



isaca.pass4sureexam.cisa.v2020-03- 23.by.mohammed.1103q.vce

CISA

CISA

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

Exam A (1103 questions)

Question 1

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 2

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 3

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 4

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 5

Which of the following is the FIRST step when conducting a business impact analysis?

- ☐ Identifying critical information resources
- ☐ Identifying events impacting continuity of operations
- ☐ Analyzing past transaction volumes
- ☐ Creating a data classification scheme

Question 6

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 7

Which of the following component of an expert system enables the expert system to collect data from nonhuman sources, such as measurement instruments in a power plant?

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

Question 8

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

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

Question 9

Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the recipient's private key.
True or false?

- ☐ False
- ☐ True

Question 10

A database is denormalized in order to:

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

Question 11

The PRIMARY advantage of a continuous audit approach is that it:

- ☐ does not require an IS auditor to collect evidence on system reliability while processing is taking place.
- ☐ requires the IS auditor to review and follow up immediately on all information collected.
- ☐ can improve system security when used in time-sharing environments that process a large number of transactions.
- ☐ does not depend on the complexity of an organization's computer systems.

Question 12

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 13

Which of the following recovery strategies is MOST appropriate for a business having multiple offices within a region and a limited recovery budget?

- ☐ A hot site maintained by the business
- ☐ A commercial cold site
- ☐ A reciprocal arrangement between its offices
- ☐ A third-party hot site

Question 14

Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?

- ☐ Session keys are dynamic
- ☐ Private symmetric keys are used
- ☐ Keys are static and shared
- ☐ Source addresses are not encrypted or authenticated

Question 15

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 16

In computer forensic which of the following describe the process that converts the information extracted into a format that can be understood by investigator?

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

Question 17

Which of the following would provide the BEST protection against the hacking of a computer connected to the Internet?

- ☐ A remote access server
- ☐ A proxy server
- ☐ A personal firewall
- ☐ A password-generating token

Question 18

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 19

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

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

Question 20

A company has decided to implement an electronic signature scheme based on public key infrastructure. The user's private key will be stored on the computer's hard drive and protected by a password. The MOST significant risk of this approach is:

- ☐ use of the user's electronic signature by another person if the password is compromised.
- ☐ forgery by using another user's private key to sign a message with an electronic signature.
- ☐ impersonation of a user by substitution of the user's public key with another person's public key.
- ☐ forgery by substitution of another person's private key on the computer.

Question 21

In computer forensics, which of the following is the process that allows bit-for-bit copy of a data to avoid damage of original data or information when multiple analysis may be performed?

- ☐ Imaging
- ☐ Extraction
- ☐ Data Protection
- ☐ Data Acquisition

Question 22

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 23

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

- ☐ True
- ☐ False

Question 24

During a postimplementation review of an enterprise resource management system, an IS auditor would MOST likely:

- ☐ review access control configuration
- ☐ evaluate interface testing.
- ☐ review detailed design documentation.
- ☐ evaluate system testing.

Question 25

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 26

The risk of communication failure in an e-commerce environment is BEST minimized through the use of:

- ☐ alternative or diverse routing
- ☐ compression software to minimize transmission duration
- ☐ a packet filtering firewall to reroute messages
- ☐ functional or message acknowledgments

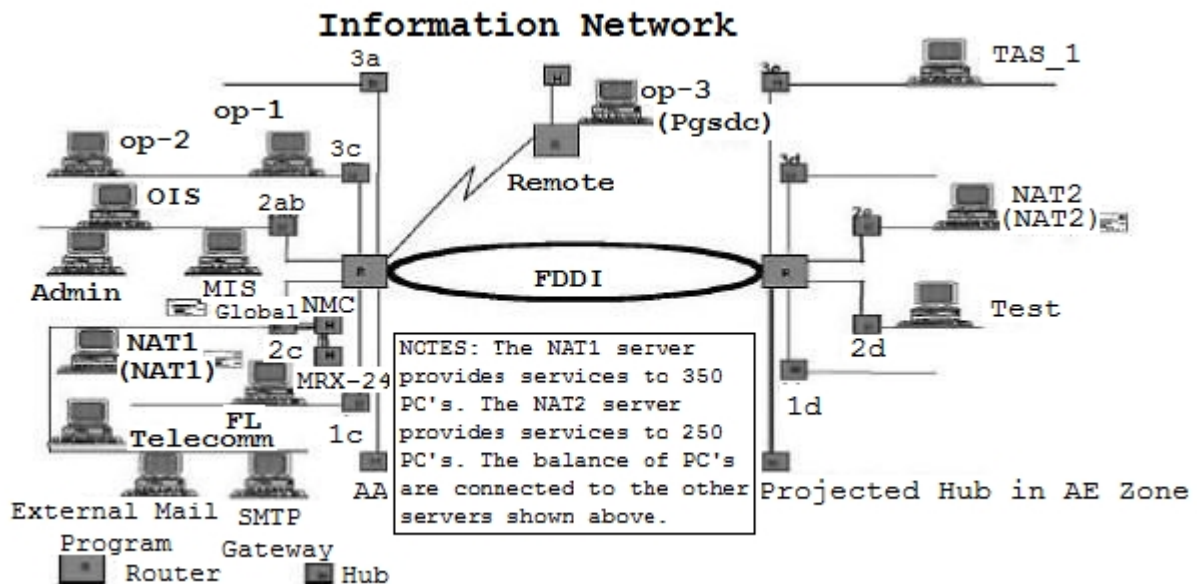
Question 27

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 28

In the 2c area of the diagram, there are three hubs connected to each other. What potential risk might this indicate?



- ☐ Virus attack
- ☐ Performance degradation
- ☐ Poor management controls
- ☐ Vulnerability to external hackers

Question 29

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 30

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 31

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 32

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

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

Question 33

An organization uses two data centers. Which of the following would BEST address the organization's need for high resiliency?

- ☐ The data centers act as mirrored sites.
- ☐ Each data center is recoverable via tape backups.
- ☐ A hot site is used for the second site.
- ☐ There is data replication across the data centers.

Question 34

A stockbroker accepts orders over the Internet. Which of the following is the MOST appropriate control to ensure confidentiality of the orders?

- ☐ Virtual private network
- ☐ Public key encryption
- ☐ Data Encryption Standard (DES)
- ☐ Digital signature

Question 35

An organization has made a strategic decision to split into separate operating entities to improve profitability. However, the IT infrastructure remains shared between the entities. Which of the following would BEST help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan?

- ☐ Increasing the frequency of risk-based IS audits for each business entity
- ☐ Revising IS audit plans to focus on IT changes introduced after the split
- ☐ Conducting an audit of newly introduced IT policies and procedures
- ☐ Developing a risk-based plan considering each entity's business processes

Question 36

Disaster recovery planning (DRP) addresses the:

- ☐ technological aspect of business continuity planning.
- ☐ operational piece of business continuity planning.
- ☐ functional aspect of business continuity planning.
- ☐ overall coordination of business continuity planning.

Question 37

An IS auditor is planning to audit an organization's infrastructure for access, patching, and change management. Which of the following is the BEST way to prioritize the systems?

- ☐ Complexity of the environment
- ☐ Criticality of the system
- ☐ System hierarchy within the infrastructure
- ☐ System retirement plan

Question 38

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

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

Question 39

Which of the following attack best describe “Computer is the target of a crime” and “Computer is the tool of a crime”?

- ☐ Denial of Service (DoS) and Installing Key loggers
- ☐ War Driving and War Chalking
- ☐ Piggybacking and Race Condition
- ☐ Traffic analysis and Eavesdropping

Question 40

An investment advisor e-mails periodic newsletters to clients and wants reasonable assurance that no one has modified the newsletter. This objective can be achieved by:

- ☐ encrypting the hash of the newsletter using the advisor's private key.
- ☐ encrypting the hash of the newsletter using the advisor's public key.
- ☐ digitally signing the document using the advisor's private key.
- ☐ encrypting the newsletter using the advisor's private key.

Question 41

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 42

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

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

Question 43

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 44

Which of the following will BEST provide an organization with ongoing assurance of the information security services provided by a cloud provider?

- ☐ Continuous monitoring of an information security risk profile
- ☐ Evaluating the provider's security incident response plan
- ☐ Requiring periodic self-assessment by the provider
- ☐ Ensuring the provider's roles and responsibilities are established

Question 45

Which of the following represents the GREATEST potential risk in an EDI environment?

- ☐ Transaction authorization
- ☐ Loss or duplication of EDI transmissions
- ☐ Transmission delay
- ☐ Deletion or manipulation of transactions prior to or after establishment of application controls

Question 46

Which of the following would provide the STRONGEST indication that senior management commitment to information security is lacking within an organization?

- ☐ Inconsistent enforcement of information security policies
- ☐ A reduction in information security investment
- ☐ A high of information security risk acceptance
- ☐ The information security manager reports to the chief risk officer

Question 47

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 48

Squid is an example of:

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

Question 49

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 50

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 51

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 52

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 53

Most access violations are:

- ☐ Accidental
- ☐ Caused by internal hackers
- ☐ Caused by external hackers
- ☐ Related to Internet

Question 54

Which of the following is a project management technique for defining and deploying software deliverables within a relatively short and fixed period of time, and with predetermined specific resources?

- ☐ Functional Point analysis
- ☐ Gantt Chart
- ☐ Critical path methodology
- ☐ Time box management

Question 55

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 56

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 57

Screening router inspects traffic through examining:

- ☐ message header.
- ☐ virus payload
- ☐ message content
- ☐ attachment type
- ☐ None of the choices.

Question 58

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 59

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 60

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 61

Which of the following layer of an OSI model transmits and receives the bit stream as electrical, optical or radio signals over an appropriate medium or carrier?

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

Question 62

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

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

Question 63

An organization that has outsourced its incident management capabilities just discovered a significant privacy breach by an unknown attacker. Which of the following is the MOST important action of the security manager?

- ☐ Follow the outsourcer's response plan
- ☐ Refer to the organization's response plan
- ☐ Notify the outsourcer of the privacy breach
- ☐ Alert the appropriate law enforcement authorities

Question 64

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

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

Question 65

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 66

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 67

What should be a security manager's PRIMARY objective in the event of a security incident?

- ☐ Identify the source of the breach and how it was perpetrated.
- ☐ Contain the threat and restore operations in a timely manner.
- ☐ Ensure that normal operations are not disrupted.
- ☐ Identify lapses in operational control effectiveness.

Question 68

The MAIN benefit of using an integrated test facility (ITF) as an online auditing technique is that it enables:

- ☐ a cost-effective approach to application controls audit
- ☐ auditors to investigate fraudulent transactions
- ☐ auditors to test without impacting production data
- ☐ the integration of financial and audit tests

Question 69

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 70

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

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

Question 71

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 72

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 73

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 74

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 75

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 76

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 77

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 78

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 79

During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be MOST concerned with the:

- ☐ allocation of resources during an emergency.
- ☐ maintenance of hardware and software compatibility.
- ☐ differences in IS policies and procedures.
- ☐ frequency of system testing.

Question 80

Following a risk assessment, new countermeasures have been approved by management. Which of the following should be performed NEXT?

- ☐ Schedule the target end date for implementation activities.
- ☐ Budget the total cost of implementation activities.
- ☐ Develop an implementation strategy.
- ☐ Calculate the residual risk for each countermeasure.

Question 81

When is the BEST time to commence continuity planning for a new application system?

- ☐ Immediately after implementation
- ☐ Just prior to the handover to the system maintenance group
- ☐ During the design phase
- ☐ Following successful user testing

Question 82

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 83

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 84

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

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

Question 85

A manufacturing company is implementing application software for its sales and distribution system. Which of the following is the MOST important reason for the company choose a centralized online database?

- ☐ Enhanced data redundancy
- ☐ Elimination of multiple points of failure
- ☐ Elimination of the need for data normalization
- ☐ Enhanced integrity controls

Question 86

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 87

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 88

An organization has implemented a control to help ensure databases containing personal information will not be updated with online transactions that are incomplete due to connectivity issues. Which of the following information attributes is PRIMARILY addressed by this control?

- ☐ Integrity
- ☐ Confidentiality
- ☐ Availability
- ☐ Compliance

Question 89

When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:

- ☐ not be concerned since there may be other compensating controls to mitigate the risks.
- ☐ ensure that overrides are automatically logged and subject to review.
- ☐ verify whether all such overrides are referred to senior management for approval.
- ☐ recommend that overrides not be permitted.

Question 90

To effectively classify data, which of the following MUST be determined?

- ☐ Data controls
- ☐ Data ownership
- ☐ Data users
- ☐ Data volume

Question 91

Which of the following is an example of a preventive control in an accounts payable system?

- ☐ The system only allows payments to vendors who are included in the system's master vendor list.
- ☐ Policies and procedures are clearly communicated to all members of the accounts payable department.
- ☐ The system produces daily payment summary reports that staff use to compare against invoice totals.
- ☐ Backups of the system and its data are performed on a nightly basis and tested periodically.

Question 92

To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

- ☐ schedule the audits and monitor the time spent on each audit.
- ☐ train the IS audit staff on current technology used in the company.
- ☐ develop the audit plan on the basis of a detailed risk assessment.
- ☐ monitor progress of audits and initiate cost control measures.

Question 93

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 94

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 95

An IS auditor is conducting a review of a healthcare organization's IT policies for handling medical records. Which of the following is MOST important to verify?

- ☐ A documented policy approval process is in place
- ☐ Policy writing standards are consistent
- ☐ The policies comply with regulatory requirements
- ☐ IT personnel receive ongoing policy training

Question 96

An IS auditor has identified the lack of an authorization process for users of an application. The IS auditor's main concern should be that:

- ☐ more than one individual can claim to be a specific user.
- ☐ there is no way to limit the functions assigned to users.
- ☐ user accounts can be shared.
- ☐ users have a need-to-know privilege.

Question 97

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 98

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 99

Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the _____. (fill-in-the-blank)

- ☐ Security administrator
- ☐ Systems auditor
- ☐ Board of directors
- ☐ Financial auditor

Question 100

Which of the following should be considered FIRST when implementing a risk management program?

- ☐ An understanding of the organization's threat, vulnerability and risk profile
- ☐ An understanding of the risk exposures and the potential consequences of compromise
- ☐ A determination of risk management priorities based on potential consequences
- ☐ A risk mitigation strategy sufficient to keep risk consequences at an acceptable level

Question 101

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 102

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

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

Question 103

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 104

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

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

Question 105

A company has implemented a new client-server enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following would BEST ensure that the orders are entered accurately and the corresponding products are produced?

- ☐ Verifying production to customer orders
- ☐ Logging all customer orders in the ERP system
- ☐ Using hash totals in the order transmitting process
- ☐ Approving (production supervisor) orders prior to production

Question 106

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 107

Sam is the security Manager of a financial institute. Senior management has requested he performs a risk analysis on all critical vulnerabilities reported by an IS auditor. After completing the risk analysis, Sam has observed that for a few of the risks, the cost benefit analysis shows that risk mitigation cost (countermeasures, controls, or safeguard) is more than the potential lost that could be incurred. What kind of a strategy should Sam recommend to the senior management to treat these risks?

- ☐ Risk Mitigation
- ☐ Risk Acceptance
- ☐ Risk Avoidance
- ☐ Risk transfer

Question 108

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 109

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

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

Question 110

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 111

John had implemented a validation check on the marital status field of a payroll record. A payroll record contains a field for marital status and acceptable status code are M for Married or S for Single. If any other code is entered, record should be rejected. Which of the following data validation control was implemented by John?

- ☐ Range Check
- ☐ Validity Check
- ☐ Existence check
- ☐ Reasonableness check

Question 112

A perpetrator looking to gain access to and gather information about encrypted data being transmitted over the network would use:

- ☐ eavesdropping
- ☐ spoofing.
- ☐ traffic analysis.
- ☐ masquerading.

Question 113

An IS auditor has discovered that a cloud-based application was not included in an application inventory that was used to confirm the scope of an audit. The business process owner explained that the application will be audited by a third party in the next year. The auditor's NEXT step should be to:

- ☐ evaluate the impact of the cloud application on the audit scope
- ☐ revise the audit scope to include the cloud-based application
- ☐ review the audit report when performed by the third party
- ☐ report the control deficiency to senior management

Question 114

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 115

Which of the following can be thought of as the simplest and almost cheapest type of firewall?

- ☐ stateful firewall
- ☐ hardware firewall
- ☐ PIX firewall
- ☐ packet filter
- ☐ None of the choices.

Question 116

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

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

Question 117

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

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

Question 118

A computer program used by multiple departments has data quality issues. There is no agreement as to who should be responsible for corrective action. Which of the following is an IS auditor's BEST course of action?

- ☐ Recommend the IT department be assigned data cleansing responsibility.
- ☐ Modify the program to automatically cleanse the data and close the issue.
- ☐ Assign responsibility to the primary department using the program.
- ☐ Note the disagreement and recommend establishing data governance.

Question 119

A LAN administrator normally would be restricted from:

- ☐ having end-user responsibilities.
- ☐ reporting to the end-user manager.
- ☐ having programming responsibilities.
- ☐ being responsible for LAN security administration.

Question 120

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 121

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 122

An organization has implemented an automated match between purchase orders, good 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 123

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 124

Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:

- ☐ include the finding in the final report, because the IS auditor is responsible for an accurate report of all findings.
- ☐ not include the finding in the final report, because the audit report should include only unresolved findings.
- ☐ not include the finding in the final report, because corrective action can be verified by the IS auditor during the audit.
- ☐ include the finding in the closing meeting for discussion purposes only.

Question 125

With respect to the outsourcing of IT services, which of the following conditions should be of GREATEST concern to an IS auditor?

- ☐ Outsourced activities are core and provide a differentiated advantage to the organization.
- ☐ Periodic renegotiation is specified in the outsourcing contract.
- ☐ The outsourcing contract fails to cover every action required by the arrangement.
- ☐ Similar activities are outsourced to more than one vendor.

Question 126

An IS auditor reviewing a proposed application software acquisition should ensure that the:

- ☐ operating system (OS) being used is compatible with the existing hardware platform.
- ☐ planned OS updates have been scheduled to minimize negative impacts on company needs.
- ☐ OS has the latest versions and updates.
- ☐ products are compatible with the current or planned OS.

Question 127

A business application system accesses a corporate database using a single ID and password embedded in a program. Which of the following would provide efficient access control over the organization's data?

- ☐ Introduce a secondary authentication method such as card swipe
- ☐ Apply role-based permissions within the application system
- ☐ Have users input the ID and password for each database transaction
- ☐ Set an expiration period for the database password embedded in the program

Question 128

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 129

A large insurance company is about to replace a major financial application. Which of the following is the IS auditor's PRIMARY focus when conducting the pre-implementation review?

- ☐ Procedure updates
- ☐ Migration of data
- ☐ System manuals
- ☐ Unit testing

Question 130

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

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

Question 131

To confirm integrity for a hashed message, the receiver should use:

- ☐ a different hashing algorithm from the sender's to create a numerical representation of the file.
- ☐ a different hashing algorithm from the sender's to create a binary image of the file.
- ☐ the same hashing algorithm as the sender's to create a binary image of the file.
- ☐ the same hashing algorithm as the sender's to create a numerical representation of the file.

