THE CISSP AND SSCP OPEN STUDY GUIDES WEB SITE IS PROUD TO PRESENT

THE CISA PRACTICE QUIZ

CCCURE
ENTERPRISE SECURITY
&
TRAINING INC.

THIS QUIZ WAS CONTRIBUTED BY:
JORGE DELGADO (jdelgado@tscinfosec.com)

I would like to thank Jorge personally for his very generous contribution. It is contribution like this one that helps in making the site better. If you have your own study notes, tips, tricks, why don't you share them with members of the site as well. Simply send them to cdupuis@cccure.org and I will be very happy to post them for all to use in their own studies.

A BIT OF LEGALITIES:

If you find error or wish to further contribute to the content of the quiz, please forward all queries to cdupuis@cccure.org

By keeping one central copy of the quiz, it will allow us to maintain one location where the most up to date copy can be downloaded and will avoid having 20 rogue copies all over the net.

For you people who have printed PDF copy of my quizzes in the past and have resold them (you know who you are), I specifically preclude anyone from reselling this quiz or making money off this quiz. This quiz was contributed to be freely shared to all and not for making money from it.

I strongly welcome anyone using the quiz to contribute back to the community by sending links, tips, tricks, and other information that can help the CISA in becoming on their exam day.

Best regards

Clement
cdupuis@cccure.org

Maintainer of The CISSP and SSCP Open Study Guides web site
http://www.cccure.org

Maintainer of the Professional Security Testers web site
http://www.professionalsecuritytesters.org

1. 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?

A. Inadequate screen/report design facilities
B. Complex programming language subsets
C. Lack of portability across operating systems
D. Inability to perform data intensive operations

Answer: D

4GLs are usually not suitable for data intensive operations. Instead, they are used mainly for graphic user interface (GUI) design or as simple query/report generators. Screen/report design facilities are one of the main advantages of 4GLs, and 4GLs have simple programming language subsets. Portability is also one of the main advantages of 4GLs.

2. Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?

A. Field checks
B. Control totals
C. Reasonableness checks
D. A before-and-after maintenance report

Answer: D

A before-and-after maintenance report is the best answer because a visual review would provide the most positive verification that updating was proper.

3. Which of the following is a dynamic analysis tool for the purpose of testing software modules?

A. Blackbox test
B. Desk checking
C. Structured walk-through
D. Design and code

Answer: A

A blackbox test is a dynamic analysis tool for testing software modules. During the testing of software modules a blackbox test works first in a cohesive manner as one single unit/entity, consisting of numerous modules and second, with the user data that flows across software modules. In some cases, this even drives the software behavior. In choices B, C and D, the software (design or code) remains static and somebody simply closely examines it by applying his/her mind, without actually activating the software. Hence, these cannot be referred to as dynamic analysis tools.

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

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

Answer: A

A BPR project more often leads to an increased number of people using technology, and this would be a cause for concern. As BPR is often technology oriented, and this technology is usually more complex and volatile than in the past, cost savings do not often materialize in this area. There is no reason for IP to conflict with a BPR project, unless the project is not run properly.

5. Which of the following devices extends the network and has the capacity to store frames and act as a storage and forward device?

A. Router
B. Bridge
C. Repeater
D. Gateway

Answer: B

A bridge connects two separate networks to form a logical network (e.g., joining an ethernet and token network) and has the storage capacity to store frames and act as a storage and forward device. Bridges operate at the OSI data link layer by examining the media access control header of a data packet. Routers are switching devices that operate at the OSI network layer by examining network addresses (i.e., routing information encoded in an IP packet). The router, by examining the IP address, can make intelligent decisions in directing the packet to its destination. Repeaters amplify transmission signals to reach remote devices by taking a signal from a LAN, reconditioning and retiming it, and sending it to another. This functionality is hardware encoded and occurs at the OSI physical layer. Gateways provide access paths to foreign networks.

6. Which of the following is a benefit of using callback devices?

A. Provide an audit trail
B. Can be used in a switchboard environment
C. Permit unlimited user mobility
D. Allow call forwarding

Answer: A

A callback feature hooks into the access control software and logs all authorized and unauthorized access attempts, permitting the follow-up and further review of potential breaches. Call forwarding (choice D) is a means of potentially bypassing callback control. By dialing through an authorized phone number from an unauthorized phone number, a perpetrator can gain computer access. This vulnerability can be controlled through callback systems that are available.

7. 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:

A. dials back to the user machine based on the user id and password using a telephone number from its database.
B. dials back to the user machine based on the user id and password using a telephone number provided by the user during this connection.
C. waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using its database.
D. waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using the sender's database.

Answer: A

A call-back system in a net centric environment would mean that a user with an id and password calls a remote server through a dial-up line first, and 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. Although the server can depend upon its own database, it cannot know the authenticity of the dialer when the user dials again. The server cannot depend upon the sender's database to dial back as the same could be manipulated.

8. Structured programming is BEST described as a technique that:

A. provides knowledge of program functions to other programmers via peer reviews.
B. reduces the maintenance time of programs by the use of small-scale program modules.
C. makes the readable coding reflect as closely as possible the dynamic execution of the program.
D. controls the coding and testing of the high-level functions of the program in the development process.

Answer: B

A characteristic of structured programming is smaller, workable units. Structured programming has evolved because smaller, workable units are easier to maintain. Structured programming is a style of programming which restricts the kinds of control structures. This limitation is not crippling any program can be written with allowed control structures. Structured programming is sometimes referred to as go-to-less programming, since a go-to statement is not allowed. This is perhaps the most well known restriction of the style, since go-to statements were common at the time structured programming was becoming more popular. Statement labels also become unnecessary, except in languages where subroutines are identified by labels.

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

A. Range check
B. Check digit
C. Validity check
D. Duplicate check

Answer: B

A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered or an incorrect, but valid, value substituted. This control is effective in detecting transposition and transcription errors. A range check is checking data that matches a predetermined range of values. A validity check is programmed checking of the data validity in accordance with predetermined criteria. In a duplicate check, new or fresh transactions are matched to those previously entered to ensure that they are not already in the system.

10. An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

A. cold site.
B. warm site.
C. dial-up site.
D. duplicate processing facility.

Answer: A

A cold site is ready to receive equipment but does not offer any components at the site in advance of the need. A warm site is an offsite backup facility that is configured partially with network connections and selected peripheral equipment, such as disk and tape units, controllers and CPUs, to operate an information processing facility. A duplicate information processing facility is a dedicated, self-developed recovery site that can back up critical applications.

11. A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

A. Unit testing
B. Integration testing
C. Design walk-throughs
D. Configuration management

Answer: B

A common system maintenance problem is that errors are often corrected quickly (especially when deadlines are tight), units are tested by the programmer, and then transferred to the acceptance test area. This often results in system problems that should have been detected during integration or system testing. Integration testing aims at ensuring that the major components of the system interface correctly.

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

A. communications handler.

B. EDI translator.
C. application interface.
D. EDI interface.

Answer: A

A communications handler transmits and receives electronic documents between trading partners and/or wide area networks (WANs). An EDI translator translates data between the standard format and a trading partner's proprietary format. An application interface moves electronic transactions to, or from, the application system and performs data mapping. An EDI interface manipulates and routes data between the application system and the communications handler.

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

A. testing stage.
B. evaluation stage.
C. maintenance stage.
D. early stages of planning.

Answer: D

A company in the early stages of a BCP will incur the most significant level of program development effort, which will level out as the BCP moves into maintenance, testing and evaluation stages. It is during the planning stage that an IS auditor will play an important role in obtaining senior management's commitment to resources and assignment of BCP responsibilities.

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

A. Bus
B. Ring
C. Star
D. Completely connected (mesh)

Answer: D

A completely connected mesh configuration creates a direct link between any two host machines. A bus configuration links all stations along one transmission line. A ring configuration forms a circle, and all stations are attached to a point on the transmission circle. In a star configuration each station is linked directly to a main hub.

15. Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

A. Check digit
B. Existence check
C. Completeness check
D. Reasonableness check

Answer: C

A completeness check is used to determine if a field contains data and not zeros or blanks. A check digit is a digit calculated mathematically to ensure original data was not altered. An existence check also checks entered data for agreement to predetermined criteria. A reasonableness check matches input to predetermined reasonable limits or occurrence rates.

16. Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

A. A substantive test of program library controls
B. A compliance test of program library controls
C. A compliance test of the program compiler controls
D. A substantive test of the program compiler controls

Answer: B

A compliance test determines if controls are operating as designed and are being applied in a manner that complies with management policies and procedures. For example, if the IS auditor is concerned whether program library controls are working properly, the IS auditor might select a sample of programs to determine if the source and object versions are the same. In other words, the broad objective of any compliance test is to provide auditors with reasonable assurance that a particular control on which the auditor plans to rely is operating as the auditor perceived it in the preliminary evaluation.

17. A data administrator is responsible for:

A. maintaining database system software.
B. defining data elements, data names and their relationship.
C. developing physical database structures.
D. developing data dictionary system software.

Answer: B

A data administrator is responsible for defining data elements, data names and their relationship. Choices A, C and D are functions of a database administrator (DBA)

18. A database administrator is responsible for:

A. defining data ownership.
B. establishing operational standards for the data dictionary.
C. creating the logical and physical database.
D. establishing ground rules for ensuring data integrity and security.

Answer: C

A database administrator is responsible for creating and controlling the logical and physical database. Defining data ownership resides with the head of the user department or top management if the data is common to the organization. IS management and the data administrator are responsible for establishing operational standards for the data dictionary. Establishing ground rules for ensuring data integrity and security in line with the corporate security policy is a function of the security administrator.

19. An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

A. defining the conceptual schema.
B. defining security and integrity checks.
C. liaising with users in developing data model.
D. mapping data model with the internal schema.

Answer: D

A DBA only in rare instances should be mapping data elements from the data model to the internal schema (physical data storage definitions). To do so would eliminate data independence for application systems. Mapping of the data model occurs with the conceptual schema since the conceptual schema represents the enterprisewide view of data within an organization and is the basis for deriving an end-user department data model.

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

A. the entire message and thereafter enciphering the message digest using the sender's private key.
B. any arbitrary part of the message and thereafter enciphering the message digest using the sender's private key.
C. the entire message and thereafter enciphering the message using the sender's private key.
D. the entire message and thereafter enciphering the message along with the message digest using the sender's private key.

Answer: A

A digital signature is a cryptographic method that ensures data integrity, authentication of the message, and non-repudiation. To ensure these, the sender first creates a message digest by applying a cryptographic hashing algorithm against the entire message and thereafter enciphers the message digest using the sender's private key. A message digest is created by applying a cryptographic hashing algorithm against the entire message not on any arbitrary part of the message. After creating the message digest, only the message digest is enciphered using the sender's private key, not the message.

21. A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

A. digest signature.
B. electronic signature.
C. digital signature.
D. hash signature.

Answer: C

A digital signature through the private cryptographic key authenticates a transmission from a sender through the private cryptographic key. It is a string of bits that uniquely represent another string of bits, a digital document. An electronic signature refers to the string of bits that digitally represents a handwritten signature captured by a computer system when a human applies it on an electronic pen pad, connected to the system.

22. A critical function of a firewall is to act as a:

A. special router that connects the Internet to a LAN.
B. device for preventing authorized users from accessing the LAN.
C. server used to connect authorized users to private trusted network resources.
D. proxy server to increase the speed of access to authorized users.

Answer: B

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users of other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling the outside resources to which its own users have access. Basically, a firewall, working closely with a router program, filters all network packets to determine whether or not to forward them toward their destination. A firewall includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so no incoming request can get directed to private network resources.

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

A. Spool
B. Cluster controller
C. Protocol converter
D. Front end processor

Answer: D

A front-end processor is a hardware device that connects all communication lines to a central computer to relieve the central computer.

24. The use of a GANTT chart can:

A. aid in scheduling project tasks.
B. determine project checkpoints.
C. ensure documentation standards.
D. direct the post-implementation review.

Answer: A

A GANTT chart is used in project control. It may aid in the identification of needed checkpoints but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the post-implementation review.

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

A. Gateway
B. Protocol converter
C. Front-end communication processor
D. Concentrator/multiplexor

Answer: A

A gateway performs the job of translating e-mail formats from one network to another so messages can make their way through all the networks. A protocol converter is a hardware device that converts between two different types of transmissions, such as asynchronous and synchronous transmissions. A front-end communication processor connects all network communication lines to a central computer to relieve the central computer from performing network control, format conversion and message handling tasks. A concentrator/multiplexor is a device used for combining several lower-speed channels into a higher-speed channel.

26. Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

A. Specific developments only
B. Business requirements only
C. All phases of the installation must be documented
D. No need to develop a customer specific documentation

Answer: C

A global enterprise product reengineering (EPR) software package can be applied to a business to replace, simplify and improve the quality of IS processing. Documentation is intended to help understand how, why and which solutions that have been selected and implemented, and therefore must be specific to the project. Documentation is also intended to support quality assurance and must be comprehensive.

27. A hub is a device that connects:

A. two LANs using different protocols.
B. a LAN with a WAN.
C. a LAN with a metropolitan area network (MAN).
D. two segments of a single LAN.

Answer: D

A hub is a device that connects two segments of a single LAN. A hub is a repeater. It provides transparent connectivity to users on all segments of the same LAN. It is a level 1 device. A bridge operates at level 2 of the OSI layer and is used to connect two LANs using different protocols (e.g., joining an ethernet and token network) to form a logical network. A gateway, which is a level 7 device, is used to connect a LAN to a WAN. A LAN is connected with a MAN using a router, which operates in the network layer.

28. A LAN administrator normally would be restricted from:

A. having end-user responsibilities.
B. reporting to the end-user manager.
C. having programming responsibilities.
D. being responsible for LAN security administration.

Answer: C

A LAN administrator should not have programming responsibilities but may have end-user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator also may be responsible for security administration over the LAN.

29. Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital?

A. Multiplexer
B. Modem
C. Protocol converter
D. Concentrator

Answer: B

A modem is a device that translates data from digital to analog and back to digital.

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

A. A neural network
B. Database management software
C. Management information systems
D. Computer assisted audit techniques

Answer: A

A neural network will monitor and learn patterns, reporting exceptions for investigation. Database management software is a method of storing and retrieving data. Management information systems provide management statistics but do not normally have a monitoring and detection function. Computer-assisted audit techniques detect specific situations, but are not intended to learn patterns and detect abnormalities.

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

A. duplicate check.
B. table lookup.
C. validity check.
D. parity check.

Answer: D

A parity check will help to detect data errors when data are read from memory or communicated from one computer to another. A one-bit digit (either 0 or 1) is added to a data item to indicate whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, an error report is generated. Choices A, B and C are types of data validation and editing controls.

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

A. Point-of-sale system
B. Corporate planning
C. Regulatory reporting
D. Departmental chargeback

Answer: A

A point-of-sale system is a critical online system that when inoperable will jeopardize the ability of a company to generate revenue and track inventory properly.

33. The initial step in establishing an information security program is the:

A. development and implementation of an information security standards manual.
B. performance of a comprehensive security control review by the IS auditor.

C. adoption of a corporate information security policy statement.
D. purchase of security access control software.

Answer: C

A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

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

A. logic bomb.
B. stealth virus.
C. trojan horse.
D. polymorphic virus.

Answer: D

A polymorphic virus has the capability of changing its own code, enabling it to have many different variants. Since they have no consistent binary pattern, such viruses are hard to identify. A logic bomb is code that is hidden in a program or system which will cause something to happen when the user performs a certain action or when certain conditions are met. A logic bomb, which can be downloaded along with a corrupted shareware or freeware program, may destroy data, violate system security, or erase the hard drive. A stealth virus is a virus that hides itself by intercepting disk access requests. When an antivirus program tries to read files or boot sectors to find the virus, the stealth virus feeds the antivirus program a clean image of the file or boot sector. A trojan horse is a virus program that appears to be useful and harmless but which has harmful side effects such as destroying data or breaking the security of the system on which it is run.

35. Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

A. Paper test
B. Post test
C. Preparedness test
D. Walk-through

Answer: C

A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments. A paper test is a walkthrough of the plan, involving major players in the plan's execution who attempt to determine what might happen in a particular type of service disruption. A paper test usually precedes the preparedness test. A post-test is actually a test phase and is comprised of a group of activities, such as returning all resources to their proper place, disconnecting equipment, returning personnel and deleting all company data from third-party systems. A walk-through is a test involving a simulated disaster situation that tests the preparedness and understanding of management and staff, rather than the actual resources.

36. An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST cost-effective test of the DRP?

A. Full operational test
B. Preparedness test
C. Paper test
D. Regression test

Answer: B

A preparedness test is performed by each local office/area to test the adequacy of the preparedness of local operations for the disaster recovery. A paper test is a structured walkthrough of the DRP and should be conducted before a preparedness test. A full operational test is conducted after the paper and preparedness test. A regression test is not a DRP test and is used in software maintenance.

37. 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?

A. Relocate the shut off switch.
B. Install protective covers.
C. Escort visitors.
D. Log environmental failures.

Answer: B

A protective cover over the switch would allow it to be accessible and visible, but would prevent accidental activation. Relocating the shut off switch would defeat the purpose of having it readily accessible. Escorting the personnel moving the equipment may not have prevented this incident and logging of environmental failures would provide management with a report of incidents, but reporting alone would not prevent a reoccurrence.

38. A company has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

A. Acceptance testing is to be managed by users.
B. A quality plan is not part of the contracted deliverables.
C. Not all business functions will be available on initial implementation.
D. Prototyping is being used to confirm that the system meets business requirements.

Answer: B

A quality plan is an essential element of all projects. It is critical that the contracted supplier be required to produce such a plan. The quality plan for the proposed development contract should be comprehensive and encompass all phases of the development and include which business functions will be included and when. Acceptance is normally managed by the user area, since they must be satisfied that the new system will meet their requirements. If the system is large, a phased-in approach to implementing the application is a reasonable approach. Prototyping is a valid method of ensuring that the system will meet business requirements.

39. In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

A. registration authority (RA).
B. issuing certification authority (CA).
C. subject CA.
D. policy management authority.

Answer: A

A RA is an entity that is responsible for identification and authentication of certificate subjects, but the RA does not sign or issue certificates. The certificate subject usually interacts with the RA for completing the process of subscribing to the services of the certification authority in terms of getting identity validated with standard identification documents, as detailed in the certificate policies of the CA. In the context of a particular certificate, the issuing CA is the CA that issued the certificate. In the context of a particular CA certificate, the subject CA is the CA whose public key is certified in the certificate.

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

A. Hash totals
B. Reasonableness checks
C. Online access controls
D. Before and after image reporting

Answer: B

A reasonableness check is a data validation edit and control, used to ensure that data conforms to predetermined criteria. Before and after image reporting is a control over data files that makes it possible to trace changes. Online access controls are designed to prevent unauthorized access to the system and data. A hash total is a total of any numeric data field or series of data elements in a data file. This total is checked against a control total of the same field or fields to ensure completeness of processing.

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

A. reasonableness check.
B. parity check.
C. redundancy check.
D. check digits.

Answer: A

A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of data. A reasonableness check compares data to predefined reasonability limits or occurrence rates established for the data. A parity check is a hardware control that detects data errors when data are read from one computer to another, from memory or during transmission. Check digits detect transposition and transcription errors.

42. Applying a retention date on a file will ensure that:

A. data cannot be read until the date is set.
B. data will not be deleted before that date.
C. backup copies are not retained after that date.
D. datasets having the same name are differentiated.

Answer: B

A retention date will ensure that a file cannot be overwritten before that date has passed. The retention date will not affect the ability to read the file. Backup copies would be expected to have a different retention date and therefore may well be retained after the file has been overwritten. The creation date, not the retention date, will differentiate files with the same name.

43. Which of the following is the BEST audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

A. Review the parameter settings
B. Interview the firewall administrator
C. Review the actual procedures
D. Review the device's log file for recent attacks

Answer: A

A review of the parameter settings will provide a good basis for comparison of the actual configuration to the security policy and will provide audit evidence documentation. The other choices do not provide as strong audit evidence as choice A.

44. An organization is considering installing a LAN in a site under construction. If system availability is the main concern, which of the following topologies is MOST appropriate?

A. Ring
B. Line
C. Star
D. Bus

Answer: A

A ring or loop topology would enable messages to be rerouted should the network cabling be severed at any point or a hardware element fail. With the correct settings in network hardware, the loss of any link would be invisible to the users. In line and bus networks, which are essentially the same thing, terminals

are connected to a single cable. If this cable is severed, all terminals beyond the point of severance will be unavailable. A star network clusters terminals around hubs, connected to the server by separate lines in the form of a star. If any line is severed, all terminals in the cluster at the end of that line would be disconnected.

45. 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:

A. scan of all floppy disks before use
B. virus monitor on the network file server
C. scheduled daily scan of all network drives
D. virus monitor on the user's personal computer

Answer: C

A scheduled daily scan of all network drives will detect the presence of a virus after the infection has occurred. All of the other choices are controls designed to prevent a computer virus from infecting the system.

46. Which of the following types of firewalls would BEST protect a network from an Internet attack?

A. Screened subnet firewall
B. Application filtering gateway
C. Packet filtering router
D. Circuit-level gateway

Answer: A

A screened subnet firewall would provide the best protection. The screening router can be a commercial router or a node with routing capabilities and the ability to allow or avoid traffic between nets or nodes based on addresses, ports, protocols, interfaces, etc. Application-level gateways are mediators between two entities that want to communicate, also known as proxy gateways. The application level (proxy) works at the application level, not only at a package level. The screening controls at package level, addresses, ports, etc. but does not see the contents of the package. A packet filtering router examines the header of every packet or data traveling between the Internet and the corporate network.

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

A. Iris scanning plus finger print scanning
B. Terminal ID plus global positioning system (GPS)
C. A smart card requiring the user's PIN
D. User ID along with password

Answer: C

A smart card addresses what the user has. This is generally used in conjunction with testing what the user knows, e.g., a key board password or personal identification number (PIN). Proving who the user is usually requires a biometrics method, such as finger print, iris scan or voice verification, to prove biology. This is not a two-factor user authentication because it proves only who the user is. A global positioning system (GPS) receiver reports on where the user is. An ID and password (what the user knows), is a single-factor user authentication.

48. Which of the following audit tools is MOST useful to an IS auditor when an audit trail is required?

A. Integrated test facility (ITF)
B. Continuous and intermittent simulation (CIS)
C. Audit hooks
D. Snapshots

Answer: D

A snapshot tool is most useful when an audit trail is required. ITF can be used to incorporate test transactions into a normal production run of a system. CIS is useful when transactions meeting certain

criteria need to be examined. Audit hooks are useful when only select transactions or processes need to be examined.

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

A. Response
B. Correction
C. Detection
D. Monitoring

Answer: A

A sound IS security policy will most likely outline a response program to handle suspected intrusions. Correction, detection and monitoring programs are all aspects of information security, but will not likely be included in an IS security policy statement.

50. Which of the following is a network architecture configuration that links each station directly to a main hub?

A. Bus
B. Ring
C. Star
D. Completed connected

Answer: C

A star network architecture configuration links each station directly to a main hub. Bus configurations link all stations along one transmission medium, ring configurations attach all stations to a point on a circle and completely connected configurations provide a direct link between two host machines.

51. A strength of an implemented quality system based on ISO 9001 is that it:

A. guarantees quality solutions to business problems.
B. results in improved software life cycle activities.
C. provides clear answers to questions concerning cost-effectiveness.
D. does not depend on the maturity of the implemented quality system.

Answer: B

A strength of an implemented quality system based on ISO 9001 is that it enhances improvements in software life cycle activities, quality assurance and quality control. Weaknesses of the system include that it can fail to provide clear answers to questions concerning productivity, reliability or cost-effectiveness of the system. A quality system is not a guarantee of quality solutions to business problems since poorly defined user requirements will adversely affect the design of the software. Depending on the maturity of the implemented quality system stages can vary from not implemented to fully implemented procedures.

52. An organization has an integrated development environment (IDE), where the program libraries reside on the server, but modification/development and testing are done from PC workstations. Which of the following would be a strength of an integrated development environment?

A. Controls the proliferation of multiple versions of programs
B. Expands the programming resources and aids available
C. Increases program and processing integrity
D. Prevents valid changes from being overwritten by other changes

Answer: B

A strength of an integrated development environment is that it expands the programming resources and aids available. The other choices are IDE weaknesses.

53. Peer reviews to detect software errors during a program development activity are called:

A. emulation techniques.
B. structured walk-throughs.
C. modular program techniques.
D. top-down program construction.

Answer: B

A structured walk-through is a management tool for improving productivity. Structured walk-throughs can detect an incorrect or improper interpretation of the program specifications. This, in turn, improves the quality of system testing and acceptance of it. The other choices are methods or tools in the overall systems development process.

54. Which of the following duties would be a concern if performed along with systems administration?

A. Maintenance of access rules
B. Review of system audit trail
C. Data librarian
D. Performance monitoring

Answer: B

A system administrator performs various functions by using the admin/root or an equivalent login. This login enables the system administrator to have unlimited access to the system resources. The only control over the system administrator's activities is the system audit trail, hence, it should be reviewed by someone other than the system administrator. Maintenance of access rules, data librarian functions and performance monitoring can be assigned to the system administrator.

55. Without compensating controls, which of the following functions would represent a risk if combined with that of a system analyst?

A. Application programming
B. Data entry
C. Quality assurance
D. Database administrator

Answer: C

A system analyst should not perform quality assurance (QA) duties as independence would be impaired, since the systems analyst is part of the team developing/designing the software. A system analyst can perform the other functions. The best example is a citizen programmer. A citizen (name related to citizen, since they have the right to do all or anything) programmer who has access to development tools can do all aspects while developing software (design, development, testing, implementation). Only good compensatory controls would be able to monitor/control these activities. Compensating controls will ensure these functions have been effectively performed. If an analyst compromises on functions in these roles, it can be detected immediately with the help of compensating controls. However, a system analyst should be discouraged from performing the role of QA, since quality assurance levels could be compromised if it does not meet the agreed standards.

56. Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance program?

A. A system downtime log
B. Vendors' reliability figures
C. Regularly scheduled maintenance log
D. A written preventive maintenance schedule

Answer: A

A system downtime log provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

57. A programmer included a routine into a payroll application to search for his/her own payroll number. As a result, if this payroll number does not appear during the payroll run, a routine will generate and place random numbers onto every paycheck. This routine is known as:

A. scavenging.
B. data leakage.
C. piggybacking.
D. a trojan horse.

Answer: D

A trojan horse is malicious code hidden in an authorized computer program. The hidden code will be executed whenever the authorized program is executed. In this case, as long as the perpetrator's payroll number is part of the payroll process nothing happens, but as soon as the payroll number is gone havoc occurs.

58. Which of the following is a form of an Internet attack?

A. Searching for software design errors
B. Guessing user passwords based on their personal information
C. Breaking the deadman's door to gain entry
D. Planting a trojan horse

Answer: D

A trojan horse is the only attack among the choices. The other choices, may be considered risks but are not in themselves attacks.

59. Which of the following would enable an enterprise to provide access to its intranet (i.e., extranet) across the Internet to its business partners?

A. Virtual private network
B. Client-server
C. Dial-in access
D. Network service provider

Answer: A

A virtual private network (VPN) allows external partners to securely participate in the extranet using public networks as a transport or shared private networks. Because of its low cost, using public networks (Internet) as a transport is the principal method. VPNs rely on tunneling/encapsulation techniques, which allow the Internet protocol (IP) to carry a variety of different protocols (e.g., SNA, IPX, NETBEUI). A client-server (choice B) does not address extending the network to business partners (i.e., client-servers refers to a group of computers within an organization connected by a communications network where the client is the request machine and the server is the supplying machine). Choice C refers to remote users accessing a secured environment. It is the means, not the method of providing access to a network. A network service provider (choice D) may provide services to a shared private network in providing Internet services, but not extended to an organization's intranet.

60. When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator to ensure that the:

A. hardware is protected against power surges.
B. integrity is maintained if the main power is interrupted.
C. immediate power will be available if the main power is lost.
D. hardware is protected against long-term power fluctuations.

Answer: A

A voltage regulator protects against short-term power fluctuations. It normally does not protect against long-term surges, nor does it maintain the integrity if power is interrupted or lost.

61. Which of the following functions is performed by a virtual private network (VPN)?

A. Hiding information from sniffers on the net
B. Enforcing security policies
C. Detecting misuse or mistakes

D. Regulating access

Answer: A

A VPN hides information from sniffers on the net. Using encryption, a VPN hides information. It works based on tunneling. A VPN does not analyze information packets and therefore cannot enforce security policies, nor does it check the content of packets and so cannot detect misuse or mistakes, and it does not perform an authentication function, and hence cannot regulate access.

62. During the review of an organization's disaster recovery and business continuity plan, the IS auditor found that a paper test was performed to verify the existence of all necessary procedures and actions within the recovery plan. This is a:

A. preparedness test.
B. module test.
C. full test.
D. walk-through test.

Answer: D

A walk-through test is an exercise, to verify the existence of all necessary procedures and actions specified within the recovery plan. A preparedness test is the smallest set (component) of instructions within the recovery plan that enables specific processes to be performed. A module is a combination of components. The full test verifies that each component within every module is workable and satisfies the strategy and recovery time objective requirement detailed in the recovery plan.

63. Which of the following BEST describes the objectives of following a standard system development methodology?

A. To ensure that appropriate staffing is assigned and to provide a method of controlling costs and schedules
B. To provide a method of controlling costs and schedules and to ensure communication among users, IS auditors, management and IS personnel
C. To provide a method of controlling costs and schedules and an effective means of auditing project development
D. To ensure communication among users, IS auditors, management and personnel and to ensure that appropriate staffing is assigned

Answer: B

A well-defined systems development methodology will facilitate effective management of the project since costs and schedules will be monitored consistently. Also, design methodologies require various approvals and sign-offs from different functional groups. This facilitates adequate communications between these groups.

64. Which of the following will help detect changes made by an intruder to the system log of a server?

A. Mirroring of the system log on another server
B. Simultaneously duplicating the system log on a write-once disk
C. Write protecting the directory containing the system log
D. Storing the backup of the system log offsite

Answer: B

A write-once CD cannot be overwritten. Therefore, the system log duplicated on the disk could be compared to the original log to detect differences, which could be the result of changes made by an intruder. Write protecting the system log does not prevent deletion or modification, since the superuser can override the write protection. Backup and mirroring may overwrite earlier files and may not be current.

65. 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. a firewall exists.

B. a secure web connection is used.
C. the source of the executable is certain.
D. the host website is part of your organization.

Answer: C

Acceptance of these mechanisms should be based on established trust. The control is provided by only knowing the source and then allowing the acceptance of the applets. Hostile applets can be received from anywhere. It is virtually impossible to filter at this level at this time. A secure web connection or firewall are considered external defenses. A firewall will find it more difficult to filter a specific file from a trusted source. A secure web connection provides confidentiality. Neither can identify an executable as friendly. Hosting the website as part of the organization is impractical. Enabling the acceptance of Java and/or Active X is an all or nothing proposition. The client will accept the program if the parameters are established to do so.

66. An organization is developing a new business system. Which of the following will provide the MOST assurance that the system provides the required functionality?

A. Unit testing
B. Regression testing
C. Acceptance testing
D. Integration testing

Answer: C

Acceptance testing is primarily conducted by the users before sign-off. It is performed from the perspective of the users to confirm that the system has the required functionality. Unit testing is used for testing the basic functionality of a program. Regression testing is used to compare changes to an application to ensure that the programs are working the same after a change as before the change. Integration testing is used to ensure that all of the programs in an application are working correctly and that information is flowing correctly.

67. The MOST effective method of preventing unauthorized use of data files is:

A. automated file entry.
B. tape librarian.
C. access control software.
D. locked library.

Answer: C

Access control software is an active control designed to prevent unauthorized access to data.

68. Access rules normally are included in which of the following documentation categories?

A. Technical reference documentation
B. User manuals
C. Functional design specifications
D. System development methodology documents

Answer: A

Access rules usually are found in technical reference documentation. Input preparation and a description of products are examples of items found in the user manual. Functional design specifications provide a detailed explanation of the application. System development documentation consists of the initial request, user requirements, design, etc.

69. An IS auditor reviewing operating system access discovers that the system is not secured properly. In this situation, the IS auditor is LEAST likely to be concerned that the user might:

A. create new users.
B. delete database and log files.
C. access the system utility tools.
D. access the system writeable directories.

Answer: A

Access to the operating system does not result necessarily in granting access to creating new users. Hence, it is not a likely concern. The other choices are likely concerns if the operating system is not defined properly. In this case, users can access the system writeable directories, delete database and log files, and access system utility tools.

70. An internal audit department, that organizationally reports exclusively to the chief financial officer (CFO) rather than to an audit committee, is MOST likely to:

A. have its audit independence questioned.
B. report more business-oriented and relevant findings.
C. enhance the implementation of the auditor's recommendations.
D. result in more effective action being taken on the recommendations.

Answer: A

According to a recent ISACA benchmarking survey most internal audit departments report directly to an audit committee. However, many organizations also choose to have the internal audit department either jointly or solely report to the chief financial officer (CFO). In this same survey, the IS audit function almost exclusively reports directly to the director of internal audit. The IS auditor who reports to the head of an operational department would have the appearance of a compromised independence. Generally, an IS auditor should report one level above the reporting level of the auditee. Reporting to the CFO may not have an impact on the content of audit findings, which should normally be business-oriented and relevant as an auditor is expected to understand the business being audited. Taking effective action on an audit's recommendations should be the responsibility of senior management and will not be enhanced by the fact that the audit department reports to the CFO. Follow-up of the implementation of audit recommendations is conducted by the auditor and/or by the administration department and would not be enhanced by reporting to the CFO.

71. Which of the following is the MOST critical and contributes the MOST to the quality of data in a data warehouse?

A. Accuracy of the source data
B. Credibility of the data source
C. Accuracy of the extraction process
D. Accuracy of the data transformation

Answer: A

Accuracy of source data is a prerequisite for the quality of the data in a data warehouse. Credibility of the data source is important, accurate extraction processes are important and accurate transformation routines are important but would not change inaccurate data into quality (accurate) data.

72. A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface in order to provide for efficient data mapping?

A. Key verification
B. One-for-one checking
C. Manual recalculations
D. Functional acknowledgements

Answer: D

Acting as an audit trail for EDI transactions, functional acknowledgements are one of the main controls used in data mapping. All the other choices are manual input controls, whereas data mapping deals with automatic integration of data in the receiving company.

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

A. adequate fire insurance exists.

B. regular hardware maintenance is performed.
C. offsite storage of transaction and master files exists.
D. backup processing facilities are tested fully.

Answer: C

Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.

74. A single digitally signed instruction was given to a financial institution to credit a customer's account. The financial institution received the instruction three times and credited the account three times. Which of the following would be the MOST appropriate control against such multiple credits?

A. Encrypting the hash of the payment instruction with the public key of the financial institution.
B. Affixing a time stamp to the instruction and using it to check for duplicate payments.
C. Encrypting the hash of the payment instruction with the private key of the instructor.
D. Affixing a time stamp to the hash of the instruction before being digitally signed by the instructor.

Answer: B

Affixing a time stamp to the instruction and using it to check for duplicate payments makes the instruction unique. The financial institution can check that the instruction was not intercepted and replayed and thus it could prevent crediting the account three times. Encrypting the hash of the payment instruction with the public key of the financial institution does not protect replay, it only protects confidentiality and integrity of the instruction. Encrypting the hash of the payment instruction with the private key of the instructor ensures integrity of the instruction and nonrepudiation of the issued instruction. The process of creating a message digest requires applying a cryptographic hashing algorithm to the entire message. The receiver, upon decrypting the message digest, will re-compute the hash using the same hashing algorithm and compare the result with what was sent. Hence, affixing a time stamp into the hash of the instruction before being digitally signed by the instructor would violate the integrity requirements of digital signature.

75. Which of the following physical access controls would provide the highest degree of security over unauthorized access?

A. Bolting door lock
B. Cipher lock
C. Electronic door lock
D. Fingerprint scanner

Answer: D

All are physical access controls designed to protect the organization from unauthorized access. However, biometric door locks, such as a fingerprint scanner, provide advantages since they are harder to duplicate, easier to deactivate and individually identified. Biometric door locks, using an individual's unique body features are used for access when extremely sensitive facilities must be protected.

76. An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

A. this lack of knowledge may lead to unintentional disclosure of sensitive information.
B. information security is not critical to all functions.
C. IS audit should provide security training to the employees.
D. the audit finding will cause management to provide continuous training to staff.

Answer: A

All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information. Training is a preventive control. Security awareness programs for employees can prevent unintentional disclosure of sensitive information to outsiders.

77. Which of the following processes is the FIRST step in developing a business continuity and disaster recovery plan for an organization?

A. Alternate site selection
B. Business impact analysis
C. Test procedures and frequency
D. Information classification

Answer: B

"All four processes are essential for developing the business continuity plan
however, a business impact analysis is the first process so as to determine the impact of a disaster on the business operations. Information classification helps to determine the priorities of application recovery, while recovering from a disaster event. Alternate site requirements are decided and the site is selected based on the business impact analysis and recovery priorities. The testing of the plan is done after the above processes are complete."

78. Which of the following techniques or tools would assist an IS auditor when performing a statistical sampling of financial transactions maintained in a financial management information system?

A. Spreadsheets
B. Parallel simulation
C. Generalized audit software
D. Regression testing

Answer: C

All generalized audit software has facilities for statistical analysis. Spreadsheets do not lend themselves to the extraction and analysis of transaction data. Parallel simulation is a process of replicating computer-based processes. Regression testing is the process of rerunning a portion of a test plan to ensure that changes or corrections have not introduced new errors.

79. Which of the following is a disadvantage of image processing?

A. Verifies signatures
B. Improves service
C. Relatively inexpensive to use
D. Reduces deterioration due to handling

Answer: C

All of the above are advantages of image processing systems, except choice C because image processing systems are relatively expensive and companies do not invest in them lightly.

80. The feature of a digital signature that ensures the sender cannot later deny generating and sending the message is:

A. data integrity.
B. authentication.
C. nonrepudiation.
D. replay protection.

Answer: C

All of the above are features of a digital signature. Nonrepudiation ensures that the claimed sender cannot later deny generating and sending the message. Data integrity refers to changes in the plaintext message that would result in the recipient failing to compute the same message hash. Since only the claimed sender has the key, authentication ensures that the message has been sent by the claimed sender. Replay protection is a method that a recipient can use to check that the message was not intercepted and replayed.

81. Which of the following is the MOST important reason for an IS auditor to be involved in a system development project?

A. Evaluate the efficiency of resource utilization.
B. Develop audit programs for subsequent audits of the system.

C. Evaluate the selection of hardware to be used by the system.
D. Ensure that adequate controls are built into the system during development.

Answer: D

All of the answers in this question are reasons why an IS auditor should be involved in a development project. However, the most important reason is to ensure that adequate controls are built into the system during development.

82. Which of the following would BEST ensure continuity of a wide area network (WAN) across the organization?

A. Built-in alternative routing
B. Full system backup taken daily
C. A repair contract with a service provider
D. A duplicate machine alongside each server

Answer: A

Alternative routing would ensure the network would continue if a server is lost or if a link is severed as message rerouting could be automatic. System backup will not afford immediate protection. The repair contract is not as effective as permanent alternative routing. Standby servers will not provide continuity if a link is severed.

83. To check the performance of flow and error control, an IS auditor should focus the use of a protocol analyzer on which of the following layers?

A. Network
B. Transport
C. Data link
D. Application

Answer: B

Although a protocol analyzer would work at all of the OSI model layers the only layer that handles flow and error control is the transport layer.

84. When a systems development life cycle (SDLC) methodology is inadequate, the MOST serious immediate risk is that the new system will:

A. be completed late.
B. exceed the cost estimates.
C. not meet business and user needs.
D. be incompatible with existing systems.

Answer: C

Although all of the answers are risks of an inadequate SDLC methodology, the first and most devastating is that the new system will not need business and user needs and requirements.

85. Which of the following is a strength of a client-server security system?

A. Change control and change management procedures are inherently strong.
B. Users can manipulate data without controlling resources on the mainframe.
C. Network components seldom become obsolete.
D. Access to confidential data or data manipulation is controlled tightly.

Answer: B

Among the choices the only strength associated with a client-server system is that users can manipulate and change data without controlling resources on the mainframe. All other answers are false and are disadvantages of a client-server system.

86. The MOST likely explanation for the use of applets in an Internet application is that:

A. it is sent over the network from the server.
B. the server does not run the program and the output is not sent over the network.
C. they improve the performance of both the web server and network.
D. it is a JAVA program downloaded through the web browser and executed by the web server of the client machine.

Answer: C

An applet is a JAVA program that is sent over the network from the web server, through a web browser, to the client machine. Then the code is run on the machine. Since the server does not run the program and the output is not sent over the network, the performance on both the web server and network over which the server and client are connected drastically improves through the use of applets. Performance improvement is more important than the reasons offered in choices A and B. Since JAVA virtual machine (JVM) is embedded in most web browsers, the applet download through the web browser runs on the client machine from the web browser, not from the web server, making choice D incorrect.

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

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

Answer: D

An applet is a program downloaded from a web server to the client, usually through a web browser that provides functionality for database access, interactive web pages and communications with other users. Applets opening connections from the client machine to other machines on the network and damaging those machines as a denial-of-service attack pose the greatest threat to an organization and could disrupt business continuity. A program that deposits a virus on a client machine is referred to as a malicious attack (specifically meant to cause harm to a client machine), but may not necessarily result in a disruption of service. Applets recording keystrokes and, therefore, passwords and downloaded code that reads files on a client's hard drive relate more to organizational privacy issues, and although significant, are less likely to cause a significant disruption of service.

88. An IS auditor performing a review of an application's controls would evaluate the:

A. efficiency of the application in meeting the business processes.
B. impact of any exposures discovered.
C. business processes served by the application.
D. the application's optimization.

Answer: B

An application control review involves the evaluation of the application's automated controls and an assessment of any exposures resulting from the control weaknesses. The other choices may be objectives of an application audit but are not part of an audit restricted to a review of controls.

89. Reconfiguring which of the following firewall types will prevent inward downloading of files through the file transfer protocol (FTP)?

A. Circuit gateway
B. Application gateway
C. Packet filter
D. Screening router

Answer: B

An application gateway firewall is effective in preventing applications, such as FTPs, from entering the organization network. A circuit gateway firewall is able to prevent paths or circuits, not applications, from

entering the organization network. A packet filter firewall or screening router will allow or prevent access based on IP packets/address.

90. An organization is considering connecting a critical PC-based system to the Internet. Which of the following would provide the BEST protection against hacking?

A. An application-level gateway
B. A remote access server
C. A proxy server
D. Port scanning

Answer: A

"An application-level gateway is the best way to protect against hacking because it can define with detail rules that describe the type of user or connection that is, or is not permitted. It analyzes in detail each package, not only in layers one through four of the OSI model but also layers five through seven, which means that it reviews the commands of each higher level protocol (HTTP, FTP, SNMP, etc.) For a remote access server there is a device (server) asking for username and passwords before entering the network. This is good when accessing private networks, but it can be mapped or scanned from the Internet creating security exposure. Proxy servers can provide protection based on the IP address and ports. However, an individual is needed who really knows how to do this, and second applications can use different ports for the different sections of their program. Port scanning works when there is a very specific task to do, but not when trying to control what comes from the Internet (or when all the ports available need to be controlled somehow). For example, the port for &quot
Ping&quot
(echo request) could be blocked and the IP addresses would be available for the application and browsing, but would not respond to &quot
Ping&quot
. "

91. An audit charter should:

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

Answer: D

An audit charter should state management's objectives for, and delegation of authority to, IS audit. This charter should not significantly change over time and should be approved at the highest level of management. The audit charter would not be at a detail level and therefore would not include specific audit objectives or procedures.

92. The reliability of an application system's audit trail may be questionable if:

A. user IDs are recorded in the audit trail.
B. the security administrator has read-only rights to the audit file.
C. date time stamps record when an action occurs.
D. users can amend audit trail records when correcting system errors.

Answer: D

An audit trail is not effective if the details in it can be amended.

93. Which of the following should be the FIRST step of an IS audit?

A. Create a flowchart of the decision branches.
B. Gain an understanding of the environment under review.
C. Perform a risk assessment.
D. Develop the audit plan.

Answer: B

An auditor needs to gain an understanding of the processes prior to creating a flowchart. Based on the scope of the audit, the IS auditor should gain an understanding of the environment under review, and then carry out a risk assessment. Finally, on the basis of understanding the environment under review and the risk assessment, the IS auditor should prepare an audit plan.

94. While reviewing the business continuity plan of an organization, the IS auditor observed that the organization's data and software files are backed up on a periodic basis. Which characteristic of an effective plan does this demonstrate?

A. Deterrence
B. Mitigation
C. Recovery
D. Response

Answer: B

An effective business continuity plan includes steps to mitigate the effects of a disaster. Files must be restored on a timely basis for a backup plan to be effective. An example of deterrence is when a plan includes installation of firewalls for information systems. An example of recovery is when a plan includes an organization's hot site to restore normal business operations.

95. Which of the following is a feature of an intrusion detection system (IDS)?

A. Gathering evidence on attack attempts
B. Identifying weakness in the policy definition
C. Blocking access to particular sites on the Internet
D. Preventing certain users from accessing specific servers

Answer: A

An IDS can gather evidence on intrusive activity like an attack or penetration attempt. Identifying weaknesses in the policy definition is a limitation of an IDS. Choices C and D are features of firewalls, and choice B requires a manual review and is, therefore, outside the functionality of IDS.

96. Which of the following can identify attacks and penetration attempts to a network?

A. Firewall
B. Packet filters
C. Stateful inspection
D. Intrusion detection system (IDs)

Answer: D

An IDS has a large database of attack signatures, which is used to ward off attacks. Packet filter and stateful inspection are types of firewalls. A firewall is a fence around a network designed to block certain types of communications routed or passing through specific ports. It is not designed to discover someone bypassing or going under the firewall.

97. One of the purposes of library control software is to allow:

A. programmers access to production source and object libraries.
B. batch program updating.
C. operators to update the control library with the production version before testing is completed.
D. read-only access to source code.

Answer: D

An important purpose of library control software is to allow read-only access to source code. Choices A, B, and C are activities which library control software should help to prevent or prohibit.

98. Which of the following is an advantage of an integrated test facility (ITF)?

A. It uses actual master files or dummies and the IS auditor does not have to review the source of the transaction.
B. Periodic testing does not require separate test processes.
C. It validates application systems and tests the ongoing operation of the system.
D. It eliminates the need to prepare test data.

Answer: B

An integrated test facility creates a fictitious entity in the database to process test transactions simultaneously with live input. Its advantage is that periodic testing does not require separate test processes. However, careful planning is necessary and test data must be isolated from production data.

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

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

Answer: C

An integrated test facility is considered a useful audit tool because it uses the same programs to compare processing using independently calculated data. This involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.

100. In a TCP/IP-based network, an IP address specifies a:

A. network connection.
B. router/gateway.
C. computer in the network.
D. device on the network.

Answer: A

An IP address, specifies a network connection. An IP address encodes both a network and a host on that network, it does not specify an individual computer, but a connection to a network. A router/gateway connects two networks and will have two IP addresses. Hence, an IP address cannot specify a router. A computer in the network can be connected to other networks as well. It will then use many IP addresses. Such computers are called multi-homed hosts. Here again an IP address cannot refer to the computer. IP addresses do not refer to individual devices on the network, but refer to the connections by which they are connected to the network.

101. Which of the following activities should the business continuity manager perform FIRST after the replacement of hardware at the primary information processing facility?

A. Verify compatibility with the hot site.
B. Review the implementation report.
C. Perform a walk-through of the DRP.
D. Update the IS assets inventory.

Answer: D

An IS assets inventory is the basic input for the business continuity/disaster recovery plan, and the plan must be updated to reflect changes in the IS infrastructure. The other choices are procedures required to update the disaster recovery plan after having updated the required assets inventory.

102. When evaluating the collective effect of preventive, detective or corrective controls within a process an IS auditor should be aware:

A. of the point at which controls are exercised as data flows through the system.
B. that only preventive and detective controls are relevant.
C. that corrective controls can only be regarded as compensating.
D. that classification allows an IS auditor to determine which controls are missing.

Answer: A

An IS auditor should focus on when controls are exercised as data flows through a computer system. Choice B is incorrect since corrective controls may also be relevant. Choice C is incorrect since corrective controls remove or reduce the effects of errors or irregularities and are exclusively regarded as compensating controls. Choice D is incorrect and irrelevant since the existence and function of controls is important, not the classification.

103. An IS auditor who is participating in a systems development project should:

A. recommend appropriate control mechanisms regardless of cost.
B. obtain and read project team meeting minutes to determine the status of the project.
C. ensure that adequate and complete documentation exists for all project phases.
D. not worry about his/her own ability to meet target dates since work will progress regardless.

Answer: C

An IS auditor who is participating in a systems development life cycle project should ensure that adequate and complete documentation exists for all project phases. Recommendations for controls to minimize risks and exposures should consider the relative costs involved. The IS auditor should attend project team meetings and offer advice throughout, and the IS auditor should be held to the same qualitative project completion measures as the rest of the team.

104. When reviewing a business process reengineering (BPR) project, which of the following is the MOST important for an IS auditor to evaluate?

A. The impact of removed controls.
B. The cost of new controls.
C. The BPR project plans.
D. The continuous improvement and monitoring plans.

Answer: A

An IS auditor's task is to identify the existing key controls from the pre-BPR processes and determine if controls still exist in the new processes. Choice B is incorrect because even though an IS auditor may review the cost of controls it is not the most important. Choices C and D are key steps in a successful BPR project.

105. Which of the following is an objective of a control self-assessment (CSA) program?

A. Audit responsibility enhancement
B. Problem identification
C. Solution brainstorming
D. Substitution for an audit

Answer: A

An objective associated with a CSA program is the enhancement of audit responsibilities (not a replacement). Choices B and C are advantages that accrue from a CSA program, but are not objectives. A CSA program is helpful in determining audit steps by gaining an overall understanding of the audit subject and audit objective. Performance of a CSA will not replace formal audits (choice D).

106. An offsite information processing facility:

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

Answer: A

An offsite information processing facility should have the same amount of physical control as the originating site. It should not be easily identified from the outside to prevent intentional sabotage. The offsite facility should not be subject to the same natural disaster that could affect the originating site and thus should not be located in proximity of the original site, and the offsite facility should possess the same level of environmental monitoring and control as the originating site.

107. Which of the following provides a mechanism for coding and compiling programs interactively?

A. Firmware
B. Utility programs
C. Online programming facilities
D. Network management software

Answer: C

An online programming facility allows programmers to code and compile programs interactively with the computer from a terminal. Firmware is operating system program code that can be stored in read-only memories, utility programs are systems software that perform systems maintenance, and network management software controls and maintains the network.

108. An IS auditor reviews an organization chart PRIMARILY for:

A. an understanding of workflows.
B. investigating various communication channels.
C. understanding the responsibilities and authority of individuals.
D. investigating the network connected to different employees.

Answer: C

An organization chart provides information about the responsibilities and authority of individuals in the organization. This helps the IS auditor to know if there is a proper segregation of functions. A work flow chart would provide information about the roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

109. The most likely error to occur when implementing a firewall is:

A. incorrectly configuring the access lists.
B. compromising the passwords due to social engineering.
C. connecting a modem to the computers in the network.
D. inadequately protecting the network and server from virus attacks.

Answer: A

An updated and flawless access list is a significant challenge and, therefore, has the greatest chance for errors at the time of the initial installation. Passwords do not apply to firewalls, a modem bypasses a firewall and a virus attack is not an element in implementing a firewall.

110. Which of the following BEST describes an integrated test facility?

A. A technique that enables the IS auditor to test a computer application for the purpose of verifying correct processing
B. The utilization of hardware and/or software to review and test the functioning of a computer system
C. A method of using special programming options to permit printout of the path through a computer program taken to process a specific transaction
D. A procedure for tagging and extending transactions and master records that are used by an IS auditor for tests

Answer: A

"Answer A best describes an integrated test facility, which is a specialized computer-assisted audit process that allows an IS auditor to test an application on a continuous basis. Answer B is an example of a systems control audit review file
answers C and D are examples of snapshots."

111. Antivirus software should be used as a:

A. detective control.
B. preventive control.
C. corrective control.
D. compensating control.

Answer: B

Antivirus software should be used as a preventive control. It may be too late to correct a problem if the problem is not prevented in the first place.

112. 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:

A. customer over the authenticity of the hosting organization.
B. hosting organization over the authenticity of the customer.
C. customer over the confidentiality of messages from the hosting organization.
D. hosting organization over the confidentiality of messages passed to the customer.

Answer: A

Any false site will not be able to encrypt using the private key of the real site, so the customer would not be able to decrypt the message using the public key. Many customers have access to the same public key so the host cannot use this mechanism to ensure the authenticity of the customer. The customer cannot be assured of the confidentiality of messages from the host as many people have access to the public key and can decrypt the messages from the host. The host cannot be assured of the confidentiality of messages sent out, as many people have access to the public key and can decrypt them.

113. The potential for unauthorized system access by way of terminals or workstations within an organization's facility is increased when:

A. connecting points are available in the facility to connect laptops to the network.
B. users take precautions to keep their passwords confidential.
C. terminals with password protection are located in unsecured locations.
D. terminals are located within the facility in small clusters under the supervision of an administrator.

Answer: A

Any person with wrongful intentions can connect a laptop to the network. The unsecured connecting points make unauthorized access possible if the individual has knowledge of a valid user id and password. The other choices are controls for preventing unauthorized network access. If system passwords are not readily available for intruders to use, they must guess, which introduces an additional factor and requires time. System passwords provide protection against unauthorized use of terminals located in unsecured locations. Supervision is a very effective control when used to monitor access to a small operating unit or production resources.

114. The intent of application controls is to ensure that when inaccurate data is entered into the system, the data is:

A. accepted and processed.
B. accepted and not processed.
C. not accepted and not processed.
D. not accepted and processed.

Answer: C

Application controls ensure that only complete, accurate and valid data are entered in a system.

115. Which of the following functions, if combined, would be the GREATEST risk to an organization?

A. Systems analyst and database administrator
B. Quality assurance and computer operator
C. Tape librarian and data entry clerk

D. Application programmer and tape librarian

Answer: D

Application programmers should not have access to system program libraries. All other combinations, although not preferred, would normally include some type of compensating control to mitigate the lack of separation of duties.

116. Which of the following would normally be found in application run manuals?

A. Details of source documents
B. Error codes and their recovery actions
C. Program flowcharts and file definitions
D. Change records for the application source code

Answer: B

Application run manuals should include actions to be taken by an operator when an error occurs. Source documents and source code are irrelevant to the operator. Although data flow diagrams may be useful, detailed program diagrams and file definitions are not.

117. Which of the following controls is LEAST likely to detect changes made online to master records?

A. Update access to master file is restricted to a supervisor independent of data entry.
B. Clerks enter updates online and are finalized by an independent supervisor.
C. An edit listing of all updates is produced daily and reviewed by an independent supervisor.
D. An update authorization form must be approved by an independent supervisor before entry.

Answer: D

Approval by an independent supervisor prior to entry cannot control changes made online. All other responses prevent or detect the circumvention of controls.

118. An IS auditor involved as a team member in the detailed system design phase of a system under development would be MOST concerned with:

A. internal control procedures.
B. user acceptance test schedules.
C. adequacy of the user training program.
D. clerical processes for resubmission of rejected items.

Answer: A

As a member of the project team, the IS auditor's primary role is to ensure that adequate and appropriate control procedures are designed and programmed into the system. At this stage, it is too early for user acceptance schedules, training programs and user procedures to be the primary concern of the IS auditor.

119. As a business process reengineering (BPR) project takes hold it is expected that:

A. business priorities will remain stable.
B. information technologies will not change.
C. the process will improve product, service and profitability.
D. input from clients and customers will no longer be necessary.

Answer: C

As a reengineering process takes hold, certain key results will begin to emerge, including a concentration on process as a means of improving product, service and profitability. In addition, new business priorities and approaches to the use of information as well as powerful and more accessible information technologies will emerge. Often, the roles of client and customers will be redefined providing them with more direct and active participation in the enterprise's business process.

120. An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

A. evaluate the record retention plans for off-premises storage.
B. interview programmers about the procedures currently being followed.
C. compare utilization records to operations schedules.
D. review data file access records to test the librarian function.

Answer: B

Asking programmers about the procedures currently being followed is useful in determining whether access to program documentation is restricted to authorized persons. Evaluating the record retention plans for off-premises storage tests recovery procedures, not access control over program documentation. Testing utilization records or data files will not address access security over program documentation.

121. Which of the following would provide a mechanism whereby IS management can determine if the activities of the organization have deviated from the planned or expected levels?

A. Quality management
B. IS assessment methods
C. Management principles
D. Industry standards/benchmarking

Answer: B

Assessment methods provide a mechanism, whereby IS management can determine if the activities of the organization have deviated from planned or expected levels. These methods include IS budgets, capacity and growth planning, industry standards/benchmarking, financial management practices and goal accomplishment. Quality management is the means by which the IS department processes are controlled, measured and improved. Management principles focus on areas such as people, change, processes, security. Industry standards/benchmarking provide a means of determining the level of performance provided by similar information processing facility environments.

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

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

Answer: A

Assimilation of the framework and intent of a written security policy by the users of the systems is critical to the successful implementation and maintenance of security policy. You may have a good password system, but if the users of the system keep passwords written on his/her table, the password system is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, education of the users on the importance on security is of paramount importance. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software and provision for punitive actions for violation of security rules also are required along with the user's education on the importance of security.

123. Assumptions while planning an IS project involve a high degree of risk because they are:

A. based on known constraints.

B. based on objective past data.
C. a result of lack of information.
D. often made by unqualified people.

Answer: C

"Assumptions are made when adequate information is not available. When an IS project manager makes an assumption, there is a high degree of risk because the lack of proper information can cause unexpected loss to an IS project. Assumptions are not based on &quot known&quot constraints. When constraints are known in advance, a project manager can plan according to those constraints rather than assuming the constraints won't affect the project. Having objective data about past IS projects will not lead to making assumptions, but rather helps the IS project manager in planning the project in a better manner. Hence, if objective past data are available and the project manager makes use of them, risk to the project is less. Regardless of whether made by qualified people or unqualified people, assumptions are risky."

124. An IS auditor performing a review of the EFT operations of a retailing company would verify that the customers credit limit is checked before funds are transferred by reviewing the EFT:

A. system's interface.
B. switch facility.
C. personal identification number generating procedure.
D. operation backup procedures.

Answer: A

At the application processing level, the IS auditor should review the interface between the EFT system and the application system that processes the accounts from which funds are transferred. Choice B is incorrect because an EFT switch is the facility that provides the communication linkage for all equipment in the network. Choices C and D are procedures that would not help determine if the customer's credit limit is verified before the funds are transferred.

125. Automated teller machines (ATMs) are a specialized form of a point-of-sale terminal that:

A. allows for cash withdrawal and financial deposits only.
B. are usually located in populous areas to deter theft or vandalism.
C. utilizes protected telecommunication lines for data transmissions.
D. must include high levels of logical and physical security.

Answer: D

ATMs are a specialized form of a point of sale terminal, and they must have a high level of logical and physical security for the customer and the machinery. ATMs allow for a variety of transactions including cash withdrawal and financial deposits, are usually located in unattended areas and utilize unprotected telecommunication lines for data transmissions.

126. A decrease in amplitude as a signal propagates along a transmission medium is known as:

A. noise.
B. crosstalk.
C. attenuation.
D. delay distortion.

Answer: C

Attenuation is a signal degradation (decrease in amplitude) that occurs as a signal propagates along a transmission medium. This is seen particularly when the medium is copper wire. Noise is also a signal degradation that refers to a large amount of electrical fluctuation that can interfere with the interpretation of the signal by the receiver. Crosstalk is one example of noise where unwanted electrical coupling between adjacent lines causes the signal in one wire to be picked up by the signal in an adjacent wire. Delay distortion can result in a misinterpretation of a signal that results from transmitting a digital signal with varying frequency components. The various components arrive at the receiver with varying delays.

127. An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long. Which of the following could be caused by the length of the cable?

A. Electromagnetic interference (EMI)
B. Cross talk
C. Dispersion
D.Attenuation

Answer: D

Attenuation is the weakening of signals during transmission. When the signal becomes weak, it begins to read a 1 for a 0, and the user may experience communication problems. UTP faces attenuation around 100 meters. Electromagnetic interference (EMI) is caused by outside electromagnetic waves affecting the desired signals, which is not the case here. Cross talk has nothing to do with the length of the UTP cable.

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

A. Attribute sampling
B. Variable sampling
C. Stratified mean per unit
D. Difference estimation

Answer: A

Attribute sampling is the primary sampling method used for compliance testing. Attribute sampling is a sampling model that is used to estimate the rate of occurrence of a specific quality (attribute) in a population and is used in compliance testing to confirm whether the quality exists or not. The other choices are used in substantive testing which involves testing of details or quantity.

129. Which of the following is a detective control?

A. Physical access controls
B. Segregation of duties
C. Backup procedures
D. Audit trails

Answer: D

Audit trails capture information, which can be used for detecting errors. Physical access controls and segregation of duties are examples of preventive controls whereas back-up procedures are corrective controls.

130. An IS auditor performing an access controls review should be LEAST concerned if:

A. audit trails were not enabled.
B. programmers have access to the live environment.
C. group logons are being used for critical functions.
D. the same user can initiate transactions and also change related parameters.

Answer: A

Audit trails not being enabled is of least concern, as it will not result in an exposure. Programmers having access to the live environment could result in unauthorized transactions. Group logons used for critical functions is a major concern. The same user who has access to and can initiate transactions, as well as change the related parameters, is an area of high concern.

131. The primary goal of a web site certificate is:

A. authentication of the web site to be surfed through.
B. authentication of the user who surfs through that site.
C. preventing surfing of the web site by hackers.
D. the same purpose as that of a digital certificate.

Answer: A

Authenticating the site to be surfed is the primary goal of a web certificate. Authentication of a user is achieved through passwords and not by a web site certificate. The site certificate does not prevent hacking nor does it authenticate a person.

132. Authentication is the process by which the:

A. system verifies that the user is entitled to input the transaction requested.
B. system verifies the identity of the user.
C. user identifies himself to the system.
D. user indicates to the system that the transaction was processed correctly.

Answer: B

Authentication is the process by which the system verifies the identity of the user. Choice A is not the best answer because authentication refers to verifying who the user is to a security table of users authorized to access the system not necessarily the functions which the user can perform. Choice C is incorrect because this does not imply that the system has verified the identity of the user. Choice D is not correct because this is an application control for accuracy.

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

A. EDI trading partner agreements.
B. physical controls for terminals.
C. authentication techniques for sending and receiving messages.
D. program change control procedures.

Answer: C

Authentication techniques over sending and receiving messages play a key role in minimizing exposure to unauthorized transactions. The EDI trading partner agreements would minimize exposure to legal issues.

134. An IS auditor discovers that programmers have update access to the live environment. In this situation, the IS auditor is LEAST likely to be concerned that programmers can:

A. authorize transactions.
B. add transactions directly to the database.
C. make modifications to programs directly.
D. access data from live environment and provide faster maintenance.

Answer: A

Authorizing transactions implies that transactions have been initiated by another person and hence would provide the least risk. The other situations, where programmers on their own can access data and make modifications or add transactions to a database, all present a greater risk and would be of concern to the IS auditor.

135. Prices are charged on the basis of a standard master file rate that changes as volume increases. Any exceptions must be manually approved. What is the MOST effective automated control to help ensure that all price exceptions are approved?

A. All amounts are displayed back to the data entry clerk, who must verify them visually.
B. Prices outside the normal range should be entered twice to verify data entry accuracy.
C. The system beeps when price exceptions are entered and prints such occurrences on a report.
D. A second-level password must be entered before a price exception can be processed.

Answer: D

"Automated control should ensure that the system processes the price exceptions only on approval of another user who is authorized to approve such exceptions. A second-level password would ensure that

price exceptions will be approved by a user who has been authorized by management. Visual verification of all amounts by a data entry clerk is not a control, but a basic requirement for any data entry. The user being able to visually verify what has been entered is a basic manual control. Entry of price exceptions twice, is an input control. This does not ensure that exceptions will be verified automatically by another user. The system beeping on entry of a price exception is only a warning to the data entry clerk it does not prevent proceeding further. Printing of these exceptions on a report is a detective (manual) control."

136. A proposed transaction processing application will have many data capture sources and outputs in both paper and electronic form. To ensure that transactions are not lost during processing, the IS auditor should recommend the inclusion of:

A. validation controls.
B. internal credibility checks.
C. clerical control procedures.
D. automated systems balancing.

Answer: D

Automated system's balancing would be the best way to ensure that no transactions are lost as any imbalance between total inputs and total outputs would be reported for investigation and correction. Validation controls and internal credibility checks are certainly valid controls, but will not detect and report lost transactions. In addition, although a clerical procedure could be used to sum and compare inputs and outputs, an automated process is less susceptible to error.

137. Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

A. Multiple cycles of backup files remain available.

B. Access controls establish accountability for e-mail activity.
C. Data classification regulates what information should be communicated via e-mail.
D. Within the enterprise, a clear policy for using e-mail ensures that evidence is available.

Answer: A

Backup files containing documents, which supposedly have been deleted, could be recovered from these files. Access controls may help establish accountability for the issuance of a particular document, but this does not provide evidence of the e-mail. Data classification standards may be in place with regards to what should be communicated via e-mail, but the creation of the policy does not provide the information required for litigation purposes.

138. An IS auditor reviewing back-up procedures for software need only determine that:

A. object code libraries are backed up.
B. source code libraries are backed up.
C. both object and source codes libraries are backed up.
D. program patches are maintained at the originating site.

Answer: C

Backup for software must include both object and source code libraries and must include a provision for maintaining program patches on a current basis at all backup locations.

139. A company performs full backup of data and programs on a regular basis. The primary purpose of this practice is to:

A. maintain data integrity in the applications.
B. restore application processing after a disruption.
C. prevent unauthorized changes to programs and data.
D. ensure recovery of data processing in case of a disaster.

Answer: B

Backup procedures are designed to restore programs and data to a previous state prior to computer or system disruption. These backup procedures merely copy data and do not test or validate integrity. Backup procedures will also not prevent changes to program and data. On the contrary, changes will simply be copied. Although backup procedures are a necessary part of the recovery process following a disaster, they are not sufficient in themselves.

140. Using test data as part of a comprehensive test of program controls in a continuous online manner is called a/an:

A. test data/deck.
B. base case system evaluation.
C. integrated test facility (ITF).
D. parallel simulation.

Answer: B

Base case system evaluation uses test data sets developed as part of comprehensive testing programs. It is used to verify correct systems operations before acceptance, as well as periodic validation. Test data/deck simulates transactions through real programs. An ITF creates fictitious files in the database with test transactions processed simultaneously with live input. Parallel simulation is the production of data processed using computer programs that simulate application program logic.

141. Which is the first software capability maturity model (CMM) level to include a standard software development process?

A. Initial (level 1)
B. Repeatable (level 2)
C. Defined (level 3)
D. Optimizing (level 5)

Answer: C

Based on lessons learned from level 1 (initial) and level 2 (repeatable), level 3 (defined) initiates documentation to provide standardized software processes across the organization. Level 1 (initial) is characterized as ad hoc, where reliance is placed on key personnel and processes are not documented. After level 1, level 2 (repeatable) creates a learning environment where disciplined processes can be repeated successfully on other projects of similar size and scope. The ability to quantitatively control software projects arises on attaining the final level (5) of CMM. At the attainment of this level, an organization is in a position to use continuous process improvement strategies in applying innovative solutions and state-of-the-art technologies to its software projects.

142. Which of the following can be used to verify output results and control totals by matching them against the input data and control totals?

A. Batch header forms
B. Batch balancing
C. Data conversion error corrections
D. Access controls over print spools

Answer: B

"Batch balancing is used to verify output results and control totals by matching them against the input data and control totals. Batch header forms control data preparation
data conversion error corrections correct errors that occur due to duplication of transactions and inaccurate data entry
and access controls over print spools prevent reports from being accidentally deleted form print spools or directed to a different printer."

143. Which of the following would be a compensating control to mitigate risks resulting from an inadequate segregation of duties?

A. Sequence check
B. Check digit
C. Source documentation retention

D. Batch control reconciliations

Answer: D

Batch control reconciliations are an example of compensating controls. Other examples of compensating controls are transaction logs, reasonableness tests, independent reviews and audit trails such as console logs, library logs and job accounting date. Sequence checks and check digits are data validation edits and source documentation retention is an example of a data file control.

144. The most common problem in the operation of an intrusion detection system (IDS) is:

A. the detection of false positives.
B. receiving trap messages.
C. reject error rates.
D. denial-of-service attacks.

Answer: A

Because of the configuration and the way IDS technology operates, the main problem in operating IDSs is the recognition (detection) of events that are not really security incidentsÑfalse positives (equivalent of a false alarm). The IS auditor needs to be aware of this, and should check for implementation of related controls, such as IDS tuning, incident handling procedures (like the screening process to know if an event is a security incident or a false positive). Trap messages are generated by the simple network management protocol (SNMP) agents when an important event happens, but are not particularly related to security or IDSs. Reject error rate is related to biometric technology and is not related to IDSs. Denial of service is a type of attack and is not a problem in the operation of IDSs.

145. Responsibility and reporting lines cannot always be established when auditing automated systems since:

A. diversified control makes ownership irrelevant.
B. staff traditionally change jobs with greater frequency.
C. ownership is difficult to establish where resources are shared.
D. duties change frequently in the rapid development of technology.

Answer: C

Because of the diversified nature of both data and application systems, the actual owner of data and applications may be hard to establish.

146. Which of the following risks would be increased by the installation of a database system?

A. Programming errors
B. Data entry errors
C. Improper file access
D. Loss of parity

Answer: C

Because of the sharing of data with a database, improper file access is of the greatest concern. Programming and data entry errors should not increase with the installation of a database. Loss of parity can affect data transmission whether database or nondatabase.

147. Which of the following procedures can a biometric system perform?

A. Measure airborne contamination.
B. Provide security over physical access.
C. Monitor temperature and humidity levels.
D. Detect hazardous electromagnetic fields in an area.

Answer: B

Biometric devices are used to maintain physical security. Some examples are fingerprint and retina scanners. Airborne contamination is measured using air-quality monitors. Temperature and humidity levels and electromagnetic fields are measured by environmental monitoring devices.

148. Which of the following security techniques is the BEST method for authenticating a user's identity?

A. Smart card
B. Biometrics
C. Challenge-response token
D. User ID and password

Answer: B

Biometrics is a security technique that verifies an individual's identity by analyzing a physical attribute, which is unique to that individual, e.g. a handprint. Hence, biometrics ensures that the person who is authorized to access the system is in actuality the person accessing the system. Smart card (choice A) is an intelligent credit card-sized device with a chip. Anybody having the possession of the smart card and knowing the password can access the system since the system is unable to know whether the authorized user is using the smart card or not. A challenge-response token (choice C) is a method of authenticating a user, but the system is unable to know whether the authorized user is using the token or not. User ID and password (choice D) are things that could be known by another individual.

149. The difference between whitebox testing and blackbox testing is that whitebox testing:

A. involves the IS auditor.
B. is performed by an independent programmer team.
C. examines a program's internal logical structure.
D. uses the bottom-up approach.

Answer: C

Blackbox testing observes a system's external behavior, while whitebox testing is a detailed exam of a logical path, checking the possible conditions. The IS auditor need not be involved in either testing method. The bottom-up approach can be used in both tests. Whitebox testing requires knowledge of the internals of the program or the module to be implemented/tested. Blackbox testing requires that the functionality of the program be known. The independent programmer team would not be aware of the application of a program in which they have not been involved. Hence, the independent programmer team cannot provide any assistance in either of these testing approaches.

150. When two or more systems are integrated, input/output controls must be reviewed by the IS auditor in the:

A. systems receiving the output of other systems.
B. systems sending output to other systems.
C. systems sending and receiving data.
D. interfaces between the two systems.

Answer: C

Both of the systems must be reviewed for input/output controls since the output for one system is the input for the other.

151. As a result of a business process reengineering (BPR) project:

A. an IS auditor would be concerned with the key controls that existed in the prior business process and not those in the new process.
B. system processes are automated in such a way that there are more manual interventions and manual controls.
C. the newly designed business processes usually do not involve changes in the way(s) of doing business.
D. advantages usually are realized when the reengineering process appropriately suits the business and risk.

Answer: D

BPR is the process of responding to competitive, economic pressures and customer demands to survive in the current business environment. Advantages of BPR usually are experienced when the reengineering process appropriately suits the business needs. Choice A is not correct, because in a BPR, an IS auditor should have a concern that all controls, especially both those in the new processes and those key controls that may have been reengineered out of a business process. Choice B is not correct because what BPR seeks is to have less manual interventions and controls. Choice C is also incorrect because in BPR the newly designed business processes, inevitably involve changes in the way of doing business.

152. An organization's disaster recovery plan should address early recovery of:

A. all information systems processes.
B. all financial processing applications.
C. only those applications designated by the IS manager.
D. processing in priority order, as defined by business management.

Answer: D

Business management should know which systems are critical and when they need to process well in advance of a disaster. It is their responsibility to develop and maintain the plan. Adequate time will not be available for this determination once the disaster occurs. IS and the information processing facility are service organizations that exist for the purpose of assisting the general user management in successfully performing their jobs.

153. Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

A. Discussion with management
B. Review of the organization chart
C. Observation and interviews
D. Testing of user access rights

Answer: C

By observing the IS staff performing their tasks, the IS auditor can identify whether they are performing any noncompatible operations and by interviewing the IS staff the auditor can get an overview of the tasks performed. Based on the observations and interviews the auditor can evaluate the segregation of duties. Management may not be aware of the detailed functions of each employee in the IS department, therefore discussion with the management would provide only limited information regarding segregation of duties. An organization chart would not provide details of the functions of the employees and testing of user rights would provide information about the rights they have within the IS systems, but would not provide complete information about the functions they perform.

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

A. sender's private key and encrypting the message using the receiver's public key.
B. sender's public key and encrypting the message using the receiver's private key.
C. the receiver's private key and encrypting the message using the sender's public key.
D. the receiver's public key and encrypting the message using the sender's private key.

Answer: A

By signing the message with the sender's private key, the receiver can verify its authenticity using the sender's public key. By encrypting the message with the receiver's public key, only the receiver can decrypt the message using his/her own private key. The receiver's private key is confidential, and therefore unknown to the sender. Messages encrypted using the sender's private key can be read by anyone (with the sender's public key).

155. The planning and monitoring of computer resources to ensure that they are being used efficiently and effectively is:

A. hardware monitoring.
B. capacity management.
C. network management.

D. job scheduling.

Answer: B

Capacity management requires that the expansion or reduction of resources takes place in parallel with overall business growth or reduction. Input from user and IS management is required to develop a capacity plan to achieve the business goals in the most efficient and effective manner. Hardware monitoring procedures and reports are used to monitor the effective and efficient use of hardware. Network management procedures cover the activities that control and maintain the network. They provide early warning signals of problems before they affect network reliability. Job scheduling procedures determine a set of jobs and the order of priority for execution.

156. Capacity monitoring software is used to ensure:

A. maximum use of available capacity.
B. that future acquisitions meet user needs.
C. concurrent use by a large number of users.
D. continuity of efficient operations.

Answer: D

Capacity monitoring software shows the actual usage of online systems versus their maximum capacity. The aim is to enable software support staff to ensure that efficient operation, in the form of response times, is maintained in the event that use begins to approach the maximum available capacity. Systems should never be allowed to operate at maximum capacity. Monitoring software is intended to prevent this. Although the software reports may be used to support a business case for future acquisitions, it would not provide information on the effect of user requirements and it would not ensure concurrent usage of the system by users, other than to highlight levels of user access.

157. Change management procedures are established by IS management to:

A. control the movement of applications from the test environment to the production environment.
B. control the interruption of business operations from lack of attention to unresolved problems.
C. ensure the uninterrupted operation of the business in the event of a disaster.
D. verify that system changes are properly documented.

Answer: A

Change management procedures are established by IS management to control the movement of applications from the test environment to the production environment. Problem escalation procedures control the interruption of business operations from lack of attention to unresolved problems, and quality assurance procedures verify that system changes are authorized and tested.

158. The rate of change of technology increases the importance of:

A. outsourcing the IS function.
B. implementing and enforcing good processes.
C. hiring personnel willing to make a career within the organization.
D. meeting user requirements.

Answer: B

Change requires that good change management processes be implemented and enforced. Outsourcing the IS function is not directly related to the rate of technological change. Personnel in a typical IS department are highly qualified and educated, usually they do not feel their jobs are at risk and are prepared to switch jobs frequently. Although meeting user requirements is important, it is not directly related to the rate of technological change in the IS environment.

159. A programmer managed to gain access to the production library, modified a program that was then used to update a sensitive table in the payroll database and restored the original program. Which of the following methods would MOST effectively detect this type of unauthorized changes?

A. Source code comparison
B. Executable code comparison

C. Integrated test facilities (ITF)
D. Review of transaction log files

Answer: D

Changes made to the payroll database table would appear in the transaction log files. Because the original program was restored, source and executable code comparisons are ineffective. ITF is less effective than source code comparison, because it is difficult to know what to look for.

160. In a business continuity plan, there are several methods of providing telecommunication continuity. One method is diverse routing which involves:

A. providing extra capacity with the intent of using the surplus capacity should the normal primary transmission capability not be available.
B. routing information via other alternate media such as copper cable or fiber optics.
C. providing diverse long-distance network availability utilizing T-1 circuits among the major long-distance carriers.
D. routing traffic through split-cable facilities or duplicate-cable facