agreement (SLA) is not reviewed annually.
- ☐ lack of independent assurance from a third party.
- ☐ service provider's data center is on the ground floor.
- ☐ service provider's platform is not compatible with legacy systems.

Question 6

The IS security group is planning to implement single sign-on. What is the IS auditor's PRIMARY concern?

- ☐ Integrated access rules will increase users' access privileges.
- ☐ Managing user IDs/passwords will require increased efforts.
- ☐ Integrated access rules will restrict users' access privileges.
- ☐ Compromise of a user ID/password will yield more privileges.

Question 7

An organization has implemented an automated match between purchase orders, goods receipts, and invoices. Which of the following risks will this control BEST mitigate?

- ☐ Customer discounts not being applied
- ☐ A legitimate transaction being paid multiple times
- ☐ Invalid payments being processed by the system
- ☐ Delay of purchase orders

Question 8

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 9

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 10

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

Question 11

Which of the following level in CMMI model focuses on process definition and process deployment?

- ☐ Level 4
- ☐ Level 5
- ☐ Level 3
- ☐ Level 2

Question 12

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 13

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 14

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 15

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 16

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

Question 17

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 18

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.

Question 19

An IS auditor notes that several users have not logged into an application for more than one year. Which of the following would be the BEST audit recommendation?

- ☐ Periodically review the information security policy.
- ☐ Update the termination procedures.
- ☐ Periodically review user access.
- ☐ Delete the affected users' IDs.

Question 20

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 21

The GREATEST risk of database denormalization is:

- ☐ decreased performance.
- ☐ loss of data confidentiality.
- ☐ loss of database integrity.
- ☐ incorrect metadata.

Question 22

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.

Question 23

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 24

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 25

Which of the following reports can MOST effectively be used to analyze a systems performance problem?

- ☐ Synchronization report
- ☐ Console log
- ☐ Utilization report
- ☐ Database usage log

Question 26

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

Question 27

Which of the following is MOST efficiently protects computer equipment against short-term reductions in electrical power?

- ☐ Power line conditioners
- ☐ Surge protective devices
- ☐ Alternative power supplies
- ☐ Interruptible power supplies

Question 28

Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

- ☐ True
- ☐ False

Question 29

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.

Question 30

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 31

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 32

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 33

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

Question 34

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 35

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 36

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 37

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

Question 38

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 39

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

Question 40

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.

Question 41

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 42

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 43

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 44

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.

Question 45

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 46

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 47

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 48

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 greater the sample size
- ☐ The greater the sample size, the lower the expected error rate

Question 49

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 50

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 51

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

Question 52

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 53

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 54

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.

Question 55

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 56

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

Question 57

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.

Question 58

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 59

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 60

A lower recovery time objective (RTO) results in:

- ☐ higher disaster tolerance.
- ☐ higher cost.
- ☐ wider interruption windows.
- ☐ more permissive data loss.

Question 61

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 62

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 63

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.

Question 64

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 65

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 66

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 67

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 68

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.

Question 69

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.

Question 70

Which of the following audit mainly focuses on discovering and disclosing on frauds and crimes?

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

Question 71

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 72

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 73

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 74

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.

Question 75

Which of the following would protect the confidentiality of information sent in email messages?

- ☐ Encryption
- ☐ Digital certificates
- ☐ Digital signatures
- ☐ Secure Hash Algorithm 1 (SHA-1)

Question 76

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 77

Which of the following should be considered when examining fire suppression systems as part of a data center environmental controls review?

- ☐ Maintenance procedures
- ☐ Onsite replacement availability
- ☐ Insurance coverage
- ☐ Installation manuals

Question 78

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 79

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.

Question 80

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 81

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

Question 82

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 83

A configuration management audit identified that predefined automated procedures are used when deploying and configuring application infrastructure in a cloud-based environment. Which of the following is MOST important for the IS auditor to review?

- ☐ Contracts of vendors responsible for maintaining provisioning tools
- ☐ Processes for making changes to cloud environment specifications
- ☐ Storage location of configuration management documentation
- ☐ Number of administrators with access to cloud management consoles

Question 84

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 85

Which of the following tools is MOST helpful in estimating budgets for tasks within a large IT business application project?

- ☐ Balanced scorecard
- ☐ Gantt chart
- ☐ Function point analysis (FPA)
- ☐ Critical path methodology (CPM)

Question 86

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 87

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 88

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 89

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 90

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 91

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 the auditee agrees with key issues in these workpapers.
- ☐ consider the appropriateness and sufficiency of the workpapers.

Question 92

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 93

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 94

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 95

Which of the following is the PRIMARY function of technology-driven enterprise architecture?

- ☐ To provide guidance on technological decisions in the context of business strategy
- ☐ To determine how new technologies fit into existing networks and data flows
- ☐ To help develop project documentation and related business process roadmaps
- ☐ To re-engineer business processes to make better use of technology

Question 96

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

Question 97

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

Question 98

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 99

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 100

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

Question 101

Which of the following BEST facilitates the ability to efficiently allocate time, effort, and resources to address security incidents?

- ☐ Incident classification
- ☐ Incident definition
- ☐ Incident escalation
- ☐ Incident monitoring

Question 102

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 103

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 104

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 105

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 106

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

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

Question 107

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.

Question 108

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.

Question 109

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.

Question 110

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 111

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 112

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 113

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

Question 114

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.

Question 115

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 116

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 117

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 118

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 119

Which of the following is the BEST indication that a newly developed information system is ready for migration into production?

- ☐ Items in the work breakdown structure are completed.
- ☐ Audit has signed off.
- ☐ User acceptance testing is successfully completed.
- ☐ Technical requirements are met.

Question 120

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 121

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 122

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 123

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 124

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 125

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 126

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 127

Which of the following is MOST important for an IS auditor to consider when auditing a vulnerability scanning software solution?

- ☐ The scanning software was purchased from an approved vendor.
- ☐ The scanning software was approved for release into production.
- ☐ The scanning software covers critical systems.
- ☐ The scanning software is cost-effective.

Question 128

Which of the following should an IS auditor expect to find when reviewing IT security policy?

- ☐ Assigned responsibility for safeguarding company assets
- ☐ A risk-based classification of systems
- ☐ An inventory of information assets
- ☐ Virus protection implementation strategies

Question 129

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 130

When providing a vendor with data containing personally identifiable information (PII) for offsite testing, the data should be:

- ☐ current
- ☐ encrypted.
- ☐ sanitized.
- ☐ backed up.

Question 131

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 132

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

Question 133

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 134

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 135

Which of the following should an IS auditor review FIRST when evaluating incident management procedures?

- ☐ Command center monitoring
- ☐ Root cause analysis steps
- ☐ Prioritization criteria
- ☐ Peer review requirements

Question 136

Which of the following is an IS auditor's BEST recommendation for mitigating risk associated with rapid expansion of hosts within a virtual environment?

- ☐ Limit access to the hypervisor operating system (OS) and administration console
- ☐ Ensure quick access to updated images of a guest operating system for fast recovery
- ☐ Consider using a third-party service provider to share the virtual machine (VM) risk
- ☐ Implement policies and processes to control virtual machine (VM) lifecycle management

Question 137

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 138

An accurate biometric system usually exhibits (Choose two.):

- ☐ low EER
- ☐ low CER
- ☐ high EER
- ☐ high CER
- ☐ None of the choices.

Question 139

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

Question 140

Which of the following is the MOST effective way for an IS auditor to identify unauthorized changes to the production state of a critical business application?

- ☐ Run an automated scan of the production environment to detect missing software patches.
- ☐ Compare a list of production system changes with the configuration management database (CMDB).
- ☐ Review recently approved changes to application programming interfaces (API) in the production environment.
- ☐ Review recent updates in the configuration management database (CMDB) for compliance with IT policies.

Question 141

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 142

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 143

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.

Question 144

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 145

"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 146

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 147

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

Question 148

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 149

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 identify 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 150

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.

Question 151

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 152

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 153

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 154

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 155

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.

Question 156

Which of the following components is responsible for the collection of data in an intrusion detection system (IDS)?

- ☐ Analyzer
- ☐ Administration console
- ☐ User interface
- ☐ Sensor

Question 157

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.

Question 158

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 159

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 160

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 161

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 162

The risk that is created if a single sign-on is implemented for all systems is that a/an:

- ☐ user can bypass current access security.
- ☐ compromised password gives access to all systems.
- ☐ authorized user can bypass the security layers.
- ☐ user has equivalent access on all systems.

Question 163

Which of the following should be a PRIMARY control objective when designing controls for system interfaces?

- ☐ Ensure peer-to-peer data transfers are minimized.
- ☐ Ensure all data transferred through system interfaces is encrypted.
- ☐ Ensure managed file transfer (MFT) systems have restart capability for interruptions.
- ☐ Ensure data on the sending system is identical to the data on the receiving system.

Question 164

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 165

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 166

Parity bits are a control used to validate:

- ☐ Data authentication
- ☐ Data completeness
- ☐ Data source
- ☐ Data accuracy

Question 167

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 168

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

Question 169

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 170

Which of the following roles is BEST suited to assign classification to an information asset?

- ☐ The data owner
- ☐ The information security manager
- ☐ The data custodian
- ☐ The senior manager

Question 171

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.

Question 172

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 173

A security review focused on data loss prevention (DLP) revealed the organization has no visibility to data stored in the cloud. What is the IS auditor's BEST recommendation to address this issue?

- ☐ Implement a file system scanner to discover data stored in the cloud.
- ☐ Utilize a DLP tool on desktops to monitor user activities.
- ☐ Employ a cloud access security broker (CASB).
- ☐ Enhance the firewall at the network perimeter.

Question 174

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 175

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 176

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.

Question 177

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 178

An audit of a database management system found the audit log was not restarted following maintenance. Which of the following is the GREATEST concern to the IS auditor?

- ☐ Changes by the database administrators will not be logged.
- ☐ The database optimization will be compromised.
- ☐ The database triggers and pointers will not be optimized.
- ☐ Changes by application users will not be logged.

Question 179

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 180

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 181

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 182

Which of the following is a standard secure email protection protocol?

- ☐ S/MIME
- ☐ SSH
- ☐ SET
- ☐ S/HTTP

Question 183

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 184

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.

Question 185

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

Question 186

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.

Question 187

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 188

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 189

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 190

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 191

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.

Question 192

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 193

What is the MOST effective method of preventing unauthorized use of data files?

- ☐ Automated file entry
- ☐ Tape librarian
- ☐ Access control software
- ☐ Locked library

Question 194

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 195

Test and development environments should be separated. True or false?

- ☐ True
- ☐ False

Question 196

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 197

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 198

Which of the following BEST enables system resiliency for an e-commerce organization that requires a low recovery time objective (RTO) and a low recovery point objective (RPO)?

- ☐ Redundant arrays
- ☐ Nightly backups
- ☐ Remote backups
- ☐ Mirrored sites

Question 199

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 200

Which of the following is NOT a defined ISO basic task related to network management?

- ☐ Fault management
- ☐ Accounting resources
- ☐ Security management
- ☐ Communications management

Question 201

Which of the following factors constitutes a strength in regard to the use of a disaster recovery planning reciprocal agreement?

- ☐ Changes to the hardware or software environment by one company could make the agreement ineffective or obsolete.
- ☐ Reciprocal agreements may not be formally established in a contract.
- ☐ The two companies might share a need for a specialized piece of equipment.
- ☐ A disaster could occur that would affect both companies.

Question 202

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 203

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 204

When reviewing a database supported by a third-party service provider, an IS auditor found minor control deficiencies. The auditor should FIRST discuss recommendations with the:

- ☐ service provider support team manager
- ☐ organization's service level manager
- ☐ organization's chief information officer (CIO)
- ☐ service provider contract liaison

Question 205

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 206

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 207

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.

Question 208

A poor choice of passwords and transmission over unprotected communications lines are examples of:

- ☐ vulnerabilities.
- ☐ threats.
- ☐ probabilities.
- ☐ impacts.

Question 209

Machines that operate as a closed system can NEVER be eavesdropped.

- ☐ True
- ☐ False

Question 210

Which of the following is NOT an example of corrective control?

- ☐ OS Upgrade
- ☐ Backup and restore
- ☐ Contingency planning
- ☐ System Monitoring

Question 211

Which of the following ensures confidentiality of information sent over the internet?

- ☐ Digital signature
- ☐ Digital certificate
- ☐ Online Certificate Status Protocol
- ☐ Private key cryptosystem

Question 212

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 213

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 214

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 215

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 216

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.

Question 217

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 218

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 219

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

Question 220

Which combination of access controls provides the BEST physical protection for a server room?

- ☐ PIN and smart card
- ☐ User ID and PIN
- ☐ Card with a magnetic strip and a smart card
- ☐ Card with a magnetic strip and a shared PIN

Question 221

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 222

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.

Question 223

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 224

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 225

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 226

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 227

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.

Question 228

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 229

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

Question 230

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 231

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 232

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

Question 233

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 234

Which of the following presents the GREATEST concern when implementing data flow across borders?

- ☐ Software piracy laws
- ☐ National privacy laws
- ☐ Political unrest
- ☐ Equipment incompatibilities

Question 235

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 236

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 237

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 238

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

Question 239

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 240

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 241

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 242

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 243

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.

Question 244

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 245

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 246

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

Question 247

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 248

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 249

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 250

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 251

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 252

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 253

Which of the following system and data conversion strategies provides the GREATEST redundancy?

- ☐ Direct cutover
- ☐ Pilot study
- ☐ Phased approach
- ☐ Parallel run

Question 254

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 255

Which of the following is the BEST indication that an organization's vulnerability identification capability has achieved a high level of maturity?

- ☐ The organization collaborates with relevant partners to correlate vulnerability data.
- ☐ Known application vulnerabilities are manually categorized and prioritized.
- ☐ Vulnerability management tools are tailored for specific operating systems.
- ☐ Tools are in place to periodically identify new and updated vulnerabilities.

Question 256

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

Question 257

An organization has selected a web-based solution to reduce transaction costs and improve productivity. Before implementation, an IS auditor should ensure that the organization has:

- ☐ performed a vulnerability assessment.
- ☐ implemented electronic data interchange.
- ☐ validated the solution against the current IT infrastructure.
- ☐ addressed the level of risk exposure.

Question 258

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

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

Question 259

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 260

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.

Question 261

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 262

An IS auditor finds that the cost of developing an application is now projected to significantly exceed the budget. Which of the following is the GREATEST risk to communicate to senior management?

- ☐ Increased staff turnover
- ☐ Project abandonment
- ☐ Noncompliance with project methodology
- ☐ Inability to achieve expected benefits

Question 263

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 264

A region where an organization conducts business has announced changes in privacy legislation. Which of the following should an IS auditor do FIRST to prepare for the changes?

- ☐ Perform a gap analysis with current privacy procedures.
- ☐ Provide suggested updates to the organization's privacy procedures.
- ☐ Communicate the changes in privacy legislation to the legal department.
- ☐ Design compensating controls to be in compliance with new privacy legislation.

Question 265

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 266

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 267

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 268

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

Question 269

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 270

An IS auditor determines that a business impact analysis (BIA) was not conducted during the development of a business continuity plan (BCP). What is the MOST significant risk that could result from this situation?

- ☐ Responsibilities are not properly defined.
- ☐ Recovery time objectives (RTOs) are not correctly determined.
- ☐ Key performance indicators (KPIs) are not aligned.
- ☐ Critical business applications are not covered.

Question 271

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 272

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 273

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 274

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 275

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 276

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 277

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 278

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 279

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 280

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 281

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 282

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 283

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 284

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 285

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 286

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 287

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 288

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 289

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 290

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 291

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 292

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 293

A vulnerability in which of the following virtual systems should be of GREATEST concern to an IS auditor?

- ☐ The virtual machine management server
- ☐ The virtual application server
- ☐ The virtual antivirus server
- ☐ The virtual file server

Question 294

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 295

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 296

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 297

Which of the following is MOST directly affected by network performance monitoring tools?

- ☐ Integrity
- ☐ Availability
- ☐ Completeness
- ☐ Confidentiality

Question 298

Which of the following would MOST effectively minimize the risk of unauthorized online banking customer transactions due to phishing?

- ☐ A strong authentication mechanism
- ☐ Clear audit trails
- ☐ An intrusion prevention system (IPS)
- ☐ A customer awareness program

Question 299

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.

Question 300

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 301

Which of the following is the GREATEST cause for concern when an organization is planning to migrate business-critical applications to the cloud using a Platform as a Service (PaaS) model?

- ☐ The organization will not manage operating system patches.
- ☐ The cloud provider does not offer regional redundancy.
- ☐ Compliance requirements are not being validated.
- ☐ Application data will not be encrypted at rest.

Question 302

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 303

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 304

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

Question 305

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 306

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 307

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

Question 308

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 309

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 310

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 311

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 312

An IS auditor is performing a follow-up audit for findings identified in an organization's user provisioning process. Which of the following is the MOST appropriate population to sample from when testing for remediation?

- ☐ All users who have followed user provisioning processes provided by management
- ☐ All users provisioned after the finding was originally identified
- ☐ All users provisioned after management resolved the audit issue
- ☐ All users provisioned after the final audit report was issued

Question 313

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

Question 314

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 imaging process was used to obtain a copy of the data from each computer.
- ☐ Audit was only involved during extraction of the information.

Question 315

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 316

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 317

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 318

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 319

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 320

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 321

The drives of a tile server are backed up at a hot site. Which of the following is the BEST way to duplicate the files stored on the server for forensic analysis?

- ☐ Capture a bit-by-bit image of the file server's drives.
- ☐ Run forensic analysis software on the backup drive.
- ☐ Create a logical copy of the file server's drives.
- ☐ Replicate the server's volatile data to another drive.

Question 322

The technique used to ensure security in virtual private networks (VPNs) is:

- ☐ encapsulation.
- ☐ wrapping.
- ☐ transform.
- ☐ encryption

Question 323

An IS audit concludes that entry to the computer room is appropriately controlled. The audit result provides assurance that:

- ☐ the theft of hardware is prevented.
- ☐ the confidentiality of data is protected.
- ☐ data leakage is prevented.
- ☐ unauthorized access is prevented.

Question 324

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.

Question 325

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 326

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.

Question 327

As part of a quality assurance initiative, an organization has engaged an external auditor to evaluate the internal IS audit function. Which of the following observations should be of MOST concern?

- ☐ Audit reports are not approved by the audit committee.
- ☐ Audit reports do not state they are conducted in accordance with industry standards.
- ☐ The audit team is not sufficiently leveraging data analytics.
- ☐ Audit engagements are not risk-based.

Question 328

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.

Question 329

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 330

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.

Question 331

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 332

Total billing amounts on invoices are automatically transferred to an organization's account ledger weekly. During an IS audit, the auditor discovers that one week's billing is missing from the ledger. Which of the following areas should the auditor examine FIRST?

- ☐ Annual reconciliations
- ☐ Change management
- ☐ Batch processing controls
- ☐ Module access rights

Question 333

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 334

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 335

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 336

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 337

Which of the following will BEST protect an organization against spear phishing?

- ☐ Email content filtering
- ☐ Acceptable use policy
- ☐ End-user training
- ☐ Antivirus software

Question 338

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 339

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 340

Which of the following is the MOST reliable sender authentication method?

- ☐ Digital signatures
- ☐ Asymmetric cryptography
- ☐ Digital certificates
- ☐ Message authentication code

Question 341

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

Question 342

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 hop 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

Question 343

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 344

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 345

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 346

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 347

Which of the following features can be provided only by asymmetric encryption?

- ☐ 128-bit key length
- ☐ Information privacy
- ☐ Data confidentiality
- ☐ Nonrepudiation

Question 348

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 349

An external security audit risk has reported multiple instances of control noncompliance. Which of the following would be MOST important 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 350

Which of the following process consist of identification and selection of data from the imaged data set in computer forensics?

- ☐ Investigation
- ☐ Interrogation
- ☐ Reporting
- ☐ Extraction

Question 351

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 352

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

Question 353

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 354

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 355

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 356

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

Question 357

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 358

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 359

Network IDS&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 360

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 361

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 362

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 363

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 364

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

Question 365

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 366

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 367

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.

Question 368

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 369

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.

Question 370

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 371

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 372

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 373

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 374

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 375

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 376

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 377

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 378

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 379

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.

Question 380

After discussing findings with an auditee, an IS auditor is required to obtain approval of the report from the CEO before issuing it to the audit committee. This requirement PRIMARILY affects the IS auditor's:

- ☐ judgment
- ☐ effectiveness
- ☐ independence
- ☐ integrity

Question 381

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 382

Which of the following is often used as a detection and deterrent control against Internet attacks?

- ☐ Honeypots
- ☐ CCTV
- ☐ VPN
- ☐ VLAN

Question 383

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 384

An IS auditor performs a follow-up audit and learns the approach taken by the auditee to fix the findings differs from the agreed-upon approach confirmed during the last audit. Which of the following should be the auditor's NEXT course of action?

- ☐ Inform senior management of the change in approach.
- ☐ Conduct a risk analysis incorporating the change.
- ☐ Report results of the follow-up to the audit committee.
- ☐ Evaluate the appropriateness of the remedial action taken.

Question 385

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 386

Which of the following is the BEST reason to utilize blockchain technology to record accounting transactions?

- ☐ Integrity of records
- ☐ Confidentiality of records
- ☐ Availability of records
- ☐ Distribution of records

Question 387

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 388

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 389

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 390

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 391

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 392

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 393

Which of the following is the MAIN advantage of using one-time passwords?

- ☐ They are suitable for e-commerce authentication.
- ☐ Passwords are hardware/software generated.
- ☐ An intercepted password would be of no use.
- ☐ The user does not need to remember passwords.

Question 394

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 395

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 396

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 397

Which of the following is the PRIMARY responsibility of an organization's IT steering committee?

- ☐ Reporting on key performance measures
- ☐ Communicating strategic goals to IT project teams
- ☐ Conducting peer reviews of other organizations
- ☐ Identifying new technological threats

Question 398

An IS auditor is auditing the infrastructure of an organization that hosts critical applications withing a virtual environment. Which of the following is MOST important for the auditor to focus on?

- ☐ The ability to copy and move virtual machines in real time
- ☐ The controls in place to prevent compromise of the host
- ☐ Issues arising from system management of a virtual infrastructure
- ☐ Qualifications of employees managing the applications

Question 399

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

Question 400

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

Question 401

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 402

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 403

Library control software restricts source code to:

- ☐ Read-only access
- ☐ Write-only access
- ☐ Full access
- ☐ Read-write access

Question 404

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 405

Which of the following provides the MOST relevant information for proactively strengthening security settings?

- ☐ Bastion host
- ☐ Intrusion detection system
- ☐ Honeypot
- ☐ Intrusion prevention system

Question 406

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 407

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 408

The security level of a private key system depends on the number of:

- ☐ encryption key bits.
- ☐ messages sent.
- ☐ keys.
- ☐ channels used.

Question 409

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 410

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 411

Which of the following attack includes social engineering, link manipulation or web site forgery techniques?

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

Question 412

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 413

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 414

When creating a new risk management program, it is CRITICAL to consider:

- ☐ the risk appetite.
- ☐ compliance measures.
- ☐ risk mitigation techniques.
- ☐ resource utilization.

Question 415

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 416

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

Question 417

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 418

An organization is designing an application programming interface (API) for business-to-business data sharing with a vendor. Which of the following is the BEST way to reduce the potential risk of data leakage?

- ☐ Implement a policy to require data transfer over hypertext transfer protocol (HTTP)
- ☐ Implement the API on a secure server and encrypt traffic between both organizations
- ☐ Restrict the allowable number of API calls within a specified period
- ☐ Conduct an independent review of the application architecture and service level agreements (SLAs)

Question 419

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 420

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 421

Which of the following will prevent dangling tuples in a database?

- ☐ Cyclic integrity
- ☐ Domain integrity
- ☐ Relational integrity
- ☐ Referential integrity

Question 422

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 423

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 424

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 425

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

Question 426

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 427

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 428

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 429

A maturity model can be used to aid the implementation of IT governance by identifying:

- ☐ critical success factors (CSF)
- ☐ performance drivers
- ☐ improvement opportunities
- ☐ accountabilities

Question 430

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 431

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 432

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.

Question 433

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 434

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 435

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 436

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 437

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 438

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 439

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.

Question 440

Which of the following would a digital signature MOST likely prevent?

- ☐ Corruption
- ☐ Unauthorized change
- ☐ Repudiation
- ☐ Disclosure

Question 441

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 442

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 443

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 444

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 445

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 446

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 447

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 448

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.

Question 449

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

Question 450

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 451

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 452

The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a(n):

- ☐ Implementor
- ☐ Facilitator
- ☐ Developer
- ☐ Sponsor

Question 453

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

Question 454

Iptables is based on which of the following frameworks?

- ☐ Netfilter
- ☐ NetDoom
- ☐ NetCheck
- ☐ NetSecure
- ☐ None of the choices.

Question 455

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 456

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 457

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%.

Question 458

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 459

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 460

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.

Question 461

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 462

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 463

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 464

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 465

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.

Question 466

Statistical sampling is NOT based on which of the following audit sample techniques?

- ☐ Haphazard Sampling
- ☐ Random Sampling
- ☐ Cell Sampling
- ☐ Fixed interval sampling

Question 467

The use of a GANTT chart can:

- ☐ aid in scheduling project tasks.
- ☐ determine project checkpoints.
- ☐ ensure documentation standards.
- ☐ direct the post-implementation review.

Question 468

Which of the following is the MOST important feature of access control software?

- ☐ Authentication
- ☐ Violation reporting
- ☐ Nonrepudiation
- ☐ Identification

Question 469

When reviewing an organization's data protection practices, an IS auditor should be MOST concerned with a lack of:

- ☐ a security team.
- ☐ data classification.
- ☐ training manuals.
- ☐ data encryption.

Question 470

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 471

Which of the following is MOST critical during the business impact assessment phase of business continuity planning?

- ☐ End-user involvement
- ☐ Senior management involvement
- ☐ Security administration involvement
- ☐ IS auditing involvement

Question 472

An IS auditor is performing a follow-up audit and notes that some critical deficiencies have not been addressed. The auditor's BEST course of action is to:

- ☐ assess the impact of not addressing deficiencies.
- ☐ document management's reasons for not addressing deficiencies.
- ☐ postpone the audit until the deficiencies are addressed.
- ☐ provide new recommendations.

Question 473

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 474

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 475

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 476

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 477

An IS auditor concludes that an organization has a quality security policy. Which of the following is MOST important to determine next? The policy must be:

- ☐ updated frequently.
- ☐ developed by process owners.
- ☐ based on industry standards.
- ☐ well understood by all employees.

Question 478

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 479

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 480

Which of the following activities should an IS auditor perform FIRST during an external network security assessment?

- ☐ Exploitation
- ☐ Enumeration
- ☐ Vulnerability scanning
- ☐ Reconnaissance

Question 481

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 482

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 483

An organization plans to allow third parties to collect customer personal data from a retail loyalty platform via an application programming interface (API). Which of the following should be the PRIMARY consideration when designing this API?

- ☐ Data governance policies
- ☐ System resilience
- ☐ Regulatory compliance
- ☐ Data availability

Question 484

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

Question 485

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 486

Which of the following should be reviewed as part of a data integrity test?

- ☐ Completeness
- ☐ Confidentiality
- ☐ Data backup
- ☐ Redundancy

Question 487

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 488

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 489

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 490

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 491

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.

Question 492

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 493

Which of the following types of transmission media provide the BEST security against unauthorized access?

- ☐ Copper wire
- ☐ Twisted pair
- ☐ Fiberoptic cables
- ☐ Coaxial cables

Question 494

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 495

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 496

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

Question 497

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

Question 498

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

Question 499

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

Question 500

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 501

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

Question 502

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

Question 503

Which of the following would provide the MOST important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program?

- ☐ Policies including BYOD acceptable use statements
- ☐ Results of a risk assessment
- ☐ An inventory of personal devices to be connected to the corporate network
- ☐ Findings from prior audits

Question 504

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.

Question 505

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 506

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 507

Which of the following would provide the BEST evidence for an IS auditor to determine whether segregation of duties is in place?

- ☐ A review of the organizational chart
- ☐ A review of personnel files
- ☐ An analysis of user access requests
- ☐ A walk-through of job functions

Question 508

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 509

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 510

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 511

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 512

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

Question 513

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 514

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 515

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 516

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 517

Which of the following results in a denial-of-service attack?

- ☐ Brute force attack
- ☐ Ping of death
- ☐ Leapfrog attack
- ☐ Negative acknowledgement (NAK) attack

Question 518

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 519

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 520

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 521

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 522

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 523

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 524

Which of the following BEST supports an organization's planning efforts for investments in IT initiatives?

- ☐ Capability maturity model
- ☐ Enterprise architecture
- ☐ Agile project management
- ☐ Continuous gap assessment

Question 525

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 526

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 527

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.

Question 528

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 529

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 530

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 531

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 532

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 533

Who should be responsible for network security operations?

- ☐ Business unit managers
- ☐ Security administrators
- ☐ Network administrators
- ☐ IS auditors

Question 534

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 535

A new regulation requires organizations to report significant security incidents to the regulator within 24 hours of identification. Which of the following is the IS auditor's BEST recommendation to facilitate compliance with the regulation?

- ☐ Include the requirement in the incident management response plan.
- ☐ Establish key performance indicators (KPIs) for timely identification of security incidents.
- ☐ Enhance the alert functionality of the intrusion detection system (IDS).
- ☐ Engage an external security incident response expert for incident handling.

Question 536

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 537

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 538

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 539

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

Question 540

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 541

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 542

Which of the following is the BEST way to ensure enterprise architectural objectives are aligned with business and technology objectives?

- ☐ Identify dependencies between current and future state technologies.
- ☐ Optimize technology investments with business requirements.
- ☐ Adopt industry-approved architecture standards and best practices.
- ☐ Identify business stakeholder responsibilities for IT projects.

Question 543

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 544

An organization has outsourced the development of a core application. However, the organization plans to bring the support and future maintenance of the application back in-house. Which of the following findings should be the IS auditor's GREATEST concern?

- ☐ A training plan for business users has not been developed.
- ☐ The cost of outsourcing is lower than in-house development.
- ☐ The vendor development team is located overseas.
- ☐ The data model is not clearly documented.

Question 545

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

Question 546

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

Question 547

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 548

Who is ultimately responsible and accountable for reviewing user access to systems?

- ☐ Systems security administrators
- ☐ Data custodians
- ☐ Data owners
- ☐ Information systems auditors

Question 549

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 550

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 551

An IS auditor discovers that management has created a system interface to receive financial data and store it in a data warehouse. Which of the following provides the BEST assurance that data in the data warehouse is accurate?

- ☐ Established risk management processes
- ☐ A documented change management process
- ☐ Management access reviews
- ☐ Management reconciliations

Question 552

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 553

Which of the following is not a good tactic to use against hackers?

- ☐ Enticement
- ☐ Entrapment

Question 554

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).

Question 555

Which of the following stakeholders should be PRIMARILY responsible for developing, implementing, and monitoring metrics for security activities?

- ☐ Chief technology officer
- ☐ Security incident response team
- ☐ Chief information security officer
- ☐ IT steering committee

Question 556

Which of the following is the PRIMARY objective of using a capability maturity model as a tool to communicate audit results to senior management?

- ☐ To evaluate management's action plan
- ☐ To confirm audit findings
- ☐ To illustrate improvement opportunities
- ☐ To prioritize remediation efforts

Question 557

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 558

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 559

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 560

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 561

What is the primary security concern for EDI environments?

- ☐ Transaction authentication
- ☐ Transaction completeness
- ☐ Transaction accuracy
- ☐ Transaction authorization

Question 562

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 563

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.

Question 564

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 565

Which of the following should be the FIRST step in the incident response process for a suspected breach?

- ☐ Inform potentially affected customers of the security breach.
- ☐ Notify business management of the security breach.
- ☐ Engage a third party to independently evaluate the alerted breach.
- ☐ Research the validity of the alerted breach.

Question 566

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

- ☐ HTTP
- ☐ FTP
- ☐ NTP
- ☐ TCP

Question 567

The PRIMARY objective of parallel testing an application is to confirm that:

- ☐ the results of calculations in the new system are as accurate as the old system.
- ☐ system response times in the new system are better than the old system.
- ☐ the costs of running the new system are the same as running the old system.
- ☐ new system processing times are similar to those of the old system.

Question 568

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 569

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 570

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

Question 571

A financial institution suspects that a manager has been crediting customer accounts without authorization. Which of the following is the MOST effective method to validate this concern?

- ☐ Variable sampling
- ☐ Stop or go sampling
- ☐ Attribute sampling
- ☐ Discovery sampling

Question 572

An organization is considering the implementation of a business application. The IS auditor should FIRST ensure that:

- ☐ user requirements are used to select the vendor.
- ☐ an approved business case is in place.
- ☐ users are represented on the project management team.
- ☐ security requirements are specified.

Question 573

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

Question 574

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

Question 575

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 576

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 577

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 578

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 579

Effective IT governance will ensure that the IT plan is consistent with the organization's:

- ☐ business plan.
- ☐ audit plan.
- ☐ security plan.
- ☐ investment plan.

Question 580

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 581

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

Question 582

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

Question 583

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

Question 584

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 585

TEMPEST is a hardware for which of the following purposes?

- ☐ Eavedropping
- ☐ Social engineering
- ☐ Virus scanning
- ☐ Firewalling
- ☐ None of the choices.

Question 586

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 587

Which of the following is the PRIMARY role of a data custodian?

- ☐ Processing information
- ☐ Securing information
- ☐ Classifying information
- ☐ Validating information

Question 588

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.

Question 589

When reviewing a contract for a disaster recovery hot site, which of the following would be the MOST significant omission?

- ☐ Audit rights
- ☐ Testing procedures
- ☐ Exposure coverage
- ☐ Equipment provided

Question 590

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 591

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.

Question 592

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.

Question 593

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 594

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 595

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 596

Which of the following protocol does NOT work at Network interface layer in TCP/IP model?

- ☐ ICMP
- ☐ DNS
- ☐ ARP
- ☐ Internet protocol

Question 597

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 598

An IS auditor is reviewing a sample of production incidents and notes that root cause analysis is not being performed. Which of the following is the GREATEST risk associated with this finding?

- ☐ Future incidents may not be resolved in a timely manner.
- ☐ Future incidents may be prioritized inappropriately.
- ☐ The same incident may occur in the future.
- ☐ Service level agreements (SLAs) may not be met.

Question 599

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 600

Which of the following should be reviewed FIRST when assessing the effectiveness of an organization's network security procedures and controls?

- ☐ Data recovery capability
- ☐ Inventory of authorized devices
- ☐ Vulnerability remediation
- ☐ Malware defenses

Question 601

A trojan horse simply cannot operate autonomously.

- ☐ true
- ☐ false

Question 602

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 603

Which of the following level in CMMI model focuses on process innovation and continuous optimization?

- ☐ Level 4
- ☐ Level 5
- ☐ Level 3
- ☐ Level 2

Question 604

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 605

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 606

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 607

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 608

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

Question 609

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 610

Which of the following is the MOST critical characteristic of a biometric system?

- ☐ Registration time
- ☐ Throughput rate
- ☐ Accuracy
- ☐ Ease of use

Question 611

Which of the following would MOST effectively detect a condition where an employee assigned to an operations role could perform system administrator functions?

- ☐ User access review
- ☐ System review
- ☐ Business process review
- ☐ Entitlement design review

Question 612

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 613

Which of the following should be of MOST concern to an IS auditor evaluating a forensics program?

- ☐ Forensic images are stored on removable media with encryption.
- ☐ Forensic images are only stored for involuntarily terminated employees.
- ☐ Forensic images are only maintained for 12 months.
- ☐ Forensic images are stored on shared disks.

Question 614

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 615

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 616

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 617

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 618

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 619

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 620

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 621

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 622

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 623

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 624

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 625

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 626

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.

Question 627

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 628

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.

Question 629

Which cloud deployment model is MOST likely to be limited in scalability?

- ☐ Public
- ☐ Private
- ☐ Hybrid
- ☐ Community

Question 630

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 631

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 632

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 633

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 634

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 635

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

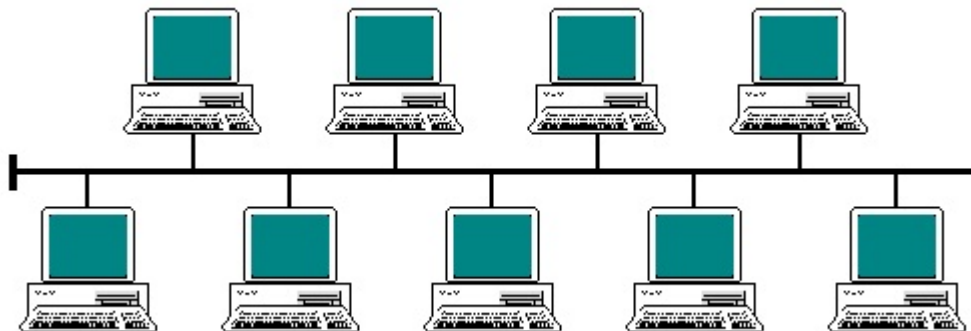
Question 636

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

Question 637

Identify the LAN topology from below diagram presented below:



bus topology

- ☐ Bus
- ☐ Star
- ☐ Ring
- ☐ Mesh

Question 638

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 639

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

Question 640

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 641

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 642

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 643

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 644

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 645

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 646

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 647

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 648

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 649

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 650

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 651

An IS auditor observed that most users do not comply with physical access controls. The business manager has explained that the control design is inefficient. What is the auditor's BEST course of action?

- ☐ Recommend changing the access control process to increase efficiency.
- ☐ Identify the impact of control failure and report the finding with a risk rating.
- ☐ Redesign and retest the physical access control.
- ☐ Work with management to design and implement a better control.

Question 652

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

Question 653

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 654

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 655

An IS auditor suspects an organization's computer may have been used to commit a crime. Which of the following is the auditor's BEST course of action?

- ☐ Examine the computer to search for evidence supporting the suspicions.
- ☐ Notify local law enforcement of the potential crime before further investigation.
- ☐ Contact the incident response team to conduct an investigation.
- ☐ Advise management of the crime after the investigation.

Question 656

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 657

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 658

Using swipe cards to limit employee access to restricted areas requires implementing which additional control?

- ☐ Physical sign-in of all employees for access to restricted areas
- ☐ Initial escort of all new hires by a current employee
- ☐ Periodic review of access profiles by management
- ☐ Employee-access criteria determined on the basis of IS experience

Question 659

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 660

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 661

An organization has outsourced many application development activities to a third party that uses contract programmers extensively. Which of the following would provide the BEST assurance 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 662

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 663

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)

Question 664

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 665

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

Question 666

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 667

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.

Question 668

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 669

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 670

Which of the following would be the MOST effective method for detecting duplicate payments?

- ☐ Enciphering and deciphering the message digest
- ☐ Reviewing sequence numbers and time stamps for each transaction
- ☐ Assessing payment history for reasonableness and approval
- ☐ Using a cryptographic hashing algorithm

Question 671

When initiating an IT project, which of the following should be completed FIRST?

- ☐ Project plan
- ☐ Request for proposal
- ☐ Feasibility study
- ☐ Requirements definition

Question 672

Which of the following biometrics has the highest reliability and lowest false-acceptance rate (FAR)?

- ☐ Palm scan
- ☐ Face recognition
- ☐ Retina scan
- ☐ Hand geometry

Question 673

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 674

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 675

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 676

The MOST important objective of security awareness training for business staff is to:

- ☐ understand intrusion methods
- ☐ reduce negative audit findings
- ☐ increase compliance
- ☐ modify behavior

Question 677

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 678

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 679

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 680

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 681

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 682

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 683

Which of the following sampling methods is MOST useful when testing for compliance?

- ☐ Attribute sampling
- ☐ Variable sampling
- ☐ Stratified mean per unit
- ☐ Difference estimation

Question 684

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 685

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.

Question 686

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 687

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

- ☐ DNS
- ☐ FTP
- ☐ SSH
- ☐ SMTP

Question 688

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 689

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 690

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

Question 691

During what process should router access control lists be reviewed?

- ☐ Environmental review
- ☐ Network security review
- ☐ Business continuity review
- ☐ Data integrity review

Question 692

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.

Question 693

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

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

Question 694

An IS auditor finds that a required security patch was not installed on a critical server for more than 6 months. The NEXT course of action should be to:

- ☐ determine the root cause of the delay.
- ☐ review patch management procedures.
- ☐ request the patch be installed as soon as possible.
- ☐ notify senior management of audit findings.

Question 695

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.

Question 696

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 697

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

Question 698

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.

Question 699

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 700

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 701

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 702

Which of the following would be of GREATEST concern to an IS auditor when auditing a small organization's purchasing department?

- ☐ The organization lacks a purchasing officer with experience in purchasing activities.
- ☐ Purchases can be approved after expenses have already been incurred.
- ☐ Some members of the department can request and approve payments for purchase requests.
- ☐ Purchasing procedures and processes have not been updated during the past two years.

Question 703

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 704

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 705

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 706

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 707

Which of the following provides an IS auditor with the BEST evidence that an organization's information security program is aligned to business objectives?

- ☐ Balanced scorecard
- ☐ Risk assessment results
- ☐ Business impact analysis (BIA)
- ☐ Cost-benefit analysis

Question 708

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 709

An IS auditor should be aware of various analysis models used by data architecture. Which of the following analysis models depict data entities and how they relate?

- ☐ Context Diagrams
- ☐ Activity Diagrams
- ☐ Swim-lane diagrams
- ☐ Entity relationship diagrams

Question 710

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 711

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 712

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 713

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 714

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 715

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 716

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 717

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 718

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 719

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

Question 720

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 721

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 722

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 723

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

Question 724

Which of the following step of PDCA implement the plan, execute the process and make product?

- ☐ Plan
- ☐ Do
- ☐ Check
- ☐ Act

Question 725

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 726

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 727

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 728

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

Question 729

Which of the following is the GREATEST risk of using a reciprocal site for disaster recovery?

- ☐ Inability to utilize the site when required
- ☐ Inability to test the recovery plans onsite
- ☐ Mismatched organizational security policies
- ☐ Equipment compatibility issues at the site

Question 730

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 731

Which of the following step of PDCA study the actual result and compares it against the expected result?

- ☐ Plan
- ☐ Do
- ☐ Check
- ☐ Act

Question 732

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 733

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 734

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.

Question 735

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 736

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 737

During a review of operations, it is noted that during a batch update, an error was detected and the database initiated a roll-back. An IT operator stopped the roll-back and re-initiated the update. What should the operator have done PRIOR to re-initiating the update?

- ☐ Determined the cause of the error
- ☐ Obtained approval before re-initiating the update
- ☐ Allowed the roll-back to complete
- ☐ Scheduled the roll-back for a later time

Question 738

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 739

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

Question 740

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)

Question 741

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

Question 742

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

Question 743

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 744

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

Question 745

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 746

Which of the following control fixes a component or system after an incident has occurred?

- ☐ Deterrent
- ☐ Preventive
- ☐ Corrective
- ☐ Recovery

Question 747

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.

Question 748

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 749

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 750

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 751

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.

Question 752

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

Question 753

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

Question 754

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.

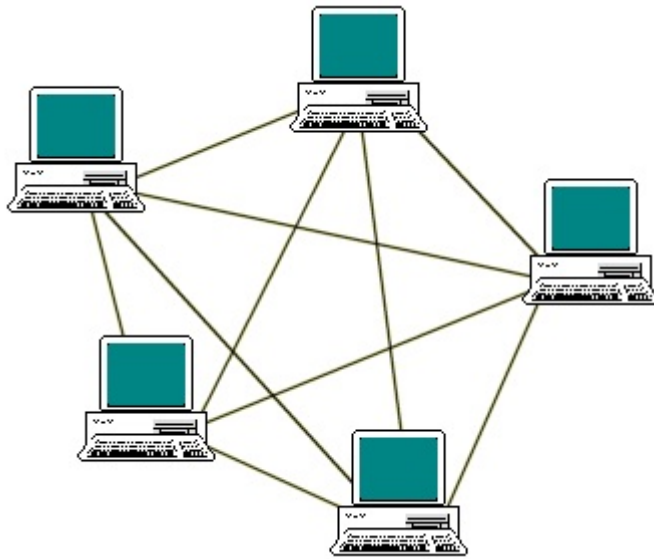
Question 755

Which of the following BEST enables an audit department to improve the quality of work performed by its auditors?

- ☐ Implementing global quality standards
- ☐ Funding additional resources for audit work
- ☐ Using audit-related data analytics tools
- ☐ Implementing peer review of audit work

Question 756

Identify the network topology from below diagram presented below:



Network Topology

- ☐ Bus
- ☐ Star
- ☐ Ring
- ☐ Mesh

Question 757

In a RACI model, which of the following roles must be assigned to only one individual?

- ☐ Responsible
- ☐ Informed
- ☐ Consulted
- ☐ Accountable

Question 758

_____ (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

Question 759

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

Question 760

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

Question 761

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 762

Which of the following is MOST important for an IS auditor to understand when planning an IS audit?

- ☐ Inherent risk of auditable areas
- ☐ Management focus on particular operations
- ☐ Number of high-risk auditable processes
- ☐ Availability of IS audit resources

Question 763

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 764

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 765

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 766

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 767

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 768

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 769

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 770

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 771

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 772

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 773

Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

- ☐ Response
- ☐ Correction
- ☐ Detection
- ☐ Monitoring

Question 774

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 775

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 776

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 777

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 778

Which of the following is the BEST way to transmit documents classified as confidential over the Internet?

- ☐ Hashing the document contents and destroying the hash value
- ☐ Sending documents as multiple packets over different network routes
- ☐ Converting documents to proprietary format before transmission
- ☐ Using a virtual private network (VPN)

Question 779

The development of an IS security policy is ultimately the responsibility of the:

- ☐ IS department.
- ☐ security committee.
- ☐ security administrator.
- ☐ board of directors.

Question 780

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 781

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 782

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 783

During a follow-up audit for a finding related to change management, an IS auditor notes that one of the changes sampled was an emergency change, which follows a different process. Which of the following is the auditor's BEST course of action?

- ☐ Mark the sample as not applicable in the workpaper and move on to testing the next sample.
- ☐ Select a replacement change for testing.
- ☐ Obtain evidence that the change was approved.
- ☐ Note the sample as a deviation and leave the finding open in the audit tracking log.

Question 784

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).

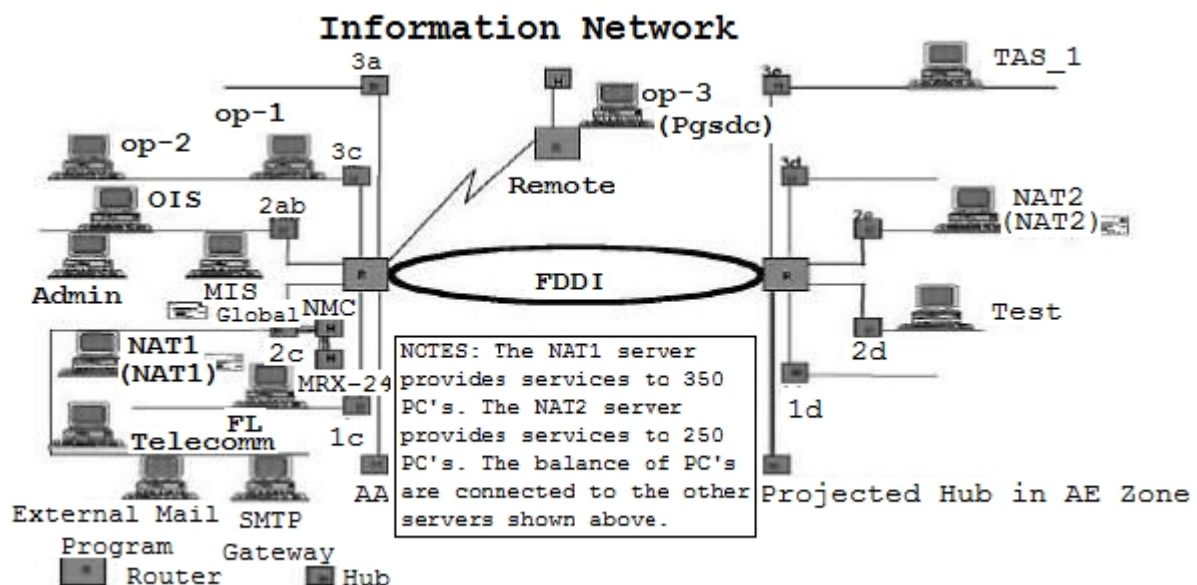
Question 785

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 786

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 787

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 788

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 789

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 790

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.

Question 791

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 792

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

Question 793

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 794

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 795

For which of the following applications would rapid recovery be MOST crucial?

- ☐ Point-of-sale system
- ☐ Corporate planning
- ☐ Regulatory reporting
- ☐ Departmental chargeback

Question 796

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 797

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 798

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 799

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.

Question 800

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
- ☐ Filing an insurance claim

Question 801

What can be used to gather evidence of network attacks?

- ☐ Access control lists (ACL)
- ☐ Intrusion-detection systems (IDS)
- ☐ Syslog reporting
- ☐ Antivirus programs

Question 802

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 803

What supports data transmission through split cable facilities or duplicate cable facilities?

- ☐ Diverse routing
- ☐ Dual routing
- ☐ Alternate routing
- ☐ Redundant routing

Question 804

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 805

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 806

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.

Question 807

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.

Question 808

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 809

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 810

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 811

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

Question 812

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 813

An IS auditor is evaluating the risk associated with moving from one database management system to another. Which of the following would be MOST helpful to ensure the integrity of the system throughout the change?

- ☐ Preserving the same data structure
- ☐ Preserving the same data classifications
- ☐ Preserving the same data interfaces
- ☐ Preserving the same data inputs

Question 814

What is the BEST way to control updates to the vendor master file in an accounts payable system?

- ☐ Using prenumbered and authorized request forms
- ☐ Having only one person updating the master file
- ☐ Periodically reviewing the entire vendor master file
- ☐ Comparing updates against authorization

Question 815

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 816

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 817

What is often assured through table link verification and reference checks?

- ☐ Database integrity
- ☐ Database synchronization
- ☐ Database normalcy
- ☐ Database accuracy

Question 818

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 819

Which of the following is the BEST point in time to conduct a post-implementation review (PIR)?

- ☐ After a full processing cycle
- ☐ Immediately after deployment
- ☐ To coincide with annual PIR cycle
- ☐ Six weeks after deployment

Question 820

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 821

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

Question 822

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 823

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 824

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 825

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.

Question 826

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 827

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 828

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 829

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

Question 830

Which of the following threats is MOST effectively controlled by a firewall?

- ☐ Network congestion
- ☐ Denial of service (DoS) attack
- ☐ Network sniffing
- ☐ Password cracking

Question 831

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

Question 832

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

Question 833

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

Question 834

An organization with high availability resource requirements is selecting a provider for cloud computing. Which of the following would cause the GREATEST concern to an IS auditor? The provider:

- ☐ is not internationally certified for high availability.
- ☐ does not store backup media offsite.
- ☐ deploys patches automatically without testing.
- ☐ hosts systems for the organization's competitor.

Question 835

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 836

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

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

Question 837

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 838

Which of the following BEST helps to ensure data integrity across system interfaces?

- ☐ Environment segregation
- ☐ System backups
- ☐ Reconciliations
- ☐ Access controls

Question 839

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 840

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

Question 841

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 842

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 843

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 844

Which of the following BEST helps to ensure that all relevant data within an organization is added to a data warehouse during deployment?

- ☐ Data migration
- ☐ Architecture review
- ☐ Project planning
- ☐ Data mining

Question 845

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 846

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 847

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

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

Question 848

An IS auditor notes that a number of application plug-ins currently in use are no longer supported. Which of the following is the auditor's BEST recommendation to management?

- ☐ Implement role-based access controls.
- ☐ Conduct a vulnerability assessment to determine exposure.
- ☐ Review content backup and archiving procedures.
- ☐ Review on-boarding and off-boarding processes.

Question 849

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

Question 850

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.

Question 851

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 852

Which of the following provides the BEST evidence that network filters are functioning?

- ☐ Reviewing network configuration rules
- ☐ Reviewing network filtering policy
- ☐ Performing network port scans
- ☐ Analyzing network performance

Question 853

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 854

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 855

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 856

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 857

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 858

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 859

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 860

When determining which IS audits to conduct during the upcoming year, internal audit has received a request from management for multiple audits of the contract division due to fraud findings during the prior year. Which of the following is the BEST basis for selecting the audits to be performed?

- ☐ Select audits based on an organizational risk assessment.
- ☐ Select audits based on collusion risk.
- ☐ Select audits based on the skill sets of the IS auditors.
- ☐ Select audits based on management's suggestion.

Question 861

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 862

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

Question 863

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

Question 864

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 865

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.

Question 866

Which of the following transmission media is MOST difficult to tap?

- ☐ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Radio System

Question 867

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 868

An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

- ☐ True
- ☐ False

Question 869

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 870

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 871

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 872

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 873

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 874

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

Question 875

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 876

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

Question 877

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 878

Which of the following attack involves slicing small amount of money from a computerized transaction or account?

- ☐ Eavesdropping
- ☐ Traffic Analysis
- ☐ Salami
- ☐ Masquerading

Question 879

Squid is an example of:

- ☐ IDS
- ☐ caching proxy
- ☐ security proxy
- ☐ connection proxy
- ☐ dialer
- ☐ None of the choices.

Question 880

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

Question 881

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

Question 882

Which of the following will MOST likely compromise the control provided by a digital signature created using RSA encryption?

- ☐ Deciphering the receiver's public key
- ☐ Obtaining the sender's private key
- ☐ Altering the plaintext message
- ☐ Reversing the hash function using the digest

Question 883

An organization migrated most of its physical servers to virtual ones in its own data center. Which of the following should be of GREATEST concern to an IS auditor reviewing the virtual environment?

- ☐ Hypervisor access control lists are outdated.
- ☐ The configuration management database (CMDB) does not include all virtual machines.
- ☐ Hypervisors have not been updated with the most recent patches.
- ☐ Virtual machine deployments are done without following an approved template.

Question 884

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 885

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 886

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.

Question 887

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 888

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.

Question 889

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 890

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 891

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

Question 892

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 893

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

Question 894

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 895

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 896

Which of the following is the GREATEST advantage of implementing an IT enterprise architecture framework within an organization?

- ☐ It helps to identify security issues in systems across the organization.
- ☐ It better equips an organization to adopt innovative and emerging technologies.
- ☐ It reduces the overlap of infrastructure technologies within the organization.
- ☐ It improves the organization's ability to meet service level agreements (SLAs).

Question 897

Who is primarily responsible for storing and safeguarding the data?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Steward
- ☐ Security Administrator

Question 898

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 899

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.

Question 900

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 901

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 902

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 903

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 904

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 905

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 906

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.

Question 907

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 908

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 909

During a post-incident review of a security breach, what type of analysis should an IS auditor expect to be performed by the organization's information security team?

- ☐ Gap analysis
- ☐ Business impact analysis (BIA)
- ☐ Qualitative risk analysis
- ☐ Root cause analysis

Question 910

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

Question 911

Which of the following is a rewrite of ipfwadm?

- ☐ ipchains
- ☐ iptables
- ☐ Netfilter
- ☐ ipcook
- ☐ None of the choices.

Question 912

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 913

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

Question 914

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 915

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 916

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 917

Which of the following is a benefit of requiring management to issue a report to stakeholders regarding the internal controls over IT?

- ☐ Transparency of IT costs
- ☐ Improved portfolio management
- ☐ Improved cost management
- ☐ Focus on IT governance

Question 918

Which of the following is an indication of possible hacker activity involving voice communications?

- ☐ A significant percentage of lines are busy during early morning and late afternoon hours.
- ☐ Outbound calls are found to significantly increase in frequency during non-business hours.
- ☐ Inbound calls experience significant fluctuations based on time-of-day and day-of-week.
- ☐ Direct inward system access (DISA) is found to be disabled on the company's exchange.

Question 919

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.

Question 920

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 921

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.

Question 922

Which of the following activities provides an IS auditor with the MOST insight regarding potential single person dependencies that might exist within the organization?

- ☐ Reviewing user activity logs
- ☐ Mapping IT processes to roles
- ☐ Reviewing vacation patterns
- ☐ Interviewing senior IT management

Question 923

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

Question 924

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 925

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 926

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 927

Which of the following term describes a failure of an electric utility company to supply power within acceptable range?

- ☐ Sag
- ☐ Blackout
- ☐ Brownout
- ☐ EMI

Question 928

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 929

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 930

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.

Question 931

The MAIN objective of incident management is to:

- ☐ have an external computer security incident response team assess damage.
- ☐ permit the incident to go on and follow the trail back to the beginning.
- ☐ test for readiness to respond when facing an incident.
- ☐ keep the business going while the response is occurring.

Question 932

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 933

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 934

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 935

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)

Question 936

Involvement of senior management is MOST important in the development of:

- ☐ strategic plans.
- ☐ IS policies.
- ☐ IS procedures.
- ☐ standards and guidelines.

Question 937

Which of the following acts as a decoy to detect active internet attacks?

- ☐ Honeypots
- ☐ Firewalls
- ☐ Trapdoors
- ☐ Traffic analysis

Question 938

Who is ultimately accountable for the development of an IS security policy?

- ☐ The board of directors
- ☐ Middle management
- ☐ Security administrators
- ☐ Network administrators

Question 939

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

Question 940

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 941

Which of the following should an IS auditor use when verifying a three-way match has occurred in an enterprise resource planning (ERP) system?

- ☐ Goods delivery notification
- ☐ Purchase requisition
- ☐ Bank confirmation
- ☐ Purchase order

Question 942

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.

Question 943

Which of the following testing approaches provides the GREATEST assurance that only approved systems development releases have been implemented in the production environment?

- ☐ Test whether a sample of approved developments have releases in production migration logs.
- ☐ Test whether a sample of developments in the systems development register have documented approvals.
- ☐ Test whether a sample of releases in production migration logs have corresponding approvals.
- ☐ Test whether a sample of releases followed the organization's segregation of duties access.

Question 944

An IS auditor is asked to provide feedback on the systems options analysis for a new project. The BEST course of action for the IS auditor would be to:

- ☐ identify the best alternative.
- ☐ request at least one other alternative.
- ☐ comment on the criteria used to assess the alternatives.
- ☐ retain comments as findings for the audit report.

Question 945

The PRIMARY reason for using digital signatures is to ensure data:

- ☐ confidentiality.
- ☐ integrity.
- ☐ availability.
- ☐ timeliness.

Question 946

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.

Question 947

Which of the following testing method examines internal structure or working of an application?

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

Question 948

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 949

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

Question 950

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 951

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 952

An accuracy measure for a biometric system is:

- ☐ system response time.
- ☐ registration time.
- ☐ input file size.
- ☐ false-acceptance rate.

Question 953

The BEST way to avoid session hijacking is to use:

- ☐ a reverse lookup
- ☐ a secure protocol
- ☐ a firewall
- ☐ strong password controls

Question 954

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 955

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

Question 956

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 957

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 958

Responsibility for the governance of IT should rest with the:

- ☐ IT strategy committee.
- ☐ chief information officer (CIO).
- ☐ audit committee.
- ☐ board of directors.

Question 959

In an online application, which of the following would provide the MOST information about the transaction audit trail?

- ☐ File layouts
- ☐ System/process flowchart
- ☐ Source code documentation
- ☐ Data architecture

Question 960

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 961

Which of the following is the BEST way to mitigate the impact of ransomware attacks?

- ☐ Backing up data frequently
- ☐ Invoking the disaster recovery plan (DRP)
- ☐ Requiring password changes for administrative accounts
- ☐ Paying the ransom

Question 962

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 963

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 964

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

Question 965

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 966

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 967

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 968

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.

Question 969

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 970

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 971

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 972

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

Question 973

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 974

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 975

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 976

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 977

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.

Question 978

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 979

Which of the following layer of an OSI model encapsulates packets into frames?

- ☐ Transport Layer
- ☐ Network Layer
- ☐ Data Link Layer
- ☐ Physical Layer
- ☐ .

Question 980

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 981

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 982

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 983

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

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

Question 984

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 985

Which of the following is a data validation edit and control?

- ☐ Hash totals
- ☐ Reasonableness checks
- ☐ Online access controls
- ☐ Before and after image reporting

Question 986

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 987

Which of the following audit assess accuracy of financial reporting?

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

Question 988

Phishing attack works primarily through:

- ☐ email and hyperlinks
- ☐ SMS
- ☐ chat
- ☐ email attachment
- ☐ news
- ☐ file download
- ☐ None of the choices.

Question 989

An IS auditor discovers an option in a database that allows the administrator to directly modify any table. This option is necessary to overcome bugs in the software, but is rarely used. Changes to tables are automatically logged. The IS auditor's FIRST action should be to:

- ☐ determine whether the log of changes to the tables is backed up.
- ☐ determine whether the audit trail is secured and reviewed.
- ☐ recommend that the option to directly modify the database be removed immediately.
- ☐ recommend that the system require two persons to be involved in modifying the database.

Question 990

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 991

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 992

Which of the following will provide the GREATEST assurance to IT management that a quality management system (QMS) is effective?

- ☐ A high percentage of incidents being quickly resolved
- ☐ A high percentage of stakeholders satisfied with the quality of IT
- ☐ A high percentage of IT processes reviewed by quality assurance
- ☐ A high percentage of IT employees attending quality training

Question 993

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 994

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 995

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

Question 996

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 997

Which of the following would provide the MOST useful input to IS audit management when developing an action plan for improving internal audit's performance?

- ☐ Feedback from departments that have participated in IS audits
- ☐ Industry benchmarking analysis
- ☐ An external quality assessment review
- ☐ Results train an improvement initiative overseen by executive management

Question 998

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 999

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 1000

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 1001

Which of the following provides for the GREATEST cost reduction in a large data center?

- ☐ Server consolidation
- ☐ Staff rotation
- ☐ Power conditioning
- ☐ Job-scheduling software

Question 1002

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 1003

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 acceptance 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 1004

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 1005

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 1006

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 1007

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

Question 1008

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

Question 1009

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 1010

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 number of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process

Question 1011

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).

Question 1012

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 1013

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 1014

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 1015

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.

Question 1016

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 1017

Which of the following is the PRIMARY reason for an IS auditor to map out the narrative of a business process?

- ☐ To verify the business process is as described in the engagement letter
- ☐ To identify the resources required to perform the audit
- ☐ To ensure alignment with organizational objectives
- ☐ To gain insight into potential risks

Question 1018

Which of the following is the BEST way for an IS auditor to assess the effectiveness of backup procedures?

- ☐ Review the backup schedule.
- ☐ Evaluate the latest data restore.
- ☐ Inspect backup logs.
- ☐ Interview the data owner.

Question 1019

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 1020

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 1021

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 1022

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 1023

Which of the following would provide management with the MOST reasonable assurance that a new data warehouse will meet the needs of the organization?

- ☐ Appointing data stewards to provide effective data governance
- ☐ Classifying data quality issues by the severity of their impact to the organization
- ☐ Integrating data requirements into the system development life cycle (SDLC)
- ☐ Facilitating effective communication between management and developers

Question 1024

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 1025

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 1026

Which of the following is BEST for providing uninterrupted services?

- ☐ Snapshots
- ☐ Differential backup
- ☐ Televaulting
- ☐ Mirroring

Question 1027

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.

Question 1028

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 1029

To protect information assets, which of the following should be done FIRST?

- ☐ Restrict access to data
- ☐ Encrypt data
- ☐ Classify data
- ☐ Back up data

Question 1030

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 1031

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 1032

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 1033

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 1034

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 1035

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 loss and processing interruption longer than 1 minute.

Question 1036

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 1037

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 1038

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 1039

Which of the following BEST limits the impact of server failures in a distributed environment?

- ☐ Redundant pathways
- ☐ Clustering
- ☐ Dial backup lines
- ☐ Standby power

Question 1040

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 1041

Which of the following is the BEST method to assess the adequacy of security awareness in an organization?

- ☐ Confirming a security awareness program exists
- ☐ Interviewing employees about security responsibility
- ☐ Administering security survey questionnaires
- ☐ Observing employee security behaviors

Question 1042

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

Question 1043

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 1044

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 1045

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 1046

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 1047

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 1048

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 1049

Which of the following is the BEST way for an IT forensics investigator to detect evidence of steganography?

- ☐ Compare file hashes between original and modified image files.
- ☐ Identify and analyze emergent properties within a file system's metadata.
- ☐ Recover deleted files from a suspected hard drive utilizing forensics software.
- ☐ Scan computer operating systems using administrative tools.

Question 1050

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 1051

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 1052

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 1053

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

Question 1054

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 1055

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.

Question 1056

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 1057

Which of the following would the IS auditor MOST likely review to determine whether modifications to the operating system parameters were authorized?

- ☐ Change control log
- ☐ System initialization logs
- ☐ Security system parameters
- ☐ Documentation of exit routines

Question 1058

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 1059

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

Question 1060

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 1061

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.

Question 1062

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 1063

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 1064

The Secure Sockets Layer (SSL) protocol addresses the confidentiality of a message through:

- ☐ symmetric encryption.
- ☐ message authentication code.
- ☐ hash function.
- ☐ digital signature certificates.

Question 1065

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

Question 1066

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 1067

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 1068

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 BEST course 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 1069

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

Question 1070

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 1071

A malicious code that changes itself with each file it infects is called a:

- ☐ logic bomb.
- ☐ stealth virus.
- ☐ trojan horse.
- ☐ polymorphic virus.

Question 1072

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 1073

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 1074

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 1075

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 1076

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 1077

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 1078

Minimum password length and password complexity verification are examples of:

- ☐ detection controls.
- ☐ control objectives.
- ☐ audit objectives.
- ☐ control procedures.

Question 1079

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 1080

Which of the following is the BEST indication of control maturity in an organization's systems development and implementation processes?

- ☐ Code changes are tested and deployed manually.
- ☐ Code changes are deployed to a test server and then to production.
- ☐ Code changes are documented and approved.
- ☐ Code changes are tested and deployed through automation.

Question 1081

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 1082

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 1083

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

Question 1084

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 1085

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 1086

An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

- ☐ True
- ☐ False

Question 1087

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 1088

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

Question 1089

During the course of an audit, an IS auditor's organizational independence is impaired. The IS auditor should FIRST:

- ☐ inform audit management of the situation.
- ☐ inform senior management in writing and proceed with the audit.
- ☐ obtain the auditee's approval before continuing the audit.
- ☐ proceed with the audit as planned after documenting the incident.

Question 1090

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 1091

Which of the following requires a consensus by key stakeholders on IT strategic goals and objectives?

- ☐ Balanced scorecards
- ☐ Benchmarking
- ☐ Maturity models
- ☐ Peer reviews

Question 1092

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.

Question 1093

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 1094

Meeting which of the following security objectives BEST ensures that information is protected against unauthorized modification?

- ☐ Availability
- ☐ Authenticity
- ☐ Confidentiality
- ☐ Integrity

Question 1095

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 1096

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 1097

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 1098

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 1099

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

Question 1100

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 1101

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 1102

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 1103

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 1104

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 1105

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 1106

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 1107

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 1108

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 1109

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 1110

Which of the following is the BEST indicator of a mature quality management system (QMS)?

- ☐ Projects are showing continuous improvement.
- ☐ Continuous improvement has been integrated into business processes.
- ☐ End users are satisfied with the outcome of IT projects.
- ☐ Most IT projects have been completed on time and within budget.

Question 1111

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 1112

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

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

Question 1113

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 1114

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

Question 1115

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 1116

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 1117

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 1118

Which of the following data validation control validates input data against predefined range values?

- ☐ Range Check
- ☐ Table lookups
- ☐ Existence check
- ☐ Reasonableness check

Question 1119

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 1120

Which of the following is the BEST way to help ensure new IT implementations align with enterprise architecture principles and requirements?

- ☐ Conduct enterprise architecture reviews as part of the change advisory board.
- ☐ Consider stakeholder concerns when defining the enterprise architecture.
- ☐ Document the security view as part of the enterprise architecture.
- ☐ Perform mandatory post-implementation reviews of IT implementations

Question 1121

In an IS auditor's review of an organization's configuration management practices for software, which of the following is MOST important?

- ☐ Service level agreements (SLAs) between the IT function and users
- ☐ Post-implementation review reports from development efforts
- ☐ Organizational policies related to release management
- ☐ Software rental contracts or lease agreements

Question 1122

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 1123

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 1124

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 1125

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 1126

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 1127

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 1128

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 1129

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 1130

An organization's software developers 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

Question 1131

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 1132

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 1133

A Trojan horse's payload would almost always take damaging effect immediately.

- ☐ True
- ☐ False

Question 1134

Which of the following is a technique that could be used to capture network user passwords?

- ☐ Encryption
- ☐ Sniffing
- ☐ Spoofing
- ☐ Data destruction

Question 1135

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 1136

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.

Question 1137

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 1138

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 1139

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.

Question 1140

Which of the following is the BEST source of information for an IS auditor to use when determining whether an organization's information security policy is adequate?

- ☐ Industry benchmarks
- ☐ Information security program plans
- ☐ Penetration test results
- ☐ Risk assessment results

Question 1141

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 1142

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)

Question 1143

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 notes 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 1144

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 1145

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 1146

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 1147

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 1148

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

Question 1149

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 1150

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 1151

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

Question 1152

Which of the following security control is intended to avoid an incident from occurring?

- ☐ Deterrent
- ☐ Preventive
- ☐ Corrective
- ☐ Recovery

Question 1153

Which of the following attacks targets the Secure Sockets Layer (SSL)?

- ☐ Man-in-the middle
- ☐ Dictionary
- ☐ Password sniffing
- ☐ Phishing

Question 1154

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.

Question 1155

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 1156

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.

Question 1157

Which of the following is the MOST reasonable option for recovering a noncritical system?

- ☐ Warm site
- ☐ Mobile site
- ☐ Hot site
- ☐ Cold site

Question 1158

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 1159

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 1160

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

Question 1161

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 1162

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 1163

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 1164

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.

Question 1165

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 1166

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 1167

Which of the following is the BEST method to maintain an audit trail of changes made to the source code of a program?

- ☐ Standardize file naming conventions.
- ☐ Utilize automated version control.
- ☐ Document details on a change register.
- ☐ Embed details within source code.

Question 1168

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 1169

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 1170

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

Question 1171

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 1172

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 1173

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 1174

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

Question 1175

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

Question 1176

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 1177

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 1178

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 1179

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 1180

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 1181

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

Question 1182

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 1183

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 1184

An IT strategic plan that BEST leverages IT in achieving organizational goals will include:

- ☐ a risk-based ranking of projects.
- ☐ a comparison of future needs against current capabilities.
- ☐ IT budgets linked to the organization's budget.
- ☐ enterprise architecture impacts.

Question 1185

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 1186

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.

Question 1187

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 1188

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 1189

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 1190

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

Question 1191

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 1192

Which of the following tests would provide the BEST assurance that a health care organization is handling patient data appropriately?

- ☐ Compliance with local laws and regulations
- ☐ Compliance with the organization's policies and procedures
- ☐ Compliance with action plans resulting from recent audits
- ☐ Compliance with industry standards and best practice

Question 1193

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.

Question 1194

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 1195

Which of the following should be done FIRST when 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 1196

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

Question 1197

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 1198

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

Question 1199

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 1200

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

Question 1201

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

Question 1202

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

Question 1203

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.

Question 1204

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.

Question 1205

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 1206

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

Question 1207

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 1208

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 1209

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 1210

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.

Question 1211

An organization is moving its on-site application servers to a service provider that operates a virtualized environment shared by multiple customers. Which of the following is the MOST significant risk to the organization?

- ☐ Account hacking from other clients
- ☐ Competing workloads from other clients
- ☐ Service provider access to organizational data
- ☐ Service provider limiting the right to audit

Question 1212

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 1213

Which of the following is the BEST type of backup to minimize the associated time and media?

- ☐ Differential
- ☐ Incremental
- ☐ Mirror
- ☐ Compressed full

Question 1214

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.

Question 1215

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 1216

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 1217

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 1218

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 1219

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 1220

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

Question 1221

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 1222

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 1223

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 1224

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 1225

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 1226

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.

Question 1227

Which of the following controls MOST efficiently ensures that orders transmitted from a sales office to a production warehouse are received accurately and completely?

- ☐ Transaction totals and record counts should be sent and reconciled before transaction processing.
- ☐ Parity checking should be incorporated into all data transmissions.
- ☐ Data should be sent back to the originating site and compared to what was sent to production.
- ☐ Continuity of numerical sequences for all sales orders should be checked.

Question 1228

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 1229

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 1230

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

Question 1231

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.

Question 1232

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 1233

Which of the following is MOST effective against system intrusions?

- ☐ Continuous monitoring
- ☐ Layered protection
- ☐ Penetration testing
- ☐ Two-factor authentication

Question 1234

What should an IS auditor review FIRST when assessing the results of a recent penetration test to identify potential vulnerabilities?

- ☐ Skill level of the network support staff
- ☐ Parameters of the test
- ☐ Number of critical issues found
- ☐ Incident response process

Question 1235

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 1236

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 1237

Run-to-run totals can verify data through which stage(s) of application processing?

- ☐ Initial
- ☐ Various
- ☐ Final
- ☐ Output

Question 1238

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 1239

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 1240

Which of the following control helps to identify an incident's activities and potentially an intruder?

- ☐ Deterrent
- ☐ Preventive
- ☐ Detective
- ☐ Compensating

Question 1241

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 1242

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.

Question 1243

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.

Question 1244

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 1245

Which of the following would be an IS auditor's GREATEST concern when reviewing the early stages of a software development project?

- ☐ The lack of acceptance criteria behind user requirements
- ☐ The lack of completion of all requirements at the end of each sprint
- ☐ The lack of technical documentation to support the program code
- ☐ The lack of a detailed unit and system test plan

Question 1246

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.

Question 1247

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 1248

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

Question 1249

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 1250

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

Question 1251

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 1252

An IS auditor is following upon a finding that determined elevated administrator accounts for servers were not being properly checked out and then back in after each use. Which of the following is the MOST appropriate sampling technique to determine the scope of the problem?

- ☐ Stratified sampling
- ☐ Random sampling
- ☐ Attribute sampling
- ☐ Statistical sampling

Question 1253

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 1254

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 1255

Which of the following network configuration options contains a direct link between any two host machines?

- ☐ Bus
- ☐ Ring
- ☐ Star
- ☐ Completely connected (mesh)

Question 1256

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 1257

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 1258

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

Question 1259

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 1260

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 1261

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

Question 1262

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 1263

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 1264

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 1265

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 1266

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

Question 1267

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 1268

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 1269

Which of the following is the safest means of transmitting confidential information over the Internet?

- ☐ Send the data to a trusted third party to resend to the destination.
- ☐ Use asymmetric encryption and encrypt the data with a private key.
- ☐ Establish a virtual private network (VPN) between the source and the destination.
- ☐ Break the data into many packets and send it over different routes.

Question 1270

Which of the following is MOST important with regard to an application development acceptance test?

- ☐ The quality assurance (QA) team is in charge of the testing process.
- ☐ User management approves the test design before the test is started.
- ☐ The programming team is involved in the testing process.
- ☐ All data files are tested for valid information before conversion.

Question 1271

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 1272

Which of the following transmission media uses a transponder to send information?

- ☐ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Coaxial cable

Question 1273

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 1274

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 1275

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 1276

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 1277

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 1278

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 1279

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 1280

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 1281

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 1282

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 1283

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 1284

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.

Question 1285

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

Question 1286

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

Question 1287

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.

Question 1288

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

Question 1289

An IS auditor reviewing a recently implemented virtual environment notices discrepancies among similar machine setups. Which of the following should the auditor recommend to minimize configuration risks?

- ☐ Implement network best practice recommendations
- ☐ Perform architectural vulnerability analysis to compare current system attributes to a reference
- ☐ Perform hypervisor software updates with available patches to minimize security weakness
- ☐ Implement templates to manage rapid deployment of virtual machines

Question 1290

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 1291

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 1292

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 1293

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 1294

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.

Question 1295

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 1296

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.

Question 1297

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 1298

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

Question 1299

Which of the following is protocol data unit (PDU) of transport layer in TCP/IP model?

- ☐ Data
- ☐ Segment
- ☐ Packet
- ☐ Frame

Question 1300

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 1301

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 1302

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 1303

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 1304

With the help of a security officer, granting access to data is the responsibility of:

- ☐ data owners.
- ☐ programmers.
- ☐ system analysts.
- ☐ librarians.

Question 1305

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

Question 1306

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

Question 1307

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 1308

Which of the following is a passive attack on a network?

- ☐ Message service interruption
- ☐ Message modification
- ☐ Traffic analysis
- ☐ Sequence analysis

Question 1309

What are often the primary safeguards for systems software and data?

- ☐ Administrative access controls
- ☐ Logical access controls
- ☐ Physical access controls
- ☐ Detective access controls

Question 1310

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 1311

Which of the following observations should be of concern to an IS auditor in the fieldwork stage of a procurement audit?

- ☐ Requisitions are being processed by the finance team.
- ☐ The purchase requester receives notifications of goods delivery.
- ☐ Purchase commitments are made prior to requisitions being approved.
- ☐ Requisitions are being facilitated by a third-party procurement service.

Question 1312

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 1313

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 1314

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

Question 1315

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 1316

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

Question 1317

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 1318

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 (EA)
- ☐ IT project value analysis
- ☐ Balanced scorecard
- ☐ Control self-assessment (CSA)

Question 1319

Allowing application programmers to directly patch or change code in production programs increases risk of fraud. True or false?

- ☐ True
- ☐ False

Question 1320

Which function in the purchasing module of an enterprise resource planning (ERP) system ensures payments are not issued for incorrect invoices?

- ☐ Sequential payment numbers
- ☐ Three-way match
- ☐ Purchasing authority levels
- ☐ Management workflow approval

Question 1321

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 1322

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.

Question 1323

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 1324

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 1325

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 1326

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 1327

Due to a recent business divestiture, 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 1328

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 1329

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

Question 1330

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 1331

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 1332

Audit software designed to detect invalid data, extreme values, or linear correlations between data elements can be classified as which type of data analytics tool?

- ☐ Descriptive
- ☐ Diagnostic
- ☐ Predictive
- ☐ Prescriptive

Question 1333

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 1334

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 1335

When auditing the security architecture of an e-commerce environment, an IS auditor should FIRST review the:

- ☐ configuration of the firewall
- ☐ alternate firewall arrangements
- ☐ location of the firewall within the network
- ☐ criteria used for selecting the firewall

Question 1336

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 1337

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.

Question 1338

Which of the following is MOST likely to improve the portability of an application connected to a database?

- ☐ Analyzing stored procedures and triggers
- ☐ Optimizing the database physical schema
- ☐ Verifying database import and export procedures
- ☐ Using a structured query language (SQL)

Question 1339

Which of the following is the BEST indication that an organization has achieved legal and regulatory compliance?

- ☐ The board of directors and senior management accept responsibility for compliance.
- ☐ An independent consultant has been appointed to ensure legal and regulatory compliance.
- ☐ Periodic external and internal audits have not identified instances of noncompliance.
- ☐ The risk management process incorporates noncompliance as a risk.

Question 1340

Which of the following tools are MOST helpful for benchmarking an existing IT capability?

- ☐ Prior IS audit reports
- ☐ IT maturity models
- ☐ Risk assessments
- ☐ IT balanced scorecards

Question 1341

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 1342

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 1343

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 1344

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 1345

In which of the following cloud service models does the user organization have the GREATEST control over the accuracy of configuration items in its configuration management database (CMDB)?

- ☐ Database as a Service (DbaaS)
- ☐ Software as a Service (SaaS)
- ☐ Platform as a Service (PaaS)
- ☐ Infrastructure as a Service (IaaS)

Question 1346

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 1347

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 1348

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 1349

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 1350

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 1351

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 1352

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.

Question 1353

The sender of a public key would be authenticated by a:

- ☐ certificate authority,
- ☐ digital signature.
- ☐ digital certificate.
- ☐ registration authority.

Question 1354

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 1355

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 1356

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 1357

In a small organization, an IS auditor finds that security administration and system analysis functions are performed by the same employee. Which of the following is the MOST significant finding?

- ☐ The security policy has not been updated to reflect the situation.
- ☐ The employee's formal job description has not been updated.
- ☐ The employee has not signed the security policy.
- ☐ The employee's activities are not independently reviewed.

Question 1358

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 1359

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 1360

An IS auditor is reviewing an organization's method to transport sensitive data between offices. Which of the following would cause the auditor MOST concern?

- ☐ The method relies exclusively on the use of digital signatures.
- ☐ The method relies exclusively on the use of asymmetric encryption algorithms.
- ☐ The method relies exclusively on the use of public key infrastructure.
- ☐ The method relies exclusively on the use of symmetric encryption algorithms.

Question 1361

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 1362

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.

Question 1363

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 1364

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 1365

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

Question 1366

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 1367

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 1368

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 1369

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 1370

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.

Question 1371

Which of the following is MOST helpful when establishing the authenticity of digital evidence collected from a hard disk?

- ☐ Bit-by-bit image of the hard disk
- ☐ Hash of the files on the hard disk
- ☐ Chain of custody documentation
- ☐ Confirmation by witnesses

Question 1372

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

Question 1373

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 1374

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 1375

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 1376

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

Question 1377

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.

Question 1378

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 1379

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 1380

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.

Question 1381

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 1382

The PRIMARY objective of value delivery in reference to IT governance is to:

- ☐ increase efficiency
- ☐ promote best practices
- ☐ optimize investments
- ☐ ensure compliance

Question 1383

Which of the following append themselves to files as a protection against viruses?

- ☐ Behavior blockers
- ☐ Cyclical redundancy checkers (CRCs)
- ☐ Immunizers
- ☐ Active monitors

Question 1384

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 1385

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 1386

In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:

- ☐ implementation.
- ☐ compliance.
- ☐ documentation.
- ☐ sufficiency.

Question 1387

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 1388

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

Question 1389

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.

Question 1390

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

Question 1391

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 1392

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.

Question 1393

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 1394

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 1395

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 1396

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.

Question 1397

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 1398

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 1399

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 1400

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 1401

An IS auditor is assessing a recent migration of mission critical applications to a virtual platform. Which of the following observations poses the GREATEST risk to the organization?

- ☐ A post-implementation review of the hypervisor has not yet been conducted.
- ☐ Role descriptions do not accurately reflect new virtualization responsibilities.
- ☐ The migration was not approved by the board of directors.
- ☐ Training for staff with new virtualization responsibilities has not been conducted.

Question 1402

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 1403

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 1404

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 1405

Which of the following would BEST support 24/7 availability?

- ☐ Daily backup
- ☐ offsite storage
- ☐ Mirroring
- ☐ Periodic testing

Question 1406

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 1407

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 1408

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 1409

Which of the following test approaches would utilize data analytics to test a dual approval payment control?

- ☐ Review payments completed in the past month that do not have a unique approver.
- ☐ Attempt to complete a payment without a secondary approval.
- ☐ Review users within the payment application who are assigned an approver role.
- ☐ Evaluate configuration settings for the secondary approval requirements.

Question 1410

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 1411

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 1412

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 1413

Which of the following mechanisms for process improvement involves examination of industry best practice?

- ☐ Continuous improvement
- ☐ Knowledge management
- ☐ Business process reengineering (BPR)
- ☐ Benchmarking

Question 1414

Which of the following would BEST facilitate the successful implementation of an IT-related framework?

- ☐ Aligning the framework to industry best practices
- ☐ Involving appropriate business representation within the framework
- ☐ Establishing committees to support and oversee framework activities
- ☐ Documenting IT-related policies and procedures

Question 1415

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 1416

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 1417

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

Question 1418

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 1419

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 1420

Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

- ☐ True
- ☐ False

Question 1421

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 1422

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

Question 1423

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.

Question 1424

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 1425

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

Question 1426

The FIRST step in data classification is to:

- ☐ establish ownership.
- ☐ perform a criticality analysis.
- ☐ define access rules.
- ☐ create a data dictionary.

Question 1427

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

Question 1428

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

Question 1429

In which phase of penetration testing would host detection and domain name system (DNS) interrogation be performed?

- ☐ Reporting
- ☐ Attacks
- ☐ Discovery
- ☐ Planning

Question 1430

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 1431

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 1432

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 1433

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 1434

Which of the following controls is MOST effective in detecting spam?

- ☐ Denying transmission control protocol (TCP) connections in the mail server
- ☐ Refusing Internet protocol (IP) connections at the router
- ☐ Registering the recipient with keepers of spam lists
- ☐ Using heuristic filters based on the content of the message

Question 1435

A database is denormalized in order to:

- ☐ prevent loss of data.
- ☐ increase processing efficiency.
- ☐ ensure data integrity.
- ☐ save storage space.

Question 1436

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 1437

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

Question 1438

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 1439

Software is considered malware based on:

- ☐ the intent of the creator.
- ☐ its particular features.
- ☐ its location.
- ☐ its compatibility.
- ☐ None of the choices.

Question 1440

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 1441

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.

Question 1442

Which of the following is the MOST important consideration when developing an online business architecture and recovery strategy?

- ☐ Vendors' network security
- ☐ Immediate problem resolution
- ☐ Vendors' financial stability
- ☐ Single points of failure

Question 1443

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 1444

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 1445

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 1446

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 1447

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

Question 1448

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 1449

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 maintain data integrity during transport?

- ☐ Ensure the data is transported in locked tamper-evident containers.
- ☐ Ensure that logging and recording of data transport takes place.
- ☐ Ensure the transport company is licensed and insured.
- ☐ Ensure the data is validated prior to transport.

Question 1450

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 1451

What type of approach to the development of organizational policies is often driven by risk assessment?

- ☐ Bottom-up
- ☐ Top-down
- ☐ Comprehensive
- ☐ Integrated

Question 1452

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 1453

Which of the following would BEST protect against web-based cross-domain attacks?

- ☐ Network addressing scheme
- ☐ Database hardening
- ☐ Encryption controls
- ☐ Application controls

Question 1454

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 1455

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 1456

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

Question 1457

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