Question 132

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 133

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 134

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 135

An organization which uses external cloud services extensively is concerned with risk monitoring and timely response. The BEST way to address this concern is to ensure:

- ☐ the availability of continuous technical support
- ☐ internal security standards are in place
- ☐ a right-to-audit clause is included in contracts
- ☐ appropriate service level agreements (SLAs) are in place

Question 136

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 137

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 138

The BEST way to avoid session hijacking is to use:

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

Question 139

The BEST test to determine whether an application's internal security controls are configured in compliance with the organization's security standards is an evaluation of the:

- ☐ availability and frequency of security reports
- ☐ intrusion detection system (IDS) logs
- ☐ application's user accounts and passwords
- ☐ business application's security parameter settings

Question 140

When the inherent risk of a business activity is lower than the acceptable risk level, the BEST course of action would be to:

- ☐ implement controls to mitigate the risk.
- ☐ report compliance to management.
- ☐ review the residual risk level.
- ☐ monitor for business changes.

Question 141

Distributed denial-of-service (DDOS) attacks on Internet sites are typically evoked by hackers using which of the following?

- ☐ Logic bombs
- ☐ Phishing
- ☐ Spyware
- ☐ Trojan horses

Question 142

Which of the following should be of MOST concern to an IS auditor reviewing the public key infrastructure (PKI) for enterprise e-mail?

- ☐ The private key certificate has not been updated.
- ☐ The certificate revocation list has not been updated.
- ☐ The certificate practice statement has not been published.
- ☐ The PKI policy has not been updated within the last year.

Question 143

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

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

Question 144

Is it appropriate for an IS auditor from a company that is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?

- ☐ Yes, because an IS auditor will evaluate the adequacy of the service bureau's plan and assist their company in implementing a complementary plan.
- ☐ Yes, because based on the plan, an IS auditor will evaluate the financial stability of the service bureau and its ability to fulfill the contract.
- ☐ No, because the backup to be provided should be specified adequately in the contract.
- ☐ No, because the service bureau's business continuity plan is proprietary information.

Question 145

What type of risk is associated with authorized program exits (trap doors)?

- ☐ Business risk
- ☐ Audit risk
- ☐ Detective risk
- ☐ Inherent risk

Question 146

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

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

Question 147

Which of the following method is recommended by security professional to PERMANENTLY erase sensitive data on magnetic media?

- ☐ Degaussing
- ☐ Overwrite every sector of magnetic media with pattern of 1's and 0's
- ☐ Format magnetic media
- ☐ Delete File allocation table

Question 148

Which of the following must be in place before an IS auditor initiates audit follow-up activities?

- ☐ A heat map with the gaps and recommendations displayed in terms of risk
- ☐ A management response in the final report with a committed implementation date
- ☐ Supporting evidence for the gaps and recommendations mentioned in the audit report
- ☐ Available resources for the activities included in the action plan

Question 149

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

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

Question 150

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 151

Which of the following is a method to prevent disclosure of classified documents printed on a shared printer?

- ☐ Requiring a key code to be entered on the printer to produce hardcopy
- ☐ Producing a header page with classification level for printed documents
- ☐ Encrypting the data stream between the user's computer and the printer
- ☐ Using passwords to allow authorized users to send documents to the printer

Question 152

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 153

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 154

Which of the following is the BEST way to mitigate the risk of unintentional modifications associated with complex calculations in end-user computing (EUC)?

- ☐ Verify EUC results through manual calculations.
- ☐ Operate copies of EUC programs out of a secure library.
- ☐ Implement data integrity checks.
- ☐ Utilize an independent party to review the source calculations.

Question 155

Following a recent acquisition, an information security manager has been requested the outstanding risk reported early in the acquisition process. Which of the following would be the manager's BEST course of action?

- ☐ Perform a vulnerability assessment of the acquired company's infrastructure.
- ☐ Re-evaluate the risk treatment plan for the outstanding risk.
- ☐ Re-assess the outstanding risk of the acquired company.
- ☐ Add the outstanding risk to the acquiring organization's risk registry

Question 156

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

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

Question 157

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 158

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

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

Question 159

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

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

Question 160

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 161

Who should be responsible for network security operations?

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

Question 162

When planning an audit to assess application controls of a cloud-based system, it is MOST important for the IS auditor to understand the:

- ☐ policies and procedures of the business area being audited.
- ☐ business process supported by the system.
- ☐ availability reports associated with the cloud-based system.
- ☐ architecture and cloud environment of the system.

Question 163

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 164

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 165

What would be the major purpose of rootkit?

- ☐ to hide evidence from system administrators.
- ☐ to encrypt files for system administrators.
- ☐ to corrupt files for system administrators.
- ☐ to hijack system sessions.
- ☐ None of the choices.

Question 166

Which of the following is the MOST important criterion when selecting a location for an offsite storage facility for IS backup files? The offsite facility must be:

- ☐ physically separated from the data center and not subject to the same risks.
- ☐ given the same level of protection as that of the computer data center.
- ☐ outsourced to a reliable third party.
- ☐ equipped with surveillance capabilities.

Question 167

Passwords should be:

- ☐ assigned by the security administrator for first time logon.
- ☐ changed every 30 days at the discretion of the user.
- ☐ reused often to ensure the user does not forget the password.
- ☐ displayed on the screen so that the user can ensure that it has been entered properly.

Question 168

During an ERP post-implementation review, it was noted that operating costs have been significantly higher than anticipated. Which of the following should the organization have done to detect this issue?

- ☐ Updated the project charter as major changes occurred
- ☐ Conducted periodic user satisfaction surveys
- ☐ Performed an analysis of system usage
- ☐ Monitored financial key performance indicators

Question 169

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 170

In an online banking application, which of the following would BEST protect against identity theft?

- ☐ Encryption of personal password
- ☐ Restricting the user to a specific terminal
- ☐ Two-factor authentication
- ☐ Periodic review of access logs

Question 171

In an EDI process, the device which transmits and receives electronic documents is the:

- ☐ communications handler.
- ☐ EDI translator.
- ☐ application interface.
- ☐ EDI interface.

Question 172

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 173

An IS auditor observes that routine backups of operational databases are taking longer than before. Which of the following would MOST effectively help to reduce backup and recovery times for operational databases?

- ☐ Utilizing database technologies to achieve efficiencies
- ☐ Using solid storage device (SSD) media
- ☐ Requiring a combination of weekly full backups and daily differential backups
- ☐ Archiving historical data in accordance with the data retention policy

Question 174

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 175

The directory system of a database-management system describes:

- ☐ The access method to the data
- ☐ The location of data AND the access method
- ☐ The location of data
- ☐ Neither the location of data NOR the access method

Question 176

While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:

- ☐ audit trail of the versioning of the work papers.
- ☐ approval of the audit phases.
- ☐ access rights to the work papers.
- ☐ confidentiality of the work papers.

Question 177

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 178

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 179

An internal IS auditor discovers that a service organization did not notify its customers following a data breach. Which of the following should the auditor do FIRST?

- ☐ Notify audit management of the finding.
- ☐ Report the finding to regulatory authorities.
- ☐ Notify the service organization's customers.
- ☐ Require the service organization to notify its customers.

Question 180

Which of the following is the BEST approach for performing a business impact analysis (BIA) of a supply-chain management application?

- ☐ Circulating questionnaires to key internal stakeholders
- ☐ Interviewing groups of key stakeholders
- ☐ Accepting IT personnel's view of business issues
- ☐ Reviewing the organization's policies and procedures

Question 181

Everything not explicitly permitted is forbidden has which of the following kinds of tradeoff?

- ☐ it improves security at a cost in functionality.
- ☐ it improves functionality at a cost in security.
- ☐ it improves security at a cost in system performance.
- ☐ it improves performance at a cost in functionality.
- ☐ None of the choices.

Question 182

The use of statistical sampling procedures helps minimize:

- ☐ Detection risk
- ☐ Business risk
- ☐ Controls risk
- ☐ Compliance risk

Question 183

When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

- ☐ has all the personnel and equipment it needs.
- ☐ plans are consistent with management strategy.
- ☐ uses its equipment and personnel efficiently and effectively.
- ☐ has sufficient excess capacity to respond to changing directions.

Question 184

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

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

Question 185

Which of the following is the MOST important security consideration when using infrastructure as a Service (IaaS)?

- ☐ User access management
- ☐ Compliance with internal standards
- ☐ Segmentation among guests
- ☐ Backup and recovery strategy

Question 186

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 187

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 188

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

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

Question 189

Which of the following is an object-oriented technology characteristic that permits an enhanced degree of security over data?

- ☐ inheritance
- ☐ Dynamic warehousing
- ☐ Encapsulation
- ☐ Polymorphism

Question 190

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

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

Question 191

An information security team has discovered that users are sharing a login account to an application with sensitive information, in violation of the access policy. Business management indicates that the practice creates operational efficiencies. The information security manager's BEST course of action should be to:

- ☐ modify the policy
- ☐ present the risk to senior management
- ☐ enforce the policy
- ☐ create an exception for the deviation

Question 192

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 193

Which of the following is the PRIMARY advantage of having an established information security governance framework in place when an organization is adopting emerging technologies?

- ☐ An emerging technologies strategy would be in place
- ☐ A cost-benefit analysis process would be easier to perform
- ☐ An effective security risk management process is established
- ☐ End-user acceptance of emerging technologies has been established

Question 194

While planning a review of IT governance, the IS auditor is MOST likely to:

- ☐ examine audit committee minutes for IS-related matters and their control.
- ☐ obtain information about the framework of control adopted by management.
- ☐ assess whether business process owner responsibilities are consistent across the organization.
- ☐ review compliance with policies and procedures issued by the board of directors.

Question 195

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 196

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 197

A PRIMARY benefit derived from an organization employing control self-assessment (CSA) techniques is that it:

- ☐ can identify high-risk areas that might need a detailed review later.
- ☐ allows IS auditors to independently assess risk.
- ☐ can be used as a replacement for traditional audits.
- ☐ allows management to relinquish responsibility for control.

Question 198

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 199

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 200

The information security policy that states 'each individual must have their badge read at every controlled door' addresses which of the following attack methods?

- ☐ Piggybacking
- ☐ Shoulder surfing
- ☐ Dumpster diving
- ☐ Impersonation

Question 201

An IS auditor is a member of an application development team that is selecting software. Which of the following would impair the auditor's independence?

- ☐ Verifying the weighting of each selection criteria
- ☐ Approving the vendor selection methodology
- ☐ Reviewing the request for proposal (RFP)
- ☐ Witnessing the vendor selection process

Question 202

The business owner's approval of software changes being moved into production is PRIMARILY necessary to:

- ☐ ensure that an application functionality requirement is satisfied.
- ☐ prevent unauthorized access to data.
- ☐ inform management of deployments of new functionality.
- ☐ confirm there is a process to control system changes.

Question 203

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 FIRST step 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 204

What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

- ☐ Test data/deck
- ☐ Base-case system evaluation
- ☐ Integrated test facility (ITF)
- ☐ Parallel simulation

Question 205

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 206

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 207

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 208

A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server. Which of the following would MOST effectively allow the hospital to avoid paying the ransom?

- ☐ A continual server replication process
- ☐ A property tested offline backup system
- ☐ A property configured firewall
- ☐ Employee training on ransomware

Question 209

A lower recovery time objective (RTO) results in:

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

Question 210

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

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

Question 211

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 212

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 213

Which of the following biometrics methods provides the HIGHEST accuracy and is LEAST accepted by users?

- ☐ Palm Scan
- ☐ Hand Geometry
- ☐ Fingerprint
- ☐ Retina scan

Question 214

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 215

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 216

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

- ☐ S/MIME
- ☐ SSH
- ☐ SET
- ☐ S/HTTP

Question 217

Reconfiguring which of the following firewall types will prevent inward downloading of files through the File Transfer Protocol (FTP)?

- ☐ Circuit gateway
- ☐ Application gateway
- ☐ Packet filter
- ☐ Screening router

Question 218

Which of the following is MOST important when an organization contracts for the long-term use of a custom-developed application?

- ☐ Documented coding standards
- ☐ Error correction management
- ☐ Contract renewal provisions
- ☐ Escrow clause

Question 219

Which of the following statements regarding an off-site information processing facility is TRUE?

- ☐ It should have the same amount of physical access restrictions as the primary processing site.
- ☐ It should be located in proximity to the originating site so that it can quickly be made operational.
- ☐ It should be easily identified from the outside so in the event of an emergency it can be easily found.
- ☐ Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

Question 220

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 221

Which of the following human resources management practices BEST leads to the detection of fraudulent activity?

- ☐ Background checks
- ☐ Time reporting
- ☐ Employee code of ethics
- ☐ Mandatory time off

Question 222

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 223

When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

- ☐ Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.
- ☐ Reviewing an audit client's business plan should be performed after reviewing an organization's IT strategic plan.
- ☐ Reviewing an audit client's business plan should be performed during the review of an organization's IT strategic plan.
- ☐ Reviewing an audit client's business plan should be performed without regard to an organization's IT strategic plan.

Question 224

Which of the following would BEST describe an audit risk?

- ☐ The company is being sued for false accusations.
- ☐ The financial report may contain undetected material errors.
- ☐ Key employees have not taken vacation for 2 years.
- ☐ Employees have been misappropriating funds.

Question 225

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 226

Which of the following term related to network performance refers to the variation in the time of arrival of packets on the receiver of the information?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Jitter

Question 227

Which of the following controls would provide the GREATEST assurance of database integrity?

- ☐ Audit log procedures
- ☐ Table link/reference checks
- ☐ Query/table access time checks
- ☐ Rollback and roll forward database features

Question 228

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

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

Question 229

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 230

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 231

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 232

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 233

What is an effective control for granting temporary access to vendors and external support personnel?

- ☐ Creating user accounts that automatically expire by a predetermined date
- ☐ Creating permanent guest accounts for temporary use
- ☐ Creating user accounts that restrict logon access to certain hours of the day
- ☐ Creating a single shared vendor administrator account on the basis of least-privileged access

Question 234

The editing/validation of data entered at a remote site would be performed MOST effectively at the:

- ☐ central processing site after running the application system.
- ☐ central processing site during the running of the application system.
- ☐ remote processing site after transmission of the data to the central processing site.
- ☐ remote processing site prior to transmission of the data to the central processing site.

Question 235

An organization has created a policy that defines the types of web sites that users are forbidden to access. What is the MOST effective technology to enforce this policy?

- ☐ Stateful inspection firewall
- ☐ Web content filter
- ☐ Web cache server
- ☐ Proxy server

Question 236

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

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

Question 237

The selection of security controls is PRIMARILY linked to:

- ☐ risk appetite of the organization.
- ☐ regulatory requirements.
- ☐ business impact assessment.
- ☐ best practices of similar organizations.

Question 238

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 239

Which of the following types of testing would determine whether a new or modifies system can operate in its target environment without adversely impacting other existing systems?

- ☐ Parallel testing
- ☐ Pilot testing
- ☐ Interface/integration testing
- ☐ Sociability testing

Question 240

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

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

Question 241

The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

- ☐ confirm that the auditors did not overlook any important issues.
- ☐ gain agreement on the findings.
- ☐ receive feedback on the adequacy of the audit procedures.
- ☐ test the structure of the final presentation.

Question 242

An IS auditor analyzing the audit log of a database management system (DBMS) finds that some transactions were partially executed as a result of an error, and are not rolled back. Which of the following transaction processing features has been violated?

- ☐ Consistency
- ☐ Isolation
- ☐ Durability
- ☐ Atomicity

Question 243

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

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

Question 244

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

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

Question 245

Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:

- ☐ include the statement of management in the audit report.
- ☐ identify whether such software is, indeed, being used by the organization.
- ☐ reconfirm with management the usage of the software.
- ☐ discuss the issue with senior management since reporting this could have a negative impact on the organization.

Question 246

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 247

The PRIMARY objective of business continuity and disaster recovery plans should be to:

- ☐ safeguard critical IS assets.
- ☐ provide for continuity of operations.
- ☐ minimize the loss to an organization.
- ☐ protect human life.

Question 248

Which of the following data validation edits is effective in detecting transposition and transcription errors?

- ☐ Range check
- ☐ Check digit
- ☐ Validity check
- ☐ Duplicate check

Question 249

Which of the following would create the GREATEST risk when migrating a critical legacy system to a new system?

- ☐ Using agile development methodology
- ☐ Following a phased approach
- ☐ Following a direct cut-over approach
- ☐ Maintaining parallel systems

Question 250

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 251

E-mail message authenticity and confidentiality is BEST achieved by signing the message using the:

- ☐ sender's private key and encrypting the message using the receiver's public key.
- ☐ sender's public key and encrypting the message using the receiver's private key.
- ☐ receiver's private key and encrypting the message using the sender's public key.
- ☐ receiver's public key and encrypting the message using the sender's private key.

Question 252

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 253

When an organization and its IT-hosting service provider are establishing a contract with each other, it is MOST important that the contract includes:

- ☐ each party's security responsibilities
- ☐ details of expected security metrics
- ☐ penalties for noncompliance with security policy
- ☐ recovery time objectives (RTOs)

Question 254

Which of the following network components is PRIMARILY set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

- ☐ Firewalls
- ☐ Routers
- ☐ Layer 2 switches
- ☐ VLANs

Question 255

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 256

Which of the following is not a common method of multiplexing data?

- ☐ Analytical multiplexing
- ☐ Time-division multiplexing
- ☐ Asynchronous time-division multiplexing
- ☐ Frequency division multiplexing

Question 257

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

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

Question 258

Which of the following controls can BEST detect accidental corruption during transmission of data across a network?

- ☐ Sequence checking
- ☐ Parity checking
- ☐ Symmetric encryption
- ☐ Check digit verification

Question 259

An organization has outsourced its wide area network (WAN) to a third-party service provider. Under these circumstances, which of the following is the PRIMARY task the IS auditor should perform during an audit of business continuity (BCP) and disaster recovery planning (DRP)?

- ☐ Review whether the service provider's BCP process is aligned with the organization's BCP and contractual obligations.
- ☐ Review whether the service level agreement (SLA) contains a penalty clause in case of failure to meet the level of service in case of a disaster.
- ☐ Review the methodology adopted by the organization in choosing the service provider.
- ☐ Review the accreditation of the third-party service provider's staff.

Question 260

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 261

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 262

The MOST important reason for documenting all aspects of a digital forensic investigation is that documentation:

- ☐ provides traceability for independent investigation by third parties.
- ☐ ensures compliance with corporate incident response policies.
- ☐ ensures the process will be repeatable in future investigations.
- ☐ meets IT audit documentation standards.

Question 263

An organization is using an enterprise resource management (ERP) application. Which of the following would be an effective access control?

- ☐ User-level permissions
- ☐ Role-based
- ☐ Fine-grained
- ☐ Discretionary

Question 264

Which of the following cloud deployment model can be shared by several organizations?

- ☐ Private Cloud\
- ☐ Community Cloud
- ☐ Public Cloud
- ☐ Hybrid Cloud

Question 265

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 266

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 267

Which of the following should an IS auditor determine FIRST when evaluating additional hardware required to support the acquisition of a new accounting system?

- ☐ A training program has been developed to support the new accounting system.
- ☐ The supplier has experience supporting accounting systems.
- ☐ The hardware specified will be compliant with the current IT strategy.
- ☐ The hardware will be installed in a secure and environmentally controlled area.

Question 268

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 269

Which of the following fourth generation language is a development tools to generate lower level programming languages?

- ☐ Query and report generator
- ☐ Embedded database 4GLs
- ☐ Relational database 4GL
- ☐ Application generators

Question 270

An IT governance framework provides an organization with:

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

Question 271

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 272

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 273

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 274

An organization is MOST at risk from a new worm being introduced through the intranet when:

- ☐ executable code is run from inside the firewall
- ☐ system software does not undergo integrity checks
- ☐ hosts have static IP addresses
- ☐ desktop virus definition files are not up to date

Question 275

An information security risk analysis BEST assists an organization in ensuring that:

- ☐ cost-effective decisions are made with regard to which assets need protection
- ☐ the organization implements appropriate security technologies
- ☐ the infrastructure has the appropriate level of access control
- ☐ an appropriate level of funding is applied to security processes

Question 276

When reviewing an intrusion detection system (IDS), an IS auditor should be MOST concerned about which of the following?

- ☐ Number of nonthreatening events identified as threatening
- ☐ Attacks not being identified by the system
- ☐ Reports/logs being produced by an automated tool
- ☐ Legitimate traffic being blocked by the system

Question 277

The MOST useful technique for maintaining management support for the information security program is:

- ☐ identifying the risks and consequences of failure to comply with standards
- ☐ benchmarking the security programs of comparable organizations
- ☐ implementing a comprehensive security awareness and training program
- ☐ informing management about the security of business operations

Question 278

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

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

Question 279

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

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

Question 280

Whenever business processes have been re-engineered, the IS auditor attempts to identify and quantify the impact of any controls that might have been removed, or controls that might not work as effectively after business process changes. True or false?

- ☐ True
- ☐ False

Question 281

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 282

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 283

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 284

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

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

Question 285

Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

- ☐ Function point analysis
- ☐ Earned value analysis
- ☐ Cost budget
- ☐ Program Evaluation and Review Technique

Question 286

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 287

An organization developed a comprehensive three-year IT strategic plan. Halfway into the plan, a major legislative change impacting the organization is enacted. Which of the following should be management's NEXT course of action?

- ☐ Develop specific procedural documentation related to the changed legislation.
- ☐ Assess the legislation to determine whether are required to the strategic IT plan.
- ☐ Perform a risk management of the legislative changes.
- ☐ Develop a new IT strategic plan that encompasses the new legislation.

Question 288

Which of the following can degrade network performance?

- ☐ Superfluous use of redundant load-sharing gateways
- ☐ Increasing traffic collisions due to host congestion by creating new collision domains
- ☐ Inefficient and superfluous use of network devices such as switches
- ☐ Inefficient and superfluous use of network devices such as hubs

Question 289

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 290

Vendors have released patches fixing security flaws in their software. Which of the following should an IS auditor recommend in this situation?

- ☐ Assess the impact of patches prior to installation.
- ☐ Ask the vendors for a new software version with all fixes included.
- ☐ install the security patch immediately.
- ☐ Decline to deal with these vendors in the future.

Question 291

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 292

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 293

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 294

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 295

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 296

An IS auditor has completed a review of an outsourcing agreement and has identified IT governance issues. Which of the following is the MOST effective and efficient way of communicating the issues at a meeting with senior management?

- ☐ Present a completed report and discuss the details.
- ☐ Provide a detailed report in advance and open the floor to questions.
- ☐ Present an overview highlighting the key findings.
- ☐ Provide a plan of action and milestones.

Question 297

Which of the following is the PRIMARY responsibility of an organization's information security function?

- ☐ Reviewing unauthorized attempts to access sensitive files
- ☐ Managing the organization's security procedures
- ☐ Approving access to data files
- ☐ Installing network security programs

Question 298

When developing a risk-based audit strategy, an IS auditor conduct a risk assessment to ensure that:

- ☐ controls needed to mitigate risks are in place.
- ☐ vulnerabilities and threats are identified.
- ☐ audit risks are considered.
- ☐ a gap analysis is appropriate.

Question 299

Which of the following is the BEST way to facilitate proper follow-up for audit findings?

- ☐ Schedule a follow-up audit for two weeks after the initial audit was completed.
- ☐ Conduct a surprise audit to determine whether remediation is in progress.
- ☐ Conduct a follow-up audit when findings escalate to incidents.
- ☐ Schedule a follow-up audit based on remediation due dates.

Question 300

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 301

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 302

Phishing attack works primarily through:

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

Question 303

Which of the following is MOST likely to be prevented by a firewall connected to the Internet?

- ☐ Dial-in penetration attacks
- ☐ Disclosure of public key infrastructure (PKI) keys
- ☐ Alteration of email message content
- ☐ External spoofing of internal addresses

Question 304

Which of the following term in business continuity determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 305

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 306

In which of the following transmission media it is MOST difficult to modify the information traveling across the network?

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

Question 307

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 308

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 309

Applying a digital signature to data traveling in a network provides:

- ☐ confidentiality and integrity.
- ☐ security and nonrepudiation.
- ☐ integrity and nonrepudiation.
- ☐ confidentiality and nonrepudiation.

Question 310

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 311

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 312

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 313

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 314

When conducting a post-implementation review, which of the following is the BEST way to determine whether the value from an IT project has been achieved?

- ☐ Calculated the return on investment (ROI).
- ☐ Interview stakeholders.
- ☐ Conduct an earned value analysis (EVA).
- ☐ Survey end users.

Question 315

Which of the following is the client organization's responsibility in a Software as a Service (SaaS) environment?

- ☐ Detecting unauthorized access
- ☐ Ensuring that users are properly authorized
- ☐ Ensuring the data is available when needed
- ☐ Preventing insertion of malicious code

Question 316

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 317

When using an integrated test facility (ITF), an IS auditor should ensure that:

- ☐ production data are used for testing.
- ☐ test data are isolated from production data.
- ☐ a test data generator is used.
- ☐ master files are updated with the test data.

Question 318

Which of the following is the GREATEST concern associated with control self-assessments?

- ☐ Employees may have insufficient awareness of controls
- ☐ Controls may not be assessed objectively
- ☐ Communication between operational management and senior management may not be effective
- ☐ The assessment may not provide sufficient assurance to stakeholders

Question 319

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 320

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 321

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 322

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 323

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 324

An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's MAIN concern should be that the:

- ☐ complexity and risks associated with the project have been analyzed.
- ☐ resources needed throughout the project have been determined.
- ☐ project deliverables have been identified.
- ☐ a contract for external parties involved in the project has been completed.

Question 325

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 326

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 327

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 328

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

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

Question 329

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

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

Question 330

The PRIMARY goal of a web site certificate is:

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

Question 331

An IS auditor examining the configuration of an operating system to verify the controls should review the:

- ☐ transaction logs.
- ☐ authorization tables.
- ☐ parameter settings.
- ☐ routing tables.

Question 332

What is the MOST important business concern when an organization is about to migrate a mission-critical application to a virtual environment?

- ☐ The organization's experience with virtual applications
- ☐ Adequacy of the fallback procedures
- ☐ Confidentiality of network traffic
- ☐ Adequacy of the virtual architecture

Question 333

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 334

During a follow-up audit, an IS auditor finds that the auditee has updated virus scanner definitions without adopting the original audit recommendation to increase the frequency of using the scanner. The MOST appropriate action for the auditor is to:

- ☐ prepare a follow-up audit report reiterating the recommendation.
- ☐ escalate the issue to senior management.
- ☐ modify the audit opinion based on the new information available.
- ☐ conclude that the residual risk is beyond tolerable levels of risk.

Question 335

A penetration test performed as part of evaluating network security:

- ☐ provides assurance that all vulnerabilities are discovered.
- ☐ should be performed without warning the organization's management.
- ☐ exploits the existing vulnerabilities to gain unauthorized access.
- ☐ would not damage the information assets when performed at network perimeters.

Question 336

Functional acknowledgements are used:

- ☐ as an audit trail for EDI transactions.
- ☐ to functionally describe the IS department.
- ☐ to document user roles and responsibilities.
- ☐ as a functional description of application software.

Question 337

Which of the following statement correctly describes the difference between IPSec and SSH protocols?

- ☐ IPSec works at the transport layer where as SSH works at the network layer of an OSI Model
- ☐ IPSec works at the network layer where as SSH works at the application layer of an OSI Model
- ☐ IPSec works at the network layer and SSH works at the transport layer of an OSI Model
- ☐ IPSec works at the transport layer and SSH works at the network layer of an OSI Model

Question 338

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 339

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 340

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 341

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 342

A message is being sent with a hash. The risk of an attacker changing the message and generating an authentic hash value can be mitigated by:

- ☐ requiring the recipient to use a different hash algorithm.
- ☐ generating hash output that is the same size as the original message.
- ☐ using a secret key in conjunction with the hash algorithm.
- ☐ using the sender's public key to encrypt the message.

Question 343

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 344

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 345

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 346

An intruder accesses an application server and makes changes to the system log. Which of the following would enable the identification of the changes?

- ☐ Mirroring the system log on another server
- ☐ Simultaneously duplicating the system log on a write-once disk
- ☐ Write-protecting the directory containing the system log
- ☐ Storing the backup of the system log offsite

Question 347

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 348

A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

- ☐ what amount of progress against schedule has been achieved.
- ☐ if the project budget can be reduced.
- ☐ if the project could be brought in ahead of schedule.
- ☐ if the budget savings can be applied to increase the project scope.

Question 349

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 350

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 351

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 352

Which of the following is the MOST effective way to ensure security policies are relevant to organizational business practices?

- ☐ Leverage security steering committee contribution.
- ☐ Obtain senior management sign-off.
- ☐ Integrate industry best practices.
- ☐ Conduct an organization-wide security audit.

Question 353

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 354

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 355

During an audit of a financial application, it was determined that many terminated users' accounts were not disabled. Which of the following should be the IS auditor's NEXT step?

- ☐ Perform a review of terminated users' account activity.
- ☐ Conclude that IT general controls are ineffective.
- ☐ Communicate risks to the application owner.
- ☐ Perform substantive testing of terminated users' access rights.

Question 356

What is the recommended minimum length of a good password?

- ☐ 6 characters
- ☐ 8 characters
- ☐ 12 characters
- ☐ 18 characters
- ☐ 22 characters
- ☐ None of the choices.

Question 357

Internal audit reports should be PRIMARILY written for and communicated to:

- ☐ audit management, as they are responsible for the quality of the audit.
- ☐ external auditors, as they provide an opinion on the financial statements.
- ☐ auditees, as they will eventually have to implement the recommendations.
- ☐ senior management, as they should be informed about the identified risks.

Question 358

For application acquisitions with significant impacts, participation of your IS audit team should be encouraged:

- ☐ early in the due diligence stage.
- ☐ at the testing stage.
- ☐ at the final approval stage.
- ☐ at the budget preparation stage.
- ☐ None of the choices.

Question 359

The Trojan.Linux.JBellz Trojan horse runs as a malformed file of what format?

- ☐ e-mails.
- ☐ MP3.
- ☐ MS Office.
- ☐ Word template.
- ☐ None of the choices.

Question 360

Which of the following is the MOST effective control to minimize the risk of cross-site scripting (XSS)?

- ☐ Periodic vulnerability assessments
- ☐ Secure coding practices
- ☐ Network intrusion prevention system
- ☐ Web firewall policy

Question 361

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 362

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 363

Integrating business continuity planning (BCP) into an IT project aids in:

- ☐ the retrofitting of the business continuity requirements.
- ☐ the development of a more comprehensive set of requirements.
- ☐ the development of a transaction flowchart.
- ☐ ensuring the application meets the user's needs.

Question 364

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 365

With the objective of mitigating the risk and impact of a major business interruption, a disaster recovery plan should endeavor to reduce the length of recovery time necessary, as well as costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs. True or false?

- ☐ True
- ☐ False

Question 366

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 367

Which of the following type of testing validate functioning of the application under test with other system, where a set of data is transferred from one system to another?

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

Question 368

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 369

In an audit of an inventory application, which approach would provide the BEST evidence that purchase orders are valid?

- ☐ Testing whether inappropriate personnel can change application parameters
- ☐ Tracing purchase orders to a computer listing
- ☐ Comparing receiving reports to purchase order details
- ☐ Reviewing the application documentation

Question 370

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 371

Your final audit report should be issued:

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

Question 372

An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:

- ☐ EDI trading partner agreements.
- ☐ physical controls for terminals.
- ☐ authentication techniques for sending and receiving messages.
- ☐ program change control procedures.

Question 373

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 374

What is the MOST prevalent security risk when an organization implements remote virtual private network (VPN) access to its network?

- ☐ Malicious code could be spread across the network
- ☐ VPN logon could be spoofed
- ☐ Traffic could be sniffed and decrypted
- ☐ VPN gateway could be compromised

Question 375

Which of the following term in business continuity determines the maximum tolerable amount of time needed to bring all critical systems back online after disaster occurs?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 376

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

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

Question 377

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 378

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 379

Which of the following should be an information security manager's MOST important consideration when conducting a physical security review of a potential outsourced data center?

- ☐ Environmental factors of the surrounding location
- ☐ Proximity to law enforcement
- ☐ Availability of network circuit connections
- ☐ Distance of the data center from the corporate office

Question 380

Which of the following term in business continuity determines the maximum acceptable amount of data loss measured in time?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 381

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 382

Effective transactional controls are often capable of offering which of the following benefits (Choose four.):

- ☐ reduced administrative and material costs
- ☐ shortened contract cycle times
- ☐ enhanced procurement decisions
- ☐ diminished legal risk
- ☐ None of the choices.

Question 383

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 384

An IS auditor is evaluating the security of an organization's data backup process, which includes the transmission of daily incremental backups to a dedicated offsite server. Which of the following findings poses the GREATEST risk to the organization?

- ☐ Backup transmissions are not encrypted
- ☐ Backup transmissions occasionally fail
- ☐ Data recovery testing is conducted once per year
- ☐ The archived data log is incomplete

Question 385

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 386

IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

- ☐ The outsourcing contract does not cover disaster recovery for the outsourced IT operations.
- ☐ The service provider does not have incident handling procedures.
- ☐ Recently a corrupted database could not be recovered because of library management problems.
- ☐ incident logs are not being reviewed.

Question 387

As described at security policy, the CSO implemented an e-mail package solution that allows for ensuring integrity of messages sent using SMIME. Which of the options below BEST describes how it implements the environment to suite policy's requirement?

- ☐ Implementing PGP and allowing for recipient to receive the private key used to sign e-mail message.
- ☐ Implementing RSA standard for messages envelope and instructing users to sign all messages using their private key from their PKI digital certificate.
- ☐ Implementing RSA standard for messages envelope and instructing users to sign all messages using their public key from their PKI digital certificate.
- ☐ Implementing MIME solutions and providing a footer within each message sent, referencing to policy constraints related to e-mail usage.

Question 388

A source code repository should be designed to:

- ☐ provide automatic incorporation and distribution of modified code.
- ☐ prevent changes from being incorporated into existing code.
- ☐ provide secure versioning and backup capabilities for existing code.
- ☐ prevent developers from accessing secure source code.

Question 389

Which of the following statement correctly describes the difference between black box testing and white box testing?

- ☐ Black box testing focuses on functional operative effectiveness where as white box assesses the effectiveness of software program logic
- ☐ White box testing focuses on functional operative effectiveness where as black box assesses the effectiveness of software program logic
- ☐ White box and black box testing focuses on functional operative effectiveness of an information systems without regard to any internal program structure
- ☐ White box and black box testing focuses on the effectiveness of the software program logic

Question 390

Which of the following could lead to an unintentional loss of confidentiality?

- ☐ Lack of employee awareness of a company's information security policy
- ☐ Failure to comply with a company's information security policy
- ☐ A momentary lapse of reason
- ☐ Lack of security policy enforcement procedures

Question 391

A company uses a standard form to document and approve all changes in production programs. To ensure that the forms are properly authorized, which of the following is the MOST effective sampling method?

- ☐ Attribute
- ☐ Variable
- ☐ Discovery
- ☐ Monetary

Question 392

Which of the following is the PRIMARY objective of an IT performance measurement process?

- ☐ Minimize errors
- ☐ Gather performance data
- ☐ Establish performance baselines
- ☐ Optimize performance

Question 393

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 394

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

- ☐ Physical access control like locks and door
- ☐ User login screen which allows only authorize user to access website
- ☐ Encrypt the data so that only authorize user can view the same
- ☐ Duplicate checking of a calculations

Question 395

An IT management group has developed a standardized security control checklist and distributed it to the control self-assessors in each organizational unit. Which of the following would be the GREATEST risk in this approach?

- ☐ Delayed feedback may increase exposures
- ☐ Over time the checklist may become outdated
- ☐ Assessors may manipulate the results
- ☐ Business-specific vulnerabilities may be overlooked

Question 396

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 397

An IS auditor is involved with a project and finds an IT project stakeholder wants to make a change that could affect both the project scope and schedule. Which of the following would be the MOST appropriate action for the project manager with respect to the change request?

- ☐ Recommend to the project sponsor whether to approve the change
- ☐ Modify the project plan as a result of the change
- ☐ Evaluate the impact of the change
- ☐ Ignore out-of-scope requests

Question 398

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 399

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 400

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 401

Which of the following would prevent accountability for an action performed, thus allowing nonrepudiation?

- ☐ Proper authentication
- ☐ Proper identification AND authentication
- ☐ Proper identification
- ☐ Proper identification, authentication, AND authorization

Question 402

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 403

An organization is in the process of deciding whether to allow a bring your own device (BYOD) program. If approved, which of the following should be the FIRST control required before implementation?

- ☐ Device baseline configurations
- ☐ Device registration
- ☐ An acceptable use policy
- ☐ An awareness program

Question 404

During a security audit, which of the following is MOST important to review to ensure data confidentiality is managed?

- ☐ Access controls
- ☐ Data flows
- ☐ Access log monitoring
- ☐ Network configuration

Question 405

Software is considered malware based on:

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

Question 406

Which of the following attack involves sending forged ICMP Echo Request packets to the broadcast address on multiple gateways in order to illicit responses from the computers behind the gateway where they all respond back with ICMP Echo Reply packets to the source IP address of the ICMP Echo Request packets?

- ☐ Reflected attack
- ☐ Brute force attack
- ☐ Buffer overflow
- ☐ Pulsing Zombie

Question 407

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

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

Question 408

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 409

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 410

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 411

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 412

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

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

Question 413

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

- ☐ True
- ☐ False

Question 414

Which of the following should be the MOST important consideration when implementing an information security framework?

- ☐ Compliance requirements
- ☐ Audit findings
- ☐ Technical capabilities
- ☐ Risk appetite

Question 415

Library control software restricts source code to:

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

Question 416

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 417

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 418

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

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

Question 419

Which of the following is the BEST way to detect software license violations?

- ☐ Implementing a corporate policy on copyright infringements and software use.
- ☐ Requiring that all PCs be diskless workstations.
- ☐ Installing metering software on the LAN so applications can be accessed through the metered software.
- ☐ Regularly scanning PCs in use to ensure that unauthorized copies of software have not been loaded on the PC.

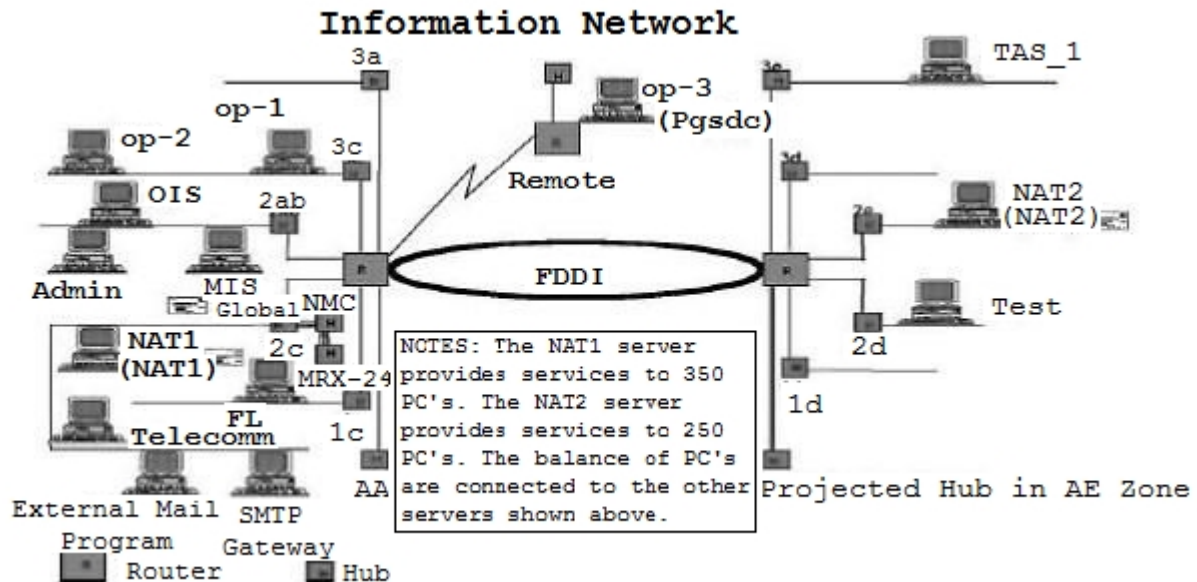
Question 420

A small organization is experiencing rapid growth and plans to create a new information security policy. Which of the following is MOST relevant to creating the policy?

- ☐ Industry standards
- ☐ The business impact analysis
- ☐ The business objectives
- ☐ Previous audit recommendations

Question 421

Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?



- ☐ No firewalls are needed
- ☐ Op-3 location only
- ☐ MIS (Global) and NAT2
- ☐ SMTP Gateway and op-3

Question 422

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

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

Question 423

Responsibility for the governance of IT should rest with the:

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

Question 424

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 425

Which of the following BEST describes the role of a directory server in a public key infrastructure (PKI)?

- ☐ Encrypts the information transmitted over the network
- ☐ Makes other users' certificates available to applications
- ☐ Facilitates the implementation of a password policy
- ☐ Stores certificate revocation lists (CRLs)

Question 426

Which of the following type of lock uses a numeric keypad or dial to gain entry?

- ☐ Bolting door locks
- ☐ Cipher lock
- ☐ Electronic door lock
- ☐ Biometric door lock

Question 427

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 428

An organization has outsourced some of its subprocesses to a service provider. When scoping the audit of the provider, the organization's internal auditor should FIRST:

- ☐ evaluate operational controls of the provider
- ☐ discuss audit objectives with the provider
- ☐ review internal audit reports of the provider
- ☐ review the contract with the provider

Question 429

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 430

Neural networks are effective in detecting fraud because they can:

- ☐ discover new trends since they are inherently linear.
- ☐ solve problems where large and general sets of training data are not obtainable.
- ☐ attack problems that require consideration of a large number of input variables.
- ☐ make assumptions about the shape of any curve relating variables to the output.

Question 431

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 432

Failure in which of the following testing stages would have the GREATEST impact on the implementation of new application software?

- ☐ System testing
- ☐ Acceptance testing
- ☐ Integration testing
- ☐ Unit testing

Question 433

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 434

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 435

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 436

Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

- ☐ Assimilation of the framework and intent of a written security policy by all appropriate parties
- ☐ Management support and approval for the implementation and maintenance of a security policy
- ☐ Enforcement of security rules by providing punitive actions for any violation of security rules
- ☐ Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Question 437

Which of the following layer in in an enterprise data flow architecture is directly death with by end user with information?

- ☐ Desktop access layer
- ☐ Data preparation layer
- ☐ Data mart layer
- ☐ Data access layer

Question 438

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 439

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 440

Which of the following are valid examples of Malware:

- ☐ viruses
- ☐ worms
- ☐ trojan horses
- ☐ spyware
- ☐ All of the above

Question 441

In reviewing the IT strategic plan, the IS auditor should consider whether it identifies the:

- ☐ major IT initiatives.
- ☐ links to operational tactical plans.
- ☐ allocation of IT staff
- ☐ project management methodologies used.

Question 442

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 443

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 444

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

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

Question 445

Which of the following measures can protect systems files and data, respectively?

- ☐ User account access controls and cryptography
- ☐ User account access controls and firewall
- ☐ User account access controls and IPS
- ☐ IDS and cryptography
- ☐ Firewall and cryptography
- ☐ None of the choices.

Question 446

Which of the following term related to network performance refers to the maximum rate that information can be transferred over a network?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Jitter

Question 447

What is used as a control to detect loss, corruption, or duplication of data?

- ☐ Redundancy check
- ☐ Reasonableness check
- ☐ Hash totals
- ☐ Accuracy check

Question 448

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 449

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 450

Which of the following concerns associated with the World Wide Web would be addressed by a firewall?

- ☐ Unauthorized access from outside the organization
- ☐ Unauthorized access from within the organization
- ☐ A delay in Internet connectivity
- ☐ A delay in downloading using File Transfer Protocol (FTP)

Question 451

An organization can ensure that the recipients of e-mails from its employees can authenticate the identity of the sender by:

- ☐ digitally signing all e-mail messages.
- ☐ encrypting all e-mail messages.
- ☐ compressing all e-mail messages.
- ☐ password protecting all e-mail messages.

Question 452

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

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

Question 453

The FIRST step in data classification is to:

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

Question 454

The use of residual biometric information to gain unauthorized access is an example of which of the following attacks?

- ☐ Replay
- ☐ Brute force
- ☐ Cryptographic
- ☐ Mimic

Question 455

An IS audit manager has been asked to perform a quality review on an audit that the same manager also supervised. Which of the following is the manager's BEST response to this situation?

- ☐ Notify the audit committee of the situation.
- ☐ Escalate the situation to senior audit leadership.
- ☐ Determine whether audit evidence supports audit conclusions.
- ☐ Discuss with the audit team to understand how conclusions were reached.

Question 456

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 457

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 458

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 459

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

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

Question 460

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 461

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

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

Question 462

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

- ☐ HTTP
- ☐ FTP
- ☐ NTP
- ☐ TCP

Question 463

A data center has a badge-entry system. Which of the following is MOST important to protect the computing assets in the center?

- ☐ Badge readers are installed in locations where tampering would be noticed
- ☐ The computer that controls the badge system is backed up frequently
- ☐ A process for promptly deactivating lost or stolen badges exists
- ☐ All badge entry attempts are logged

Question 464

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 465

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 466

Which of the following provides the best evidence of the adequacy of a security awareness program?

- ☐ The number of stakeholders including employees trained at various levels
- ☐ Coverage of training at all locations across the enterprise
- ☐ The implementation of security devices from different vendors
- ☐ Periodic reviews and comparison with best practices

Question 467

When information security management is receiving an increased number of false positive incident reports, which of the following is MOST important to review?

- ☐ The security awareness programs
- ☐ Post-incident analysis results
- ☐ The risk management processes
- ☐ Firewall logs

Question 468

The effectiveness of an information security governance framework will BEST be enhanced if:

- ☐ consultants review the information security governance framework
- ☐ a culture of legal and regulatory compliance is promoted by management
- ☐ IS auditors are empowered to evaluate governance activities
- ☐ risk management is built into operational and strategic activities

Question 469

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 470

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 471

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

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

Question 472

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

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

Question 473

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 474

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 475

The information security function in a large organization is MOST effective when:

- ☐ decentralized as close to the user as possible.
- ☐ the function reports directly to the IS operations manager.
- ☐ partnered with the IS development team to determine access rights.
- ☐ established at a corporate-wide level.

Question 476

Who is responsible for authorizing access level of a data user?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☐ Security Administrator

Question 477

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 478

An IS auditor observes a weakness in the tape management system at a data center in that some parameters are set to bypass or ignore tape header records. Which of the following is the MOST effective compensating control for this weakness?

- ☐ Staging and job set up
- ☐ Supervisory review of logs
- ☐ Regular back-up of tapes
- ☐ Offsite storage of tapes

Question 479

Which of the following is an analytical review procedure for a payroll system?

- ☐ Performing penetration attempts on the payroll system
- ☐ Evaluating the performance of the payroll system, using benchmarking software
- ☐ Performing reasonableness tests by multiplying the number of employees by the average wage rate
- ☐ Testing hours reported on time sheets

Question 480

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

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

Question 481

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 482

Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?

- ☐ increase the time allocated for system testing
- ☐ implement formal software inspections
- ☐ increase the development staff
- ☐ Require the sign-off of all project deliverables

Question 483

ALL computer programming languages are vulnerable to command injection attack.

- ☐ True
- ☐ False

Question 484

If an IS auditor finds evidence of risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function, what is the auditor's primary responsibility?

- ☐ To advise senior management.
- ☐ To reassign job functions to eliminate potential fraud.
- ☐ To implement compensator controls.
- ☐ Segregation of duties is an administrative control not considered by an IS auditor.

Question 485

Which of the following device in Frame Relay WAN technique is generally customer owned device that provides a connectivity between company's own network and the frame relays network?

- ☐ DTE
- ☐ DCE
- ☐ DME
- ☐ DLE

Question 486

An IS auditor determines that a business continuity plan has not been reviewed and approved by management. Which of the following is the MOST significant risk associated with this situation?

- ☐ Continuity planning may be subject to resource constraints.
- ☐ The plan may not be aligned with industry best practice.
- ☐ Critical business processes may not be addressed adequately.
- ☐ The plan has not been reviewed by risk management.

Question 487

Which of the following IT governance best practices improves strategic alignment?

- ☐ Supplier and partner risks are managed.
- ☐ A knowledge base on customers, products, markets and processes is in place.
- ☐ A structure is provided that facilitates the creation and sharing of business information.
- ☐ Top management mediate between the imperatives of business and technology.

Question 488

What would an IS auditor expect to find in the console log?

- ☐ Evidence of password spoofing
- ☐ System errors
- ☐ Evidence of data copy activities
- ☐ Evidence of password sharing

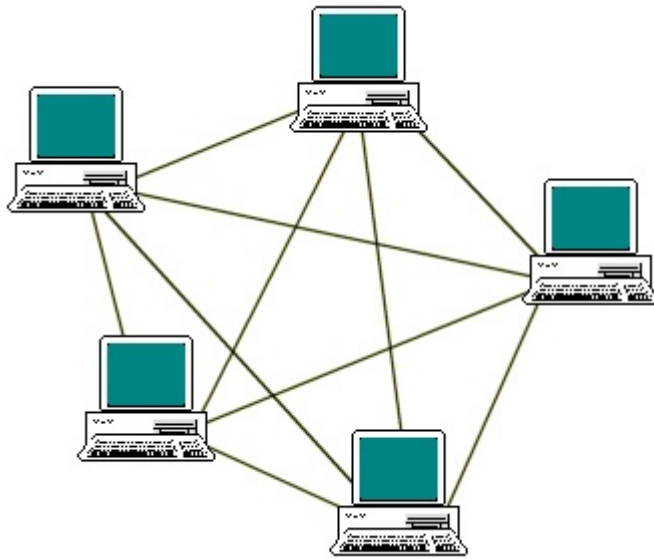
Question 489

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 490

Identify the network topology from below diagram presented below:



Network Topology

- ☐ Bus
- ☐ Star
- ☐ Ring
- ☐ Mesh

Question 491

An IS auditor is planning on utilizing attribute sampling to determine the error rate for health care claims processed. Which of the following factors will cause the sample size to decrease?

- ☐ Population size increase
- ☐ Expected error rate increase
- ☐ Acceptable risk level decrease
- ☐ Tolerate error rate increase

Question 492

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 493

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 494

In which of the following WAN message transmission technique does two network nodes establish a dedicated communications channel through the network before the nodes may communicate?

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

Question 495

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

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

Question 496

Which of the following is BEST suited for secure communications within a small group?

- ☐ Key distribution center
- ☐ Certification authority
- ☐ Web of trust
- ☐ Kerberos Authentication System

Question 497

Which of the following would provide the BEST justification for a new information security investment?

- ☐ Defined key performance indicators (KPIs)
- ☐ Projected reduction in risk
- ☐ Results of a comprehensive threat analysis
- ☐ Senior management involvement in project prioritization

Question 498

When installing an intrusion detection system (IDS), which of the following is MOST important?

- ☐ Properly locating it in the network architecture
- ☐ Preventing denial-of-service (DoS) attacks
- ☐ Identifying messages that need to be quarantined
- ☐ Minimizing the rejection errors

Question 499

Which of the following PBX feature provides the possibility to break into a busy line to inform another user of an important message?

- ☐ Account Codes
- ☐ Access Codes
- ☐ Override
- ☐ Tenanting

Question 500

Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits vulnerability in a protocol?

- ☐ Install the vendor's security fix for the vulnerability.
- ☐ Block the protocol traffic in the perimeter firewall.
- ☐ Block the protocol traffic between internal network segments.
- ☐ Stop the service until an appropriate security fix is installed.

Question 501

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 502

Which of the following ensures a sender's authenticity and an e-mail's confidentiality?

- ☐ Encrypting the hash of the message with the sender's private key and thereafter encrypting the hash of the message with the receiver's public key
- ☐ The sender digitally signing the message and thereafter encrypting the hash of the message with the sender's private key
- ☐ Encrypting the hash of the message with the sender's private key and thereafter encrypting the message with the receiver's public key
- ☐ Encrypting the message with the sender's private key and encrypting the message hash with the receiver's public key.

Question 503

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 504

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 505

An IS auditor is performing an audit of a large organization's operating system maintenance procedures. Which of the following findings presents the GREATEST risk?

- ☐ Some internal servers cannot be patched due to software incompatibility.
- ☐ The configuration management database is not up-to-date.
- ☐ Vulnerability testing is not performed on the development servers.
- ☐ Critical patches are applied immediately while others follow quarterly release cycles.

Question 506

Which of the following is the unique identifier within an IPsec packet that enables the sending host to reference the security parameter to apply?

- ☐ SPI
- ☐ SA
- ☐ ESP
- ☐ AH

Question 507

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 508

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

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

Question 509

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

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

Question 510

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

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

Question 511

A review of an organization's IT portfolio revealed several applications that are not in use. The BEST way to prevent this situation from recurring would be to implement:

- ☐ a formal request for proposal (RFP) process
- ☐ an information asset acquisition policy
- ☐ asset life cycle management
- ☐ business development procedures

Question 512

A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:

- ☐ payroll reports should be compared to input forms.
- ☐ gross payroll should be recalculated manually.
- ☐ checks (cheques) should be compared to input forms.
- ☐ checks (cheques) should be reconciled with output reports.

Question 513

When implementing an application software package, which of the following presents the GREATEST risk?

- ☐ Uncontrolled multiple software versions
- ☐ Source programs that are not synchronized with object code
- ☐ incorrectly set parameters
- ☐ Programming errors.

Question 514

A third-party service provider has proposed a data loss prevention (DLP) solution. Which of the following MUST be in place for this solution to be relevant to the organization?

- ☐ An adequate data testing environment
- ☐ Senior management support
- ☐ A business case
- ☐ A data classification

Question 515

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 516

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 517

When reviewing system parameters, an IS auditor's PRIMARY concern should be that:

- ☐ they are set to meet security and performance requirements.
- ☐ changes are recorded in an audit trail and periodically reviewed.
- ☐ changes are authorized and supported by appropriate documents.
- ☐ access to parameters in the system is restricted.

Question 518

As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up on tape. During the backup procedure, a drive malfunctions and the order entry files are lost. Which of the following is necessary to restore these files?

- ☐ The previous day's backup file and the current transaction tape
- ☐ The previous day's transaction file and the current transaction tape
- ☐ The current transaction tape and the current hard copy transaction log
- ☐ The current hard copy transaction log and the previous day's transaction file

Question 519

With respect to business continuity strategies, an IS auditor interviews key stakeholders in an organization to determine whether they understand their roles and responsibilities. The IS auditor is attempting to evaluate the:

- ☐ clarity and simplicity of the business continuity plans.
- ☐ adequacy of the business continuity plans.
- ☐ effectiveness of the business continuity plans.
- ☐ ability of IS and end-user personnel to respond effectively in emergencies.

Question 520

Intrusion detection systems (IDSs) can:

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

Question 521

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 522

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 523

Which of the following control provides an alternative measure of control?

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

Question 524

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

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

Question 525

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

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

Question 526

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 527

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

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

Question 528

An IS auditor reviewing the acquisition of new equipment would consider which of the following to be a significant weakness?

- ☐ Staff involved in the evaluation were aware of the vendors being evaluated.
- ☐ Independent consultants prepared the request for proposal (RFP) documents.
- ☐ Evaluation criteria were finalized after the initial assessment of responses.
- ☐ The closing date for responses was extended after a request from potential vendors.

Question 529

An accuracy measure for a biometric system is:

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

Question 530

A hacker could obtain passwords without the use of computer tools or programs through the technique of:

- ☐ social engineering.
- ☐ sniffers.
- ☐ back doors.
- ☐ Trojan horses.

Question 531

To BEST evaluate the effectiveness of a disaster recovery plan, the IS auditor should review the:

- ☐ test plan and results of past tests.
- ☐ plans and procedures in the business continuity plan.
- ☐ capacity of backup facilities.
- ☐ hardware and software inventory.

Question 532

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 533

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 534

Identify the correct sequence of Business Process Reengineering (BPR) application steps from the given choices below?

- ☐ Envision, Initiate, Diagnose, Redesign, Reconstruct and Evaluate
- ☐ Initiate, Envision, Diagnose, Redesign, Reconstruct and Evaluate
- ☐ Envision, Diagnose, Initiate, Redesign, Reconstruct and Evaluate
- ☐ Evaluate, Envision, Initiate, Diagnose, Redesign, Reconstruct

Question 535

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 536

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 537

Which of the following practices associated with capacity planning provides the GREATEST assurance that future incidents related to server performance will be prevented?

- ☐ Anticipating current service level agreements (SLAs) will remain unchanged
- ☐ Prorating the current processing workloads
- ☐ Negotiating agreements to acquire required cloud services
- ☐ Duplicating existing disk drive systems to improve redundancy and data storage

Question 538

Which of the following is MOST likely to result from a business process reengineering (BPR) project?

- ☐ An increased number of people using technology
- ☐ Significant cost savings, through a reduction in the complexity of information technology
- ☐ A weaker organizational structures and less accountability
- ☐ Increased information protection (IP) risk will increase

Question 539

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

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

Question 540

Which type of control is being implemented when a biometric access device is installed at the entrance to a facility?

- ☐ Preventive
- ☐ Deterrent
- ☐ Corrective
- ☐ Detective

Question 541

Which of the following is MOST effective against system intrusions?

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

Question 542

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 543

Which of the following risk handling technique involves the practice of being proactive so that the risk in question is not realized?

- ☐ Risk Mitigation
- ☐ Risk Acceptance
- ☐ Risk Avoidance
- ☐ Risk transfer

Question 544

An IS auditor is reviewing documentation of application systems change control and identifies several patches that were not tested before being put into production. Which of the following is the MOST significant risk from this situation?

- ☐ Developer access to production
- ☐ Lack of system integrity
- ☐ Outdated system documentation
- ☐ Loss of application support

Question 545

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 546

When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

- ☐ incorporates state of the art technology.
- ☐ addresses the required operational controls.
- ☐ articulates the IT mission and vision.
- ☐ specifies project management practices.

Question 547

Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

- ☐ Gateway
- ☐ Protocol converter
- ☐ Front-end communication processor
- ☐ Concentrator/multiplexor

Question 548

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 549

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 550

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

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

Question 551

An IS auditor reviewing an organization's data file control procedures finds that transactions are applied to the most current files, while restart procedures use earlier versions. The IS auditor should recommend the implementation of:

- ☐ source documentation retention.
- ☐ data file security.
- ☐ version usage control.
- ☐ one-for-one checking.

Question 552

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

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

Question 553

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 554

Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

- ☐ meets or exceeds industry security standards.
- ☐ agrees to be subject to external security reviews.
- ☐ has a good market reputation for service and experience.
- ☐ complies with security policies of the organization.

Question 555

Which of the following encrypt/decrypt steps provides the GREATEST assurance of achieving confidentiality, message integrity and nonrepudiation by either sender or recipient?

- ☐ The recipient uses their private key to decrypt the secret key.
- ☐ The encrypted prehash code and the message are encrypted using a secret key.
- ☐ The encrypted prehash code is derived mathematically from the message to be sent.
- ☐ The recipient uses the sender's public key, verified with a certificate authority, to decrypt the prehash code.

Question 556

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 557

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

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

Question 558

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

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

Question 559

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 560

What determines the strength of a secret key within a symmetric key cryptosystem?

- ☐ A combination of key length, degree of permutation, and the complexity of the data-encryption algorithm that uses the key
- ☐ A combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key
- ☐ A combination of key length and the complexity of the data-encryption algorithm that uses the key
- ☐ Initial input vectors and the complexity of the data-encryption algorithm that uses the key

Question 561

IS audits should be selected through a risk analysis process to concentrate on:

- ☐ those areas of greatest risk and opportunity for improvements.
- ☐ those areas of least risk and opportunity for improvements.
- ☐ those areas of the greatest financial value.
- ☐ areas led by the key people of the organization.
- ☐ random events.
- ☐ irregular events.

Question 562

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 563

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 564

A disaster recovery plan for an organization's financial system specifies that the recovery point objective (RPO) is no data loss and the recovery time objective (RTO) is 72 hours. Which of the following is the MOST cost-effective solution?

- ☐ A hot site that can be operational in eight hours with asynchronous backup of the transaction logs
- ☐ Distributed database systems in multiple locations updated asynchronously
- ☐ Synchronous updates of the data and standby active systems in a hot site
- ☐ Synchronous remote copy of the data in a warm site that can be operational in 48 hours

Question 565

An organization's IS audit charter should specify the:

- ☐ short- and long-term plans for IS audit engagements
- ☐ objectives and scope of IS audit engagements.
- ☐ detailed training plan for the IS audit staff.
- ☐ role of the IS audit function.

Question 566

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 567

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 568

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 569

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 570

Which of the following is an advantage of asymmetric crypto system over symmetric key crypto system?

- ☐ Performance and Speed
- ☐ Key Management is built in
- ☐ Adequate for Bulk encryption
- ☐ Number of keys grows very quickly

Question 571

Which of the following is the MOST important outcome of testing incident response plans?

- ☐ Internal procedures are improved.
- ☐ An action plan is available for senior management.
- ☐ Staff is educated about current threats.
- ☐ Areas requiring investment are identified.

Question 572

What is the MOST effective way to ensure security policies and procedures are up-to-date?

- ☐ Verify security requirements are being identified and consistently applied.
- ☐ Align the organization's security practices with industry standards and best practice.
- ☐ Define and document senior management's vision for the direction of the security
- ☐ Prevent security documentation audit issues from being raised

Question 573

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 574

A firewall is being deployed at a new location. Which of the following is the MOST important factor in ensuring a successful deployment?

- ☐ Reviewing logs frequently
- ☐ Testing and validating the rules
- ☐ Training a local administrator at the new location
- ☐ Sharing firewall administrative duties

Question 575

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 576

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 577

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 578

Why is a clause for requiring source code escrow in an application vendor agreement important?

- ☐ To segregate systems development and live environments
- ☐ To protect the organization from copyright disputes
- ☐ To ensure that sufficient code is available when needed
- ☐ To ensure that the source code remains available even if the application vendor goes out of business

Question 579

Which of the following is the GREATEST concern with conducting penetration testing on an internally developed application in the production environment?

- ☐ The testing could create application availability issues.
- ☐ The testing may identify only known operating system vulnerabilities.
- ☐ The issues identified during the testing may require significant remediation efforts.
- ☐ Internal security staff may not be qualified to conduct application penetration testing.

Question 580

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

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

Question 581

In-house personnel performing IS audits should possess which of the following knowledge and/or skills (Choose two.):

- ☐ information systems knowledge commensurate with the scope of the IT environment in question
- ☐ sufficient analytical skills to determine root cause of deficiencies in question
- ☐ sufficient knowledge on secure system coding
- ☐ sufficient knowledge on secure platform development
- ☐ information systems knowledge commensurate outside of the scope of the IT environment in question

Question 582

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.
- ☐ Assess whether the service provider meets the organization's data protection policies.

Question 583

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 584

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 585

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

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

Question 586

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 587

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

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

Question 588

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 589

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 590

The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

- ☐ testing stage.
- ☐ evaluation stage.
- ☐ maintenance stage.
- ☐ early stages of planning.

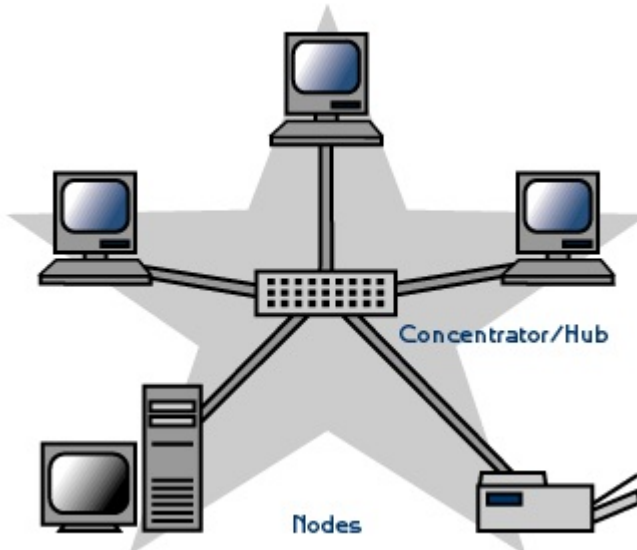
Question 591

A start-up company acquiring servers for its order-taking system is unable to predict the volume of transactions. Which of the following is MOST important for the company to consider?

- ☐ Scalability
- ☐ Configuration
- ☐ Optimization
- ☐ Compatibility

Question 592

Identify the network topology from below diagram presented below:



Network Topology

- ☐ Bus
- ☐ Star
- ☐ Ring
- ☐ Mesh

Question 593

Which of the following is the GREATEST concern when an organization's backup facility is at a warm site?

- ☐ Timely availability of hardware
- ☐ Availability of heat, humidity and air conditioning equipment
- ☐ Adequacy of electrical power connections
- ☐ Effectiveness of the telecommunications network

Question 594

In which of the following database models is the data represented in terms of tuples and grouped into relations?

- ☐ Hierarchical database model
- ☐ Network database model
- ☐ Relational database model
- ☐ Object-relational database model

Question 595

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 596

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 597

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 598

An IS auditor has audited a business continuity plan (BCP). Which of the following findings is the MOST critical?

- ☐ Nonavailability of an alternate private branch exchange (PBX) system
- ☐ Absence of a backup for the network backbone
- ☐ Lack of backup systems for the users' PCs
- ☐ Failure of the access card system

Question 599

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 600

Which of the following is the GREATEST threat to Voice-over Internet Protocol (VoIP) related to privacy release?

- ☐ Incorrect routing
- ☐ Eavesdropping
- ☐ Call recording
- ☐ Denial of service

Question 601

Many WEP systems require a key in a relatively insecure format. What format is this?

- ☐ binary format.
- ☐ hexadecimal format.
- ☐ 128 bit format.
- ☐ 256 bit format.
- ☐ None of the choices.

Question 602

Which of the following is the BEST reason for an organization to develop a business continuity plan?

- ☐ To develop a detailed description of information systems and processes
- ☐ To identify the users of information systems and processes
- ☐ To avoid the costs resulting from the failure of key systems and processes
- ☐ To establish business unit prioritization of systems, projects, and strategies

Question 603

Which of the following software development methods is based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams?

- ☐ Agile Development
- ☐ Software prototyping
- ☐ Rapid application development
- ☐ Component based development

Question 604

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 605

The PRIMARY purpose of audit trails is to:

- ☐ improve response time for users.
- ☐ establish accountability and responsibility for processed transactions.
- ☐ improve the operational efficiency of the system.
- ☐ provide useful information to auditors who may wish to track transactions

Question 606

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 607

Network ILDP 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 608

Batch control reconciliation is a _____ (fill the blank) control for mitigating risk of inadequate segregation of duties.

- ☐ Detective
- ☐ Corrective
- ☐ Preventative
- ☐ Compensatory

Question 609

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 610

Which of the following are BEST suited for continuous auditing?

- ☐ Manual transactions
- ☐ Irregular transactions
- ☐ Low-value transactions
- ☐ Real-time transactions

Question 611

What is the PRIMARY objective of performing a vulnerability assessment following a business system update?

- ☐ Update the threat landscape
- ☐ Review the effectiveness of controls
- ☐ Determine operational losses
- ☐ Improve the change control process

Question 612

A company is planning to implement a new administrative system at many sites. The new system contains four integrated modules. Which of the following implementation approaches would be MOST appropriate?

- ☐ Parallel implementation module by module
- ☐ Pilot run of the new system
- ☐ Full implementation of the new system
- ☐ Parallel run at all locations

Question 613

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

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

Question 614

_____ (fill in the blank) should be implemented as early as data preparation to support data integrity at the earliest point possible.

- ☐ Control totals
- ☐ Authentication controls
- ☐ Parity bits
- ☐ Authorization controls

Question 615

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 616

Which of the following would be of GREATEST concern to an IS auditor receiving an organization's security incident handling procedures?

- ☐ Annual tabletop exercises are performed instead of functional incident response exercises.
- ☐ Roles for computer emergency response team (CERT) members have not been formally documented.
- ☐ Guidelines for prioritizing incidents have not been identified.
- ☐ Workstation antivirus software alerts are not regularly reviewed.

Question 617

Which of the following is a function of an IS steering committee?

- ☐ Monitoring vendor-controlled change control and testing
- ☐ Ensuring a separation of duties within the information's processing environment
- ☐ Approving and monitoring major projects, the status of IS plans and budgets
- ☐ Liaising between the IS department and the end users

Question 618

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

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

Question 619

Which of the following option INCORRECTLY describes PBX feature?

- ☐ Voice mail -Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.
- ☐ Tenanting-Provides for the possibility to break into a busy line to inform another user an important message
- ☐ Automatic Call Distribution - Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available
- ☐ Diagnostics -Allows for bypassing normal call restriction procedures

Question 620

Which of the following is MOST important for an IS auditor to ensure is included in a global organization's online data privacy notification to customers?

- ☐ Consequences to the organization for mishandling the data
- ☐ Consent terms including the purpose of data collection
- ☐ Contact information for reporting violations of consent
- ☐ Industry standards for data breach notification

Question 621

An organization establishes an internal document collaboration site. To ensure data confidentiality of each project group, it is MOST important to:

- ☐ conduct a vulnerability assessment.
- ☐ enforce document life cycle management.
- ☐ prohibit remote access to the site.
- ☐ periodically recertify access rights.

Question 622

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 623

Which of the following is the MOST likely 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 624

Which of the following threats is prevented by using token-based authentication?

- ☐ Password sniffing attack on the network
- ☐ Session eavesdropping attack on the network
- ☐ Man-in-the-middle attack on the client
- ☐ Denial of service attack over the network

Question 625

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 626

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 627

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 628

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 629

Which of the following is the GREATEST risk of cloud computing?

- ☐ Reduced performance
- ☐ Disclosure of data
- ☐ Lack of scalability
- ☐ Inflexibility

Question 630

Which of the following is the BEST course of action for an information security manager to align security and business goals?

- ☐ Reviewing the business strategy
- ☐ Actively engaging with stakeholders
- ☐ Conducting a business impact analysis
- ☐ Defining key performance indicators

Question 631

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

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

Question 632

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 633

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 634

Labeling information according to its security classification:

- ☐ reduces the need to identify baseline controls for each classification.
- ☐ reduces the number and type of countermeasures required.
- ☐ enhances the likelihood of people handling information securely.
- ☐ affects the consequences if information is handled insecurely.

Question 635

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 636

Data flow diagrams are used by IS auditors to:

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

Question 637

A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

- ☐ reasonableness check.
- ☐ parity check.
- ☐ redundancy check.
- ☐ check digits.

Question 638

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 639

A design company has multiple name and address file for its customers in several of its independent systems. Which of the following is the BEST control to ensure that the customer name and address agree across all files?

- ☐ Use of hash totals on customer records
- ☐ Periodic review of each master file by management
- ☐ Matching of records and review of exception reports
- ☐ Use of authorized master file change forms

Question 640

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 641

Which of the following is the MOST important control to implement when senior managers use smartphones to access sensitive company information?

- ☐ Mandatory virtual private network (VPN) connectivity
- ☐ Centralized device administration
- ☐ Strong passwords
- ☐ Anti-malware on the devices

Question 642

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 643

A previously agreed-upon recommendation was not implemented because the auditee no longer agrees with the original findings. The IS auditor's FIRST course of action should be to:

- ☐ exclude the finding in the follow-up audit report.
- ☐ escalate the disagreement to the audit committee.
- ☐ assess the reason for the disagreement.
- ☐ require implementation of the original recommendation.

Question 644

Which of the following is a mechanism for mitigating risks?

- ☐ Security and control practices
- ☐ Property and liability insurance
- ☐ Audit and certification
- ☐ Contracts and service level agreements (SLAs)

Question 645

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 646

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

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

Question 647

Which of the following forms of evidence for the auditor would be considered the MOST reliable?

- ☐ An oral statement from the auditee
- ☐ The results of a test performed by an IS auditor
- ☐ An internally generated computer accounting report
- ☐ A confirmation letter received from an outside source

Question 648

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 649

An organization has developed mature risk management practices that are followed across all departments. What is the MOST effective way for the audit team to leverage this risk management maturity?

- ☐ Facilitating audit risk identification and evaluation workshops
- ☐ Implementing risk responses on management's behalf
- ☐ Providing assurances to management regarding risk
- ☐ Integrating the risk register for audit planning purposes

Question 650

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 651

Who is responsible for restricting and monitoring access of a data user?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☐ Security Administrator

Question 652

The responsibility for authorizing access to application data should be with the:

- ☐ data custodian.
- ☐ database administrator (DBA).
- ☐ data owner.
- ☐ security administrator.

Question 653

Diskless workstation is an example of:

- ☐ Handheld devices
- ☐ Thin client computer
- ☐ Personal computer
- ☐ Midrange server

Question 654

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 655

Which of the following is the MOST beneficial outcome of testing an incident response plan?

- ☐ The plan is enhanced to reflect the findings of the test.
- ☐ Test plan results are documented.
- ☐ Incident response time is improved.
- ☐ The response includes escalation to senior management.

Question 656

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

- ☐ True
- ☐ False

Question 657

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 658

Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?

- ☐ Spool
- ☐ Cluster controller
- ☐ Protocol converter
- ☐ Front end processor

Question 659

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

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

Question 660

When conducting a follow-up of previous audit findings, an IS auditor is told by management that a recommendation to make security changes to an application has not been implemented. The IS auditor should FIRST determine whether:

- ☐ additional time to implement changes is needed.
- ☐ the associated risk is still relevant.
- ☐ the recommendation should be re-issued.
- ☐ the issue should be escalated.

Question 661

The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

- ☐ a lack of investment in technology.
- ☐ a lack of a methodology for systems development.
- ☐ technology not aligning with the organization's objectives.
- ☐ an absence of control over technology contracts.

Question 662

Which of the following is MOST important to consider when developing a bring your own device (BYOD) policy?

- ☐ Supported operating systems
- ☐ Procedure for accessing the network
- ☐ Application download restrictions
- ☐ Remote wipe procedures

Question 663

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 664

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

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

Question 665

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 666

Which of the following is the dominating objective of BCP and DRP?

- ☐ To protect human life
- ☐ To mitigate the risk and impact of a business interruption
- ☐ To eliminate the risk and impact of a business interruption
- ☐ To transfer the risk and impact of a business interruption

Question 667

Which of the following is the BEST approach for determining the maturity level of an information security program?

- ☐ Review internal audit results.
- ☐ Engage a third-party review.
- ☐ Perform a self-assessment.
- ☐ Evaluate key performance indicators (KPIs).

Question 668

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 669

Which of the following outsourced services has the GREATEST need for security monitoring?

- ☐ Web site hosting
- ☐ Application development
- ☐ Virtual private network (VPN) services
- ☐ Enterprise infrastructure

Question 670

In an organization that has a staff-rotation policy, the MOST appropriate access control model is:

- ☐ role based.
- ☐ discretionary.
- ☐ mandatory.
- ☐ lattice based.

Question 671

Which of the following is MOST important to consider when assessing the scope of privacy concerns for an IT project?

- ☐ Applicable laws and regulations
- ☐ End user access rights
- ☐ Business requirements
- ☐ Classification of data

Question 672

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 673

Which of the following refers to an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer?

- ☐ buffer overflow
- ☐ format string vulnerabilities
- ☐ integer misappropriation
- ☐ code injection
- ☐ None of the choices.

Question 674

Which of the following provides the strongest authentication for physical access control?

- ☐ Sign-in logs
- ☐ Dynamic passwords
- ☐ Key verification
- ☐ Biometrics

Question 675

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

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

Question 676

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

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

Question 677

During the evaluation of a firm's newly established whistleblower system, an auditor notes several findings. Which of the following should be the auditor's GREATEST concern?

- ☐ New employees have not been informed of the whistleblower policy.
- ☐ The whistleblower's privacy is not protected.
- ☐ The whistleblower system does not track the time and date of submission.
- ☐ The whistleblower system is only available during business hours.

Question 678

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 679

The decision to accept an IT control risk related to data quality should be the responsibility of the:

- ☐ information security team
- ☐ chief information officer
- ☐ business owner
- ☐ IS audit manager

Question 680

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 681

Which of the following property of the core data warehouse layer of an enterprise data flow architecture uses common attributes to access a cross section of an information in the warehouse?

- ☐ Drill up
- ☐ Drill down
- ☐ Drill across
- ☐ Historical Analysis

Question 682

An organization has a number of branches across a wide geographical area. To ensure that all aspects of the disaster recovery plan are evaluated in a cost effective manner, an IS auditor should recommend the use of a:

- ☐ data recovery test.
- ☐ full operational test.
- ☐ posttest.
- ☐ preparedness test.

Question 683

When should systems administrators first assess the impact of applications or systems patches?

- ☐ Within five business days following installation
- ☐ Prior to installation
- ☐ No sooner than five business days following installation
- ☐ Immediately following installation

Question 684

To address an organization's disaster recovery requirements, backup intervals should not exceed the:

- ☐ service level objective (SLO).
- ☐ recovery time objective (RTO).
- ☐ recovery point objective (RPO).
- ☐ maximum acceptable outage (MAO).

Question 685

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 686

When should plans for testing for user acceptance be prepared?

- ☐ In the requirements definition phase of the systems-development project
- ☐ In the feasibility phase of the systems-development project
- ☐ In the design phase of the systems-development project
- ☐ In the development phase of the systems-development project

Question 687

An IS auditor is evaluating the completeness of privacy procedures involving personally identifiable information (PII). Which of the following is MOST important for the auditor to verify is included in the procedures?

- ☐ Regulatory requirements for protecting PII
- ☐ The organization's definition of PII
- ☐ Encryption requirements for transmitting PII externally
- ☐ A description of how PII is masked within key systems

Question 688

Which of the following is necessary to determine what would constitute a disaster for an organization?

- ☐ Backup strategy analysis
- ☐ Threat probability analysis
- ☐ Risk analysis
- ☐ Recovery strategy analysis

Question 689

Which of the following is a detective control?

- ☐ Procedures for authorizing transactions
- ☐ Echo checks in telecommunications
- ☐ A router rule restricting a service
- ☐ Programmed edit checks

Question 690

What is a risk associated with attempting to control physical access to sensitive areas such as computer rooms using card keys or locks?

- ☐ Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.
- ☐ The contingency plan for the organization cannot effectively test controlled access practices.
- ☐ Access cards, keys and pads can be easily duplicated allowing easy compromise of the control.
- ☐ Removing access for those who are no longer authorized is complex.

Question 691

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 692

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

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

Question 693

In regard to moving an application program from the test environment to the production environment, the BEST control would be to have the:

- ☐ application programmer copy the source program and compiled object module to the production libraries
- ☐ application programmer copy the source program to the production libraries and then have the production control group compile the program.
- ☐ production control group compile the object module to the production libraries using the source program in the test environment.
- ☐ production control group copy the source program to the production libraries and then compile the program.

Question 694

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 695

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 696

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 697

Which of the following satisfies a two-factor user authentication?

- ☐ Iris scanning plus fingerprint scanning
- ☐ Terminal ID plus global positioning system (GPS)
- ☐ A smart card requiring the user's PIN
- ☐ User ID along with password

Question 698

Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?

- ☐ Overwriting the tapes
- ☐ initializing the tape labels
- ☐ Degaussing the tapes
- ☐ Erasing the tapes

Question 699

Which of the following is an advantage of prototyping?

- ☐ The finished system normally has strong internal controls.
- ☐ Prototype systems can provide significant time and cost savings.
- ☐ Change control is often less complicated with prototype systems.
- ☐ it ensures that functions or extras are not added to the intended system.

Question 700

IS management is considering a Voice-over Internet Protocol (VoIP) network to reduce telecommunication costs and management asked the IS auditor to comment on appropriate security controls. Which of the following security measures is MOST appropriate?

- ☐ Review and, where necessary, upgrade firewall capabilities
- ☐ Install modems to allow remote maintenance support access
- ☐ Create a physically distinct network to handle VoIP traffic
- ☐ Redirect all VoIP traffic to allow clear text logging of authentication credentials

Question 701

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 702

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 703

The technique of rummaging through commercial trash to collect useful business information is known as:

- ☐ Information diving
- ☐ Intelligence diving
- ☐ Identity diving
- ☐ System diving
- ☐ Program diving
- ☐ None of the choices.

Question 704

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 705

The MOST effective control for addressing the risk of piggybacking is:

- ☐ a single entry point with a receptionist.
- ☐ the use of smart cards.
- ☐ a biometric door lock.
- ☐ a deadman door.

Question 706

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 707

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 708

Which of the following should be performed immediately after a computer security incident has been detected and analyzed by an incident response team?

- ☐ Assess the impact of the incident on critical systems
- ☐ Categorize the incident
- ☐ Eradicate the component that caused the incident
- ☐ Contain the incident before it spreads

Question 709

Which of the following would BEST support a business case to implement a data leakage prevention (DLP) solution?

- ☐ An unusual upward trend in outbound email volume
- ☐ Lack of visibility into previous data leakage incidents
- ☐ Industry benchmark of DLP investments
- ☐ A risk assessment on the threat of data leakage

Question 710

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 711

An existing system is being replaced with a new application package. User acceptance testing should ensure that:

- ☐ data from the old system has been converted correctly
- ☐ the new system functions as expected
- ☐ the new system is better than the old system
- ☐ there is a business need for the new system

Question 712

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 713

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 714

Which of the following is the BEST method for determining the criticality of each application system in the production environment?

- ☐ interview the application programmers.
- ☐ Perform a gap analysis.
- ☐ Review the most recent application audits.
- ☐ Perform a business impact analysis.

Question 715

The operations team of an organization has reported an IS security attack. Which of the following should be the NEXT step for the security incident response team?

- ☐ Document lessons learned.
- ☐ Prioritize resources for corrective action.
- ☐ Perform a damage assessment.
- ☐ Report results to management.

Question 716

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

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

Question 717

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

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

Question 718

When preventive controls to appropriately mitigate risk are not feasible, which of the following is the MOST important action for the information security manager to perform?

- ☐ Identity unacceptable risk levels
- ☐ Manage the impact
- ☐ Evaluate potential threats
- ☐ Assess vulnerabilities

Question 719

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

- ☐ Security audit reports
- ☐ Benchmarking reports
- ☐ Information security standards
- ☐ Compliance requirements

Question 720

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 721

Which of the following procedures would BEST contribute to the reliability of information in a data warehouse?

- ☐ Retaining only current data
- ☐ Storing only a single type of data
- ☐ Maintaining archive data
- ☐ Maintaining current metadata

Question 722

Which of the following is the MOST important consideration for an organization when strategizing to comply with privacy regulations?

- ☐ Ensuring there are staff members with in-depth knowledge of the privacy regulations
- ☐ Ensuring up-to-date knowledge of where customer data is saved
- ☐ Ensuring regularly updated contracts with third parties that process customer data
- ☐ Ensuring appropriate access to information systems containing privacy information.

Question 723

During a business process re-engineering (BPR) program, IT can assist with:

- ☐ total cost of ownership.
- ☐ focusing on value-added tasks.
- ☐ segregation of duties.
- ☐ streamlining of tasks.

Question 724

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 725

Which of the following statement correctly describes the differences between tunnel mode and transport mode of the IPSec protocol?

- ☐ In transport mode the ESP is encrypted where as in tunnel mode the ESP and its header's are encrypted
- ☐ In tunnel mode the ESP is encrypted where as in transport mode the ESP and its header's are encrypted
- ☐ In both modes (tunnel and transport mode) the ESP and its header's are encrypted
- ☐ There is no encryption provided when using ESP or AH

Question 726

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 727

Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

- ☐ System owners
- ☐ System users
- ☐ System designers
- ☐ System builders

Question 728

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 729

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 730

Which of the following is the BEST source for describing the objectives of an organization's information systems?

- ☐ Business process owners
- ☐ End users
- ☐ IT management
- ☐ Information security management

Question 731

What control detects transmission errors by appending calculated bits onto the end of each segment of data?

- ☐ Reasonableness check
- ☐ Parity check
- ☐ Redundancy check
- ☐ Check digits

Question 732

Which of the following is MOST likely to result from compliance testing?

- ☐ Comparison of data with physical counts
- ☐ Confirmation of data with outside sources
- ☐ Identification of errors due to processing mistakes
- ☐ Discovery of controls that have not been applied

Question 733

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 734

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 735

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 736

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

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

Question 737

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 738

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

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

Question 739

An organization has outsourced its data leakage monitoring to an Internet service provider (ISP). Which of the following is the BEST way for an IS auditor to determine the effectiveness of this service?

- ☐ Verify the ISP has staff to deal with data leakage
- ☐ Review the ISP's external audit report
- ☐ Review the data leakage clause in the SLA
- ☐ Simulate a data leakage incident

Question 740

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 741

Which of the following software tools is often used for stealing money from infected PC owner through taking control of the modem?

- ☐ System patcher
- ☐ Porn dialer
- ☐ War dialer
- ☐ T1 dialer
- ☐ T3 dialer
- ☐ None of the choices.

Question 742

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 743

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 744

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 745

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

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

Question 746

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 747

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 748

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 749

IS management has decided to rewrite a legacy customer relations system using fourth generation languages (4GLs). Which of the following risks is MOST often associated with system development using 4GLs?

- ☐ Inadequate screen/report design facilities
- ☐ Complex programming language subsets
- ☐ Lack of portability across operating systems
- ☐ Inability to perform data intensive operations

Question 750

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

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

Question 751

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 752

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 753

Which of the following layer of an OSI model ensures that messages are delivered error-free, in sequence, and with no losses or duplications?

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

Question 754

While copying files from a floppy disk, a user introduced a virus into the network. Which of the following would MOST effectively detect the existence of the virus?

- ☐ A scan of all floppy disks before use
- ☐ A virus monitor on the network file server
- ☐ Scheduled daily scans of all network drives
- ☐ A virus monitor on the user's personal computer

Question 755

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 756

Which of the following is the MOST important reason for performing vulnerability assessments periodically?

- ☐ Technology risks must be mitigated.
- ☐ Management requires regular reports.
- ☐ The environment changes constantly.
- ☐ The current threat levels are being assessed.

Question 757

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 758

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 759

Which of the following weaknesses would have the GREATEST impact on the effective operation of a perimeter firewall?

- ☐ Ad-hoc monitoring of firewall activity
- ☐ Potential back doors to the firewall software
- ☐ Misconfiguration on the firewall rules
- ☐ Use of stateful firewalls with default configuration

Question 760

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 761

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

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

Question 762

An organization has shifted from a bottom-up approach to a top-down approach in the development of IT policies. This should result in:

- ☐ a synthesis of existing operational policies
- ☐ greater consistency across the organization
- ☐ greater adherence to best practices
- ☐ a more comprehensive risk assessment plan

Question 763

An advantage of the use of hot sites as a backup alternative is that:

- ☐ the costs associated with hot sites are low.
- ☐ hot sites can be used for an extended amount of time.
- ☐ hot sites can be made ready for operation within a short period of time.
- ☐ they do not require that equipment and systems software be compatible with the primary site.

Question 764

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

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

Question 765

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 766

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 767

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 768

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

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

Question 769

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 770

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 771

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 772

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 773

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 774

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 775

An IS auditor finds that a DBA has read and write access to production data. The IS auditor should:

- ☐ accept the DBA access as a common practice.
- ☐ assess the controls relevant to the DBA function.
- ☐ recommend the immediate revocation of the DBA access to production data.
- ☐ review user access authorizations approved by the DBA.

Question 776

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

- ☐ Enticement
- ☐ Entrapment

Question 777

The PRIMARY purpose of asset valuation for the management of information security is to:

- ☐ eliminate the least significant assets.
- ☐ provide a basis for asset classification.
- ☐ determine the value of each asset.
- ☐ prioritize risk management activities.

Question 778

Which of the following software development methodology uses minimal planning and in favor of rapid prototyping?

- ☐ Agile Developments
- ☐ Software prototyping
- ☐ Rapid application development
- ☐ Component based development

Question 779

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 780

isk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a _____ risk assessment is more appropriate. Fill in the blanks.

- ☐ Quantitative; qualitative
- ☐ Qualitative; quantitative
- ☐ Residual; subjective
- ☐ Quantitative; subjective

Question 781

To ensure appropriate control of information processed in IT systems, security safeguards should be based PRIMARILY on:

- ☐ established guidelines.
- ☐ overall IT capacity and operational constraints.
- ☐ efficient technical processing considerations.
- ☐ criteria consistent with classification levels.

Question 782

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

- ☐ True
- ☐ False

Question 783

Which of the following should be the FIRST step when conducting an IT risk assessment?

- ☐ Assess vulnerabilities
- ☐ Identify assets to be protected
- ☐ Evaluate controls in place
- ☐ Identify potential threats

Question 784

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 785

An organization has recently installed a security patch, which crashed the production server. To minimize the probability of this occurring again, an IS auditor should:

- ☐ apply the patch according to the patch's release notes.
- ☐ ensure that a good change management process is in place.
- ☐ thoroughly test the patch before sending it to production.
- ☐ approve the patch after doing a risk assessment.

Question 786

Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

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

Question 787

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 788

Effective IT governance requires organizational structures and processes to ensure that:

- ☐ the organization's strategies and objectives extend the IT strategy.
- ☐ the business strategy is derived from an IT strategy.
- ☐ IT governance is separate and distinct from the overall governance.
- ☐ the IT strategy extends the organization's strategies and objectives.

Question 789

From a risk management perspective, which of the following is MOST important to be tracked in continuous monitoring?

- ☐ Number of prevented attacks
- ☐ Changes in the threat environment
- ☐ Changes in user privileges
- ☐ Number of failed logins

Question 790

Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would MOST likely focus on a review of:

- ☐ pre-BPR process flowcharts.
- ☐ post-BPR process flowcharts.
- ☐ BPR project plans.
- ☐ continuous improvement and monitoring plans.

Question 791

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 792

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 793

Who is responsible for reviewing the result and deliverables within and at the end of each phase, as well as confirming compliance with requirements?

- ☐ Project Sponsor
- ☐ Quality Assurance
- ☐ User Management
- ☐ Senior Management

Question 794

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 795

Properly planned risk-based audit programs are often capable of offering which of the following benefits?

- ☐ audit efficiency and effectiveness.
- ☐ audit efficiency only.
- ☐ audit effectiveness only.
- ☐ audit transparency only.
- ☐ audit transparency and effectiveness.
- ☐ None of the choices.

Question 796

Which of the following should be the GREATEST concern to an IS auditor reviewing the information security framework of an organization?

- ☐ The information security policy has not been updated in the last two years.
- ☐ A list of critical information assets was not included in the information security policy.
- ☐ Senior management was not involved in the development of the information security policy.
- ☐ The information security policy is not aligned with regulatory requirements.

Question 797

Which of the following is used to evaluate biometric access controls?

- ☐ FAR
- ☐ EER
- ☐ ERR
- ☐ FRR

Question 798

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 799

Who is responsible for implementing cost-effective controls in an automated system?

- ☐ Security policy administrators
- ☐ Business unit management
- ☐ Senior management
- ☐ Board of directors

Question 800

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 801

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 802

Over the long term, which of the following has the greatest potential to improve the security incident response process?

- ☐ A walkthrough review of incident response procedures
- ☐ Postevent reviews by the incident response team
- ☐ Ongoing security training for users
- ☐ Documenting responses to an incident

Question 803

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

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

Question 804

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

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

Question 805

Which of the following is MOST important to consider when developing a disaster recovery plan?

- ☐ Business continuity plan (BCP)
- ☐ Feasibility assessment
- ☐ Business impact analysis (BIA)
- ☐ Cost-benefit analysis

Question 806

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 807

The BEST way to obtain funding from senior management for a security awareness program is to:

- ☐ meet regulatory requirements
- ☐ produce an impact analysis report of potential breaches
- ☐ demonstrate that the program will adequately reduce risk
- ☐ produce a report of organizational risks

Question 808

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 809

Pretexting is an act of:

- ☐ DoS
- ☐ social engineering
- ☐ eavesdropping
- ☐ soft coding
- ☐ hard coding
- ☐ None of the choices.

Question 810

Spreadsheets are used to calculate project cost estimates. Totals for each cost category are then keyed into the job-costing system. What is the BEST control to ensure that data are accurately entered into the system?

- ☐ Reasonableness checks for each cost type
- ☐ Validity checks, preventing entry of character data
- ☐ Display back of project detail after entry
- ☐ Reconciliation of total amounts by project

Question 811

Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?

- ☐ Allocating resources
- ☐ Keeping current with technology advances
- ☐ Conducting control self-assessment
- ☐ Evaluating hardware needs

Question 812

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 813

John has been hired to fill a new position in one of the well-known financial institute. The position is for IS auditor. He has been assigned to complete IS audit of one of critical financial system. Which of the following should be the first step for John to be perform during IS audit planning?

- ☐ Perform risk assessment
- ☐ Determine the objective of the audit
- ☐ Gain an understanding of the business process
- ☐ Assign the personnel resource to audit

Question 814

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 815

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 816

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

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

Question 817

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 818

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 819

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 820

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 821

Which of the following cloud computing service model provides a way to rent operating systems, storage and network capacity over the Internet?

- ☐ Software as a service
- ☐ Data as a service
- ☐ Platform as a service
- ☐ Infrastructure as a service

Question 822

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 823

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 824

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 825

An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

- ☐ this lack of knowledge may lead to unintentional disclosure of sensitive information.
- ☐ information security is not critical to all functions.
- ☐ IS audit should provide security training to the employees.
- ☐ the audit finding will cause management to provide continuous training to staff.

Question 826

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 827

An efficient use of public key infrastructure (PKI) should encrypt the:

- ☐ entire message.
- ☐ private key.
- ☐ public key.
- ☐ symmetric session key.

Question 828

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 829

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 830

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 831

An IS auditor reviewing access controls for a client-server environment should FIRST:

- ☐ evaluate the encryption technique.
- ☐ identify the network access points.
- ☐ review the identity management system.
- ☐ review the application level access controls.

Question 832

Which of the following Confidentiality, Integrity, Availability (CIA) attribute supports the principle of least privilege by providing access to information only to authorized and intended users?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Accuracy

Question 833

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 834

An IS auditor reviewing the threat assessment for a data center would be MOST concerned if:

- ☐ all identified threats relate to external entities
- ☐ some of the identified threats are unlikely to occur
- ☐ neighboring organizations' operations have been included
- ☐ the exercise was completed by local management

Question 835

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 836

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

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

Question 837

Two-factor authentication can be circumvented through which of the following attacks?

- ☐ Denial-of-service
- ☐ Man-in-the-middle
- ☐ Key logging
- ☐ Brute force

Question 838

Which of the following would MOST effectively control the usage of universal storage bus (USB) storage devices?

- ☐ Policies that require instant dismissal if such devices are found
- ☐ Software for tracking and managing USB storage devices
- ☐ Administratively disabling the USB port
- ☐ Searching personnel for USB storage devices at the facility's entrance

Question 839

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

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

Question 840

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 841

Which of the following is MOST important for an IS auditor to review when evaluating the effectiveness of an organization's incident response process?

- ☐ Past incident response actions
- ☐ Incident response staff experience and qualifications
- ☐ Results from management testing of incident response procedures
- ☐ Incident response roles and responsibilities

Question 842

A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?

- ☐ Key verification
- ☐ One-for-one checking
- ☐ Manual recalculations
- ☐ Functional acknowledgements

Question 843

Which policy helps an auditor to gain a better understanding of biometrics system in an organization?

- ☐ BIMS Policy
- ☐ BOMS Policy
- ☐ BMS Policy
- ☐ BOS Policy

Question 844

The feature of a digital signature that ensures the sender cannot later deny generating and sending the message is called:

- ☐ data integrity.
- ☐ authentication.
- ☐ non repudiation.
- ☐ replay protection.

Question 845

Reevaluation of risk is MOST critical when there is:

- ☐ resistance to the implementation of mitigating controls
- ☐ a change in security policy
- ☐ a management request for updated security reports
- ☐ a change in the threat landscape

Question 846

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 847

An IS auditor needs to consider many factors while evaluating an encryption system. Which of the following is LEAST important factor to be considered while evaluating an encryption system?

- ☐ Encryption algorithm
- ☐ Encryption keys
- ☐ Key length
- ☐ Implementation language

Question 848

Which of the following types of firewall treats each network frame or packet in isolation?

- ☐ statefull firewall
- ☐ hardware firewall
- ☐ combination firewall
- ☐ packet filtering firewall
- ☐ stateless firewall
- ☐ None of the choices.

Question 849

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 850

Multiple invoices are usually received for individual purchase orders, since purchase orders require staggered delivery dates. Which of the following is the BEST audit technique to test for duplicate payments?

- ☐ Run the data on the software programs used to process supplier payments.
- ☐ Use generalized audit software on the invoice transaction file.
- ☐ Run the data on the software programs used to process purchase orders.
- ☐ Use generalized audit software on the purchase order transaction file.

Question 851

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 852

Which of the following is a PRIMARY security responsibility of an information owner?

- ☐ Determining the controls associated with information classification
- ☐ Testing information classification controls
- ☐ Maintaining the integrity of data in the information systems
- ☐ Deciding what level of classification the information requires

Question 853

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

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

Question 854

Which of the following is MOST likely to enable a hacker to successfully penetrate a system?

- ☐ Lack of virus protection
- ☐ Unpatched software
- ☐ Decentralized dialup access
- ☐ Lack of DoS protection

Question 855

Iptables is based on which of the following frameworks?

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

Question 856

In which of the following database model is the data organized into a tree-like structure, implying a single parent for each record?

- ☐ Hierarchical database model
- ☐ Network database model
- ☐ Relational database model
- ☐ Object-relational database model

Question 857

What is the purpose of a hypervisor?

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

Question 858

An IS auditor has been assigned to review IT structures and activities recently outsourced to various providers. Which of the following should the IS auditor determine FIRST?

- ☐ That an audit clause is present in all contracts
- ☐ That the SLA of each contract is substantiated by appropriate KPIs
- ☐ That the contractual warranties of the providers support the business needs of the organization
- ☐ That at contract termination, support is guaranteed by each outsourcer for new outsourcers

Question 859

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

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

Question 860

Following best practices, formal plans for implementation of new information systems are developed during the:

- ☐ development phase.
- ☐ design phase.
- ☐ testing phase.
- ☐ deployment phase.

Question 861

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 862

An IS steering committee should:

- ☐ include a mix of members from different departments and staff levels.
- ☐ ensure that IS security policies and procedures have been executed properly.
- ☐ have formal terms of reference and maintain minutes of its meetings.
- ☐ be briefed about new trends and products at each meeting by a vendor.

Question 863

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

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

Question 864

Off-site data backup and storage should be geographically separated so as to _____ (fill in the blank) the risk of a widespread physical disaster such as a hurricane or earthquake.

- ☐ Accept
- ☐ Eliminate
- ☐ Transfer
- ☐ Mitigate

Question 865

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 866

An IS auditor is assessing risk associated with peer-to-peer file sharing within an organization. Which of the following should be of GREATEST concern?

- ☐ File-sharing policies have not been reviewed since last year
- ☐ Only some employees are required to attend security awareness training
- ☐ Not all devices are running antivirus programs
- ☐ The organization does not have an efficient patch management process

Question 867

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 868

Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

- ☐ Discussion with management
- ☐ Review of the organization chart
- ☐ Observation and interviews
- ☐ Testing of user access rights

Question 869

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 870

An IS auditor is reviewing the physical security measures of an organization. Regarding the access card system, the IS auditor should be MOST concerned that:

- ☐ nonpersonalized access cards are given to the cleaning staff, who use a sign-in sheet but show no proof of identity.
- ☐ access cards are not labeled with the organization's name and address to facilitate easy return of a lost card.
- ☐ card issuance and rights administration for the cards are done by different departments, causing unnecessary lead time for new cards.
- ☐ the computer system used for programming the cards can only be replaced after three weeks in the event of a system failure.

Question 871

Which of the following would be the MOST effective control to mitigate unintentional misuse of authorized access?

- ☐ Regular monitoring of user access logs
- ☐ Annual sign-off of acceptable use policy
- ☐ Security awareness training
- ☐ Formalized disciplinary action

Question 872

When preparing an audit report, the IS auditor should ensure that the results are supported by:

- ☐ statements from IS management.
- ☐ workpapers of other auditors.
- ☐ an organizational control self-assessment.
- ☐ sufficient and appropriate audit evidence.

Question 873

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 874

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 875

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 876

The optimum business continuity strategy for an entity is determined by the:

- ☐ lowest downtime cost and highest recovery cost.
- ☐ lowest sum of downtime cost and recovery cost.
- ☐ lowest recovery cost and highest downtime cost.
- ☐ average of the combined downtime and recovery cost.

Question 877

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 878

An IS auditor has completed a service level management audit related to order management services provided by a third party. Which of the following is the MOST significant finding?

- ☐ The third party has offshore support arrangements.
- ☐ Penalties for missing service levels are limited.
- ☐ The service level agreement does not define how availability is measured.
- ☐ Service desk support is not available outside the company's business hours.

Question 879

An IS auditor has been asked to advise on the design and implementation of IT management best practices. Which of the following actions would impair the auditor's independence?

- ☐ Providing consulting advice for managing applications
- ☐ Designing an embedded audit module
- ☐ Implementing risk response on management's behalf
- ☐ Evaluating the risk management process

Question 880

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 881

An information security manager learns that a departmental system is out of compliance with the information security policy's authentication requirements. Which of the following should be the information security manager's FIRST course of action?

- ☐ Isolate the noncompliant system from the rest of the network.
- ☐ Submit the issue to the steering committee for escalation.
- ☐ Request risk acceptance from senior management.
- ☐ Conduct an impact analysis to quantify the associated risk.

Question 882

Which of the following provides the BEST evidence of an organization's disaster recovery readiness?

- ☐ A disaster recovery plan
- ☐ Customer references for the alternate site provider
- ☐ Processes for maintaining the disaster recovery plan
- ☐ Results of tests and drills

Question 883

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

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

Question 884

Which of the following layer of an enterprise data flow architecture is concerned with transporting information between the various layers?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☐ Application messaging layer
- ☐ Data access layer

Question 885

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 886

Which of the following presents an inherent risk with no distinct identifiable preventive controls?

- ☐ Piggybacking
- ☐ Viruses
- ☐ Data diddling
- ☐ Unauthorized application shutdown

Question 887

What is the primary security concern for EDI environments?

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

Question 888

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 889

One advantage of managing an entire collection of projects as a portfolio is that it highlights the need to:

- ☐ identify dependencies between projects.
- ☐ inform users about all ongoing projects.
- ☐ manage the risk of each individual project.
- ☐ manage the quality of each project.

Question 890

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 891

The prioritization of incident response actions should be PRIMARILY based on which of the following?

- ☐ Scope of disaster
- ☐ Business impact
- ☐ Availability of personnel
- ☐ Escalation process

Question 892

An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the GREATEST risk?

- ☐ Pilot
- ☐ Parallel
- ☐ Direct cutover
- ☐ Phased

Question 893

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 894

Which of the following methods of encryption has been proven to be almost unbreakable when correctly used?

- ☐ key pair
- ☐ Oakley
- ☐ certificate
- ☐ 3-DES
- ☐ one-time pad
- ☐ None of the choices.

Question 895

Which of the following would MOST likely require a business continuity plan to be invoked?

- ☐ A distributed denial of service attack on an email server
- ☐ An unauthorized visitor discovered in the data center
- ☐ An epidemic preventing staff from performing job functions
- ☐ A hacker holding personally identifiable information hostage.

Question 896

When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

- ☐ analysis.
- ☐ evaluation.
- ☐ preservation.
- ☐ disclosure.

Question 897

Which of the following would be the GREATEST cause for concern when data are sent over the Internet using HTTPS protocol?

- ☐ Presence of spyware in one of the ends
- ☐ The use of a traffic sniffing tool
- ☐ The implementation of an RSA-compliant solution
- ☐ A symmetric cryptography is used for transmitting data

Question 898

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

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

Question 899

Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

- ☐ True
- ☐ False

Question 900

An employee of an organization has reported losing a smartphone that contains sensitive information. The BEST step to address this situation should be to:

- ☐ terminate the device connectivity
- ☐ escalated to the user's management
- ☐ disable the user's access to corporate resources
- ☐ remotely wipe the device

Question 901

In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as:

- ☐ wormnets
- ☐ trojannets
- ☐ spynets
- ☐ botnets
- ☐ rootnets
- ☐ backdoor

Question 902

Whenever an application is modified, what should be tested to determine the full impact of the change?

- ☐ Interface systems with other applications or systems
- ☐ The entire program, including any interface systems with other applications or systems
- ☐ All programs, including interface systems with other applications or systems
- ☐ Mission-critical functions and any interface systems with other applications or systems

Question 903

In a relational database with referential integrity, the use of which of the following keys would prevent deletion of a row from a customer table as long as the customer number of that row is stored with live orders on the orders table?

- ☐ Foreign key
- ☐ Primary key
- ☐ Secondary key
- ☐ Public key

Question 904

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

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

Question 905

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

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

Question 906

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

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

Question 907

Which of the following activities is MOST important in determining whether a test of a disaster recovery plan 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 908

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 909

Which of the following is the BEST IS audit strategy?

- ☐ Perform audits based on impact and probability of error and failure.
- ☐ Cycle general control and application audits over a two-year period.
- ☐ Conduct general control audits annually and application audits in alternating years.
- ☐ Limit audits to new application system developments.

Question 910

An auditor needs to be aware of technical controls which are used to protect computer from malware. Which of the following technical control interrupts DoS and ROM BIOS call and look for malware like action?

- ☐ Scanners
- ☐ Active Monitors
- ☐ Immunizer
- ☐ Behavior blocker

Question 911

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 912

The BEST way to evaluate the effectiveness of a newly developed application is to:

- ☐ perform a post-implementation review.
- ☐ analyze load-testing results.
- ☐ review acceptance-testing results.
- ☐ perform a pre-implementation review.

Question 913

During an internal audit review of an HR recruitment system implementation, the IS auditor notes a number of defects were unresolved at the time the system went live. Which of the following is the auditor's MOST important task prior to formulating an audit opinion?

- ☐ Identify the root cause of the defects to confirm severity.
- ☐ Review the user acceptance test results.
- ☐ Verify risk acceptance by the project steering committee.
- ☐ Confirm the timeline for migration of the defects.

Question 914

A financial services organization is developing and documenting business continuity measures. In which of the following cases would an IS auditor MOST likely raise an issue?

- ☐ The organization uses good practice guidelines instead of industry standards and relies on external advisors to ensure the adequacy of the methodology.
- ☐ The business continuity capabilities are planned around a carefully selected set of scenarios which describe events that might happen with a reasonable probability.
- ☐ The recovery time objectives (RTOs) do not take IT disaster recovery constraints into account, such as personnel or system dependencies during the recovery phase.
- ☐ The organization plans to rent a shared alternate site with emergency workplaces which has only enough room for half of the normal staff.

Question 915

Change management procedures are established by IS management to:

- ☐ control the movement of applications from the test environment to the production environment.
- ☐ control the interruption of business operations from lack of attention to unresolved problems.
- ☐ ensure the uninterrupted operation of the business in the event of a disaster.
- ☐ verify that system changes are properly documented.

Question 916

The MOST important difference between hashing and encryption is that hashing:

- ☐ is irreversible.
- ☐ output is the same length as the original message.
- ☐ is concerned with integrity and security.
- ☐ is the same at the sending and receiving end.

Question 917

Which of the following would contribute MOST to an effective business continuity plan (BCP)?

- ☐ Document is circulated to all interested parties
- ☐ Planning involves all user departments
- ☐ Approval by senior management
- ☐ Audit by an external IS auditor

Question 918

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 919

What is an initial step in creating a proper firewall policy?

- ☐ Assigning access to users according to the principle of least privilege
- ☐ Determining appropriate firewall hardware and software
- ☐ Identifying network applications such as mail, web, or FTP servers
- ☐ Configuring firewall access rules

Question 920

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 921

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 922

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

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

Question 923

During a business continuity audit an IS auditor found that the business continuity plan (BCP) covered only critical processes. The IS auditor should:

- ☐ recommend that the BCP cover all business processes.
- ☐ assess the impact of the processes not covered.
- ☐ report the findings to the IT manager.
- ☐ redefine critical processes.

Question 924

Which of the following should be the MOST important consideration when prioritizing the funding for competing IT projects?

- ☐ Criteria used to determine the benefits of projects
- ☐ Skills and capabilities within the project management team
- ☐ Quality and accuracy of the IT project inventory
- ☐ Senior management preferences

Question 925

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

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

Question 926

An organization has begun using social media to communicate with current and potential clients. Which of the following should be of PRIMARY concern to the auditor?

- ☐ Using a third-party provider to host and manage content
- ☐ Lack of guidance on appropriate social media usage and monitoring
- ☐ Negative posts by customers affecting the organization's image
- ☐ Reduced productivity of staff using social media

Question 927

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 928

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

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

Question 929

The sophistication and formality of IS audit programs may vary significantly depending on which of the following factors?

- ☐ the target's management hands-on involvement.
- ☐ the target's location.
- ☐ the target's size and complexity.
- ☐ the target's budget.
- ☐ the target's head count.
- ☐ None of the choices.

Question 930

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 931

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 932

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

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

Question 933

Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

- ☐ has been approved by line management.
- ☐ does not vary from the IS department's preliminary budget.
- ☐ complies with procurement procedures.
- ☐ supports the business objectives of the organization.

Question 934

When planning an audit, it is acceptable for an IS auditor to rely on a third-party provider's external audit report on service level management when the:

- ☐ report was released within the last 12 months.
- ☐ scope and methodology meet audit requirements.
- ☐ service provider is independently certified and accredited.
- ☐ report confirms that service levels were not violated.

Question 935

Which of the following virus prevention techniques can be implemented through hardware?

- ☐ Remote booting
- ☐ Heuristic scanners
- ☐ Behavior blockers
- ☐ Immunizers

Question 936

What is a reliable technique for estimating the scope and cost of a software-development project?

- ☐ Function point analysis (FPA)
- ☐ Feature point analysis (FPA)
- ☐ GANTT
- ☐ PERT

Question 937

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 938

During an IS audit, auditor has observed that authentication and authorization steps are split into two functions and there is a possibility to force the authorization step to be completed before the authentication step. Which of the following technique an attacker could user to force authorization step before authentication?

- ☐ Eavesdropping
- ☐ Traffic analysis
- ☐ Masquerading
- ☐ Race Condition

Question 939

After threats to a data center are identified, an IS auditor would expect management to FIRST:

- ☐ recommend required actions to executive management.
- ☐ discuss risk management practices with neighboring firms.
- ☐ implement procedures to address all identified threats.
- ☐ establish and quantify the potential effects if each threat occurs.

Question 940

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 941

To address the issue that performance pressures on IT may conflict with information security controls, it is MOST important that:

- ☐ the security policy is changed to accommodate IT performance pressure
- ☐ noncompliance issues are reported senior management
- ☐ senior management provides guidance and dispute resolution
- ☐ information security management understands business performance issues

Question 942

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

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

Question 943

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 944

During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

- ☐ an unauthorized user may use the ID to gain access.
- ☐ user access management is time consuming.
- ☐ passwords are easily guessed.
- ☐ user accountability may not be established.

Question 945

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

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

Question 946

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 947

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 948

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 949

A CEO requests access to corporate documents from a mobile device that does not comply with organizational policy. The information security manager should FIRST:

- ☐ evaluate the business risk
- ☐ evaluate a third-party solution
- ☐ initiate an exception approval process
- ☐ deploy additional security controls

Question 950

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 951

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 952

In addition to the backup considerations for all systems, which of the following is an important consideration in providing backup for online systems?

- ☐ Maintaining system software parameters
- ☐ Ensuring periodic dumps of transaction logs
- ☐ Ensuring grandfather-father-son file backups
- ☐ Maintaining important data at an offsite location

Question 953

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 954

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 955

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

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

Question 956

Which of the following would BEST assist an information security manager in gaining strategic support from executive management?

- ☐ Research on trends in global information security breaches
- ☐ Risk analysis specific to the organization
- ☐ Annual report of security incidents within the organization
- ☐ Rating of the organization's security based on international standards

Question 957

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

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

Question 958

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 959

An IS auditor evaluating the resilience of a high-availability network should be MOST concerned if:

- ☐ the setup is geographically dispersed.
- ☐ the network servers are clustered in a site.
- ☐ a hot site is ready for activation.
- ☐ diverse routing is implemented for the network.

Question 960

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 961

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 962

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 963

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 964

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

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

Question 965

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 966

The reason a certification and accreditation process is performed on critical systems is to ensure that:

- ☐ security compliance has been technically evaluated.
- ☐ data have been encrypted and are ready to be stored.
- ☐ the systems have been tested to run on different platforms.
- ☐ the systems have followed the phases of a waterfall model.

Question 967

Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirety or not at all. Atomicity is part of the ACID test reference for transaction processing.

True or false?

- ☐ True
- ☐ False

Question 968

To prevent IP spoofing attacks, a firewall should be configured to drop a packet if:

- ☐ the source routing field is enabled.
- ☐ it has a broadcast address in the destination field.
- ☐ a reset flag (RST) is turned on for the TCP connection.
- ☐ dynamic routing is used instead of static routing.

Question 969

As part of the business continuity planning process, which of the following should be identified FIRST in the business impact analysis?

- ☐ Organizational risks, such as single point-of-failure and infrastructure risk
- ☐ Threats to critical business processes
- ☐ Critical business processes for ascertaining the priority for recovery
- ☐ Resources required for resumption of business

Question 970

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 971

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 972

An IS auditor is told by IS management that the organization has recently reached the highest level of the software capability maturity model (CMM). The software quality process MOST recently added by the organization is:

- ☐ continuous improvement.
- ☐ quantitative quality goals.
- ☐ a documented process.
- ☐ a process tailored to specific projects.

Question 973

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 974

Which of the following types of attack works by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs?

- ☐ format string vulnerabilities
- ☐ integer overflow
- ☐ code injection
- ☐ command injection
- ☐ None of the choices.

Question 975

An organization currently using tape backups takes one full backup weekly and incremental backups daily. They recently augmented their tape backup procedures with a backup-to-disk solution. This is appropriate because:

- ☐ fast synthetic backups for offsite storage are supported.
- ☐ backup to disk is always significantly faster than backup to tape.
- ☐ tape libraries are no longer needed.
- ☐ data storage on disks is more reliable than on tapes.

Question 976

What is the BEST action to prevent loss of data integrity or confidentiality in the case of an e-commerce application running on a LAN, processing electronic fund transfers (EFT) and orders?

- ☐ Using virtual private network (VPN) tunnels for data transfer
- ☐ Enabling data encryption within the application
- ☐ Auditing the access control to the network
- ☐ Logging all changes to access lists

Question 977

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

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

Question 978

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 979

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

- ☐ Plan
- ☐ Do
- ☐ Check
- ☐ Act

Question 980

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 981

An organization has detected sensitive data leakage caused by an employee of a third-party contractor. What is the BEST course of action to address this issue?

- ☐ Include security requirements in outsourcing contracts.
- ☐ Activate the organization's incident response plan.
- ☐ Limit access to the third-party contractor.
- ☐ Terminate the agreement with the third-party contractor.

Question 982

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 983

What is a common vulnerability, allowing denial-of-service attacks?

- ☐ Assigning access to users according to the principle of least privilege
- ☐ Lack of employee awareness of organizational security policies
- ☐ Improperly configured routers and router access lists
- ☐ Configuring firewall access rules

Question 984

Which of the following should be the PRIMARY consideration for IT management when selecting a new information security tool that monitors suspicious file access patterns?

- ☐ Integration with existing architecture
- ☐ Ease of support and troubleshooting
- ☐ Data correlation and visualization capabilities
- ☐ Ability to contribute to key performance indicator data

Question 985

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 986

Which of the following would provide the BEST evidence of successfully completed batch uploads?

- ☐ Sign-off on the batch journal
- ☐ Using sequence controls
- ☐ Enforcing batch cut-off times
- ☐ Reviewing process logs

Question 987

An organization is using a single account shared by personnel for its social networking marketing page. Which of the following is the BEST method to maintain accountability over the account?

- ☐ Reviewing access rights on a periodic basis
- ☐ Integrating the account with a single sign-on
- ☐ Regular monitoring of proxy server logs
- ☐ Implementing an account password check-out process

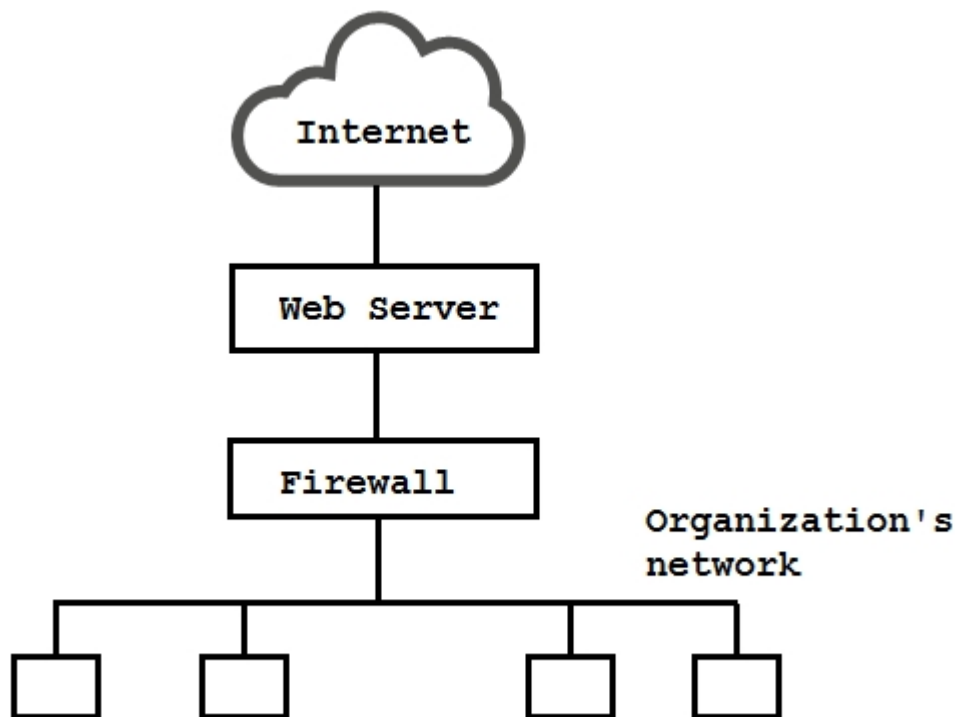
Question 988

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 989

E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network.



The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

- ☐ alert the appropriate staff.
- ☐ create an entry in the log.
- ☐ close firewall-2.
- ☐ close firewall-1.

Question 990

An IS auditor submitted audit reports and scheduled a follow-up audit engagement with a client. The client has requested to engage the services of the same auditor to develop enhanced controls. What is the GREATEST concern with this request?

- ☐ It would require the approval of the audit manager.
- ☐ It would be beyond the original audit scope.
- ☐ It would a possible conflict of interest.
- ☐ It would require a change to the audit plan.

Question 991

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

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

Question 992

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

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

Question 993

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 994

What is the most effective means of determining that controls are functioning properly within an operating system?

- ☐ Interview with computer operator
- ☐ Review of software control features and/or parameters
- ☐ Review of operating system manual
- ☐ Interview with product vendor

Question 995

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 996

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

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

Question 997

Which of the following would have the HIGHEST priority in a business continuity plan (BCP)?

- ☐ Resuming critical processes
- ☐ Recovering sensitive processes
- ☐ Restoring the site
- ☐ Relocating operations to an alternative site

Question 998

An IS auditor is assessing the results of an organization's post-implementation review of a newly developed information system. Which of the following should be the auditor's MAIN focus?

- ☐ The procurement contract has been closed.
- ☐ Lessons learned have been identified.
- ☐ The disaster recovery plan has been updated.
- ☐ Benefits realization analysis has been completed.

Question 999

Active radio frequency ID (RFID) tags are subject to which of the following exposures?

- ☐ Session hijacking
- ☐ Eavesdropping
- ☐ Malicious code
- ☐ Phishing

Question 1000

Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs. True or false?

- ☐ True
- ☐ False

Question 1001

Which of the following is the MOST effective type of antivirus software?

- ☐ Scanners
- ☐ Active monitors
- ☐ integrity checkers
- ☐ Vaccines

Question 1002

Which of the following statement correctly describes the difference between total flooding and local application extinguishing agent?

- ☐ The local application design contain physical barrier enclosing the fire space where as physical barrier is not present in total flooding extinguisher
- ☐ The total flooding design contain physical barrier enclosing the fire space where as physical barrier is not present in local application design extinguisher
- ☐ The physical barrier enclosing fire space is not present in total flooding and local application extinguisher agent
- ☐ The physical barrier enclosing fire space is present in total flooding and local application extinguisher agent

Question 1003

After implementing an information security governance framework, which of the following would provide the BEST information to develop an information security project plan?

- ☐ Balanced scorecard
- ☐ Recent audit results
- ☐ Risk heat map
- ☐ Gap analysis

Question 1004

In a multinational organization, local security regulations should be implemented over global security policy because:

- ☐ global security policies include unnecessary controls for local businesses
- ☐ business objectives are defined by local business unit managers
- ☐ requirements of local regulations take precedence
- ☐ deploying awareness of local regulations is more practical than of global policy

Question 1005

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

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

Question 1006

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

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

Question 1007

During an application audit, an IS auditor finds several problems related to corrupted data in the database. Which of the following is a corrective control that the IS auditor should recommend?

- ☐ implement data backup and recovery procedures.
- ☐ Define standards and closely monitor for compliance.
- ☐ Ensure that only authorized personnel can update the database.
- ☐ Establish controls to handle concurrent access problems.

Question 1008

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 1009

A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:

- ☐ Identify high-risk areas that might need a detailed review later
- ☐ Reduce audit costs
- ☐ Reduce audit time
- ☐ Increase audit accuracy

Question 1010

Sending a message and a message hash encrypted by the sender's private key will ensure:

- ☐ authenticity and integrity.
- ☐ authenticity and privacy.
- ☐ integrity and privacy.
- ☐ privacy and nonrepudiation.

Question 1011

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 1012

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

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

Question 1013

A benefit of open system architecture is that it:

- ☐ facilitates interoperability.
- ☐ facilitates the integration of proprietary components.
- ☐ will be a basis for volume discounts from equipment vendors.
- ☐ allows for the achievement of more economies of scale for equipment.

Question 1014

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 1015

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 1016

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 1017

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 1018

Which of the following is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality?

- ☐ Function point analysis
- ☐ Critical path methodology
- ☐ Rapid application development
- ☐ Program evaluation review technique

Question 1019

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 1020

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 1021

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 1022

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 1023

To ensure authentication, confidentiality and integrity of a message, the sender should encrypt the hash of the message with the sender's:

- ☐ public key and then encrypt the message with the receiver's private key.
- ☐ private key and then encrypt the message with the receiver's public key.
- ☐ public key and then encrypt the message with the receiver's public key.
- ☐ private key and then encrypt the message with the receiver's private key.

Question 1024

The GREATEST benefit of using a prototyping approach in software development is that it helps to:

- ☐ decrease the time allocated for user testing and review
- ☐ minimize scope changes to the system
- ☐ conceptualize and clarify requirements
- ☐ improve efficiency of quality assurance (QA) testing

Question 1025

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 1026

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 1027

Which of the following uses a prototype that can be updated continually to meet changing user or business requirements?

- ☐ PERT
- ☐ Rapid application development (RAD)
- ☐ Function point analysis (FPA)
- ☐ GANTT

Question 1028

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

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

Question 1029

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 1030

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 1031

An employee has accidentally posted confidential data to the company's social media page. Which of the following is the BEST control to prevent this from recurring?

- ☐ Require all updates to be made by the marketing director
- ☐ Implement a moderator approval process
- ☐ Perform periodic audits of social media updates
- ☐ Establish two-factor access control for social media accounts

Question 1032

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 1033

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

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

Question 1034

Which of the following is a rewrite of ipfwadm?

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

Question 1035

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 1036

What should the information security manager do FISRT when end users express that new security controls are too restrictive?

- ☐ Perform a risk assessment on modifying the control environment.
- ☐ Perform a cost-benefit analysis on modifying the control environment.
- ☐ Conduct a business impact analysis (BIA).
- ☐ Obtain process owner buy-in to remove the controls.

Question 1037

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 1038

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 1039

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

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

Question 1040

Which of the following term related to network performance refers to the number of corrupted bits expressed as a percentage or fraction of the total sent?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Error Rate

Question 1041

Which of the following component of an expert system allows the expert to enter knowledge into the system without the traditional mediation of a software engineer?

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

Question 1042

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 1043

An IS auditor is assigned to audit a software development project which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

- ☐ Report that the organization does not have effective project management.
- ☐ Recommend the project manager be changed.
- ☐ Review the IT governance structure.
- ☐ Review the conduct of the project and the business case.

Question 1044

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 1045

During a follow-up audit, an IS auditor concludes that a previously identified issue has not been adequately remediated. The auditee insists the risk has been addressed. The auditor should:

- ☐ recommend an independent assessment by a third party
- ☐ report the disagreement according to established procedures
- ☐ follow-up on the finding next year
- ☐ accept the auditee's position and close the finding

Question 1046

Which of the following types of attack makes use of common consumer devices that can be used to transfer data surreptitiously?

- ☐ Direct access attacks
- ☐ Indirect access attacks
- ☐ Port attack
- ☐ Window attack
- ☐ Social attack
- ☐ None of the choices.

Question 1047

The extent to which data will be collected during an IS audit should be determined based on the:

- ☐ availability of critical and required information.
- ☐ auditor's familiarity with the circumstances.
- ☐ auditee's ability to find relevant evidence.
- ☐ purpose and scope of the audit being done.

Question 1048

Which of the following functions is performed by a virtual private network (VPN)?

- ☐ Hiding information from sniffers on the net
- ☐ Enforcing security policies
- ☐ Detecting misuse or mistakes
- ☐ Regulating access

Question 1049

The advantage of a bottom-up approach to the development of organizational policies is that the policies:

- ☐ are developed for the organization as a whole
- ☐ are more likely to be derived as a result of a risk assessment.
- ☐ will not conflict with overall corporate policy.
- ☐ ensure consistency across the organization.

Question 1050

Which of the following methods BEST ensures that a comprehensive approach is used to direct information security activities?

- ☐ Creating communication channels
- ☐ Promoting security training
- ☐ Establishing a steering committee
- ☐ Holding periodic meetings with business owners

Question 1051

What is the first step in a business process re-engineering project?

- ☐ Identifying current business processes
- ☐ Forming a BPR steering committee
- ☐ Defining the scope of areas to be reviewed
- ☐ Reviewing the organizational strategic plan

Question 1052

During what process should router access control lists be reviewed?

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

Question 1053

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

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

Question 1054

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 1055

An IS auditor conducting a review of disaster recovery planning (DRP) at a financial processing organization has discovered the following:

- The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.
- The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting their attention.
- the plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.

The IS auditor's report should recommend that:

- ☐ the deputy CEO be censured for their failure to approve the plan.
- ☐ a board of senior managers is set up to review the existing plan.
- ☐ the existing plan is approved and circulated to all key management and staff.
- ☐ a manager coordinates the creation of a new or revised plan within a defined time limit.

Question 1056

Who is primarily responsible for storing and safeguarding the data?

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

Question 1057

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

- ☐ True
- ☐ False

Question 1058

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 1059

The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

- ☐ Inherent
- ☐ Detection
- ☐ Control
- ☐ Business

Question 1060

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

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

Question 1061

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 1062

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 1063

Which of the following refers to a method of bypassing normal system authentication procedures?

- ☐ virus
- ☐ worm
- ☐ trojan horse
- ☐ spyware
- ☐ rootkits
- ☐ backdoor
- ☐ None of the choices.

Question 1064

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 1065

A database administrator has detected a performance problem with some tables which could be solved through denormalization. This situation will increase the risk of:

- ☐ concurrent access.
- ☐ deadlocks.
- ☐ unauthorized access to data.
- ☐ a loss of data integrity.

Question 1066

As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

- ☐ The same value.
- ☐ Greater value.
- ☐ Lesser value.
- ☐ Prior audit reports are not relevant.

Question 1067

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

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

Question 1068

Which of the following audit risk is related to material error exist that would not be prevented or detected on timely basis by the system of internal controls?

- ☐ Inherent Risk
- ☐ Control Risk
- ☐ Detection Risk
- ☐ Overall Audit Risk

Question 1069

Which type of risk would MOST influence the selection of a sampling methodology?

- ☐ Control
- ☐ Inherent
- ☐ Residual
- ☐ Detection

Question 1070

Which of the following is an estimation technique where the results can be measure by the functional size of an information system based on the number and complexity of input, output, interface and queries?

- ☐ Functional Point analysis
- ☐ Gantt Chart
- ☐ Time box management
- ☐ Critical path methodology

Question 1071

Which of the following is the BEST reason to certify an organization to an international security standard?

- ☐ The certification covers enterprise security end-to-end.
- ☐ The certification reduces information security risk.
- ☐ The certification ensures that optimal controls are in place.
- ☐ The certification delivers value to stakeholders.

Question 1072

Which of the following activities would be 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 1073

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 1074

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 1075

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

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

Question 1076

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 1077

An information security policy stating that 'the display of passwords must be masked or suppressed' addresses which of the following attack methods?

- ☐ Piggybacking
- ☐ Dumpster diving
- ☐ Shoulder surfing
- ☐ Impersonation

Question 1078

Due to the increasing size of a database, user access times and daily backups continue to increase. Which of the following would be the BEST way to address this situation?

- ☐ Data modeling
- ☐ Data visualization
- ☐ Data mining
- ☐ Data purging

Question 1079

The reason for establishing a stop or freezing point on the design of a new system is to:

- ☐ prevent further changes to a project in process.
- ☐ indicate the point at which the design is to be completed.
- ☐ require that changes after that point be evaluated for cost-effectiveness.
- ☐ provide the project management team with more control over the project design.

Question 1080

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 1081

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 1082

The MOST important reason why an IT risk assessment should be updated on a regular basis is to:

- ☐ utilize IT resources in a cost-effective manner
- ☐ comply with data classification changes
- ☐ comply with risk management policies
- ☐ react to changes in the IT environment

Question 1083

Which of the following is the MOST effective mitigation strategy to protect confidential information from insider threats?

- ☐ Implementing authentication mechanisms
- ☐ Performing an entitlement review process
- ☐ Defining segregation of duties
- ☐ Establishing authorization controls.

Question 1084

Which of the following BEST ensures that effective change management is in place in an IS environment?

- ☐ User authorization procedures for application access are well established.
- ☐ User-prepared detailed test criteria for acceptance testing of the software.
- ☐ Adequate testing was carried out by the development team.
- ☐ Access to production source and object programs is well controlled.

Question 1085

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 1086

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 1087

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 1088

An advantage of installing a thin client architecture in a local area network (LAN) is that this would:

- ☐ stabilize network bandwidth requirements
- ☐ facilitate the updating of software versions
- ☐ ensure application availability when the server is down
- ☐ reduce the risk of a single point of failure

Question 1089

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 1090

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 1091

What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

- ☐ Document existing internal controls
- ☐ Perform compliance testing on internal controls
- ☐ Establish a controls-monitoring steering committee
- ☐ Identify high-risk areas within the organization

Question 1092

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 1093

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

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

Question 1094

An organization is considering whether to allow employees to use personal computing devices for business purposes. To BEST facilitate senior management's decision, the information security manager should:

- ☐ perform a cost-benefit analysis
- ☐ map the strategy to business objectives
- ☐ conduct a risk assessment
- ☐ develop a business case

Question 1095

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 1096

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

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

Question 1097

The MAIN criterion for determining the severity level of a service disruption incident is:

- ☐ cost of recovery.
- ☐ negative public opinion.
- ☐ geographic location.
- ☐ downtime.

Question 1098

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 1099

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 1100

Which of the following should an IS auditor be MOST concerned with during a post-implementation review?

- ☐ The system does not have a maintenance plan
- ☐ The system contains several minor defects
- ☐ The system was over budget by 15%
- ☐ The system deployment was delayed by three weeks

Question 1101

In an annual audit cycle, the audit of an organization's IT department resulted in many findings. Which of the following would be the MOST important consideration when planning the next audit?

- ☐ Limiting the review to the deficient areas
- ☐ Verifying that all recommendations have been implemented
- ☐ Postponing the review until all of the findings have been rectified
- ☐ Following up on the status of all recommendations

Question 1102

Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

- ☐ Apply single sign-on for access control.
- ☐ Enforce an internal data access policy.
- ☐ Enforce the use of digital signatures.
- ☐ Implement segregation of duties.

Question 1103

The BEST way to minimize the risk of communication failures in an e-commerce environment would be to use:

- ☐ compression software to minimize transmission duration.
- ☐ functional or message acknowledgments.
- ☐ a packet-filtering firewall to reroute messages.
- ☐ leased asynchronous transfer mode lines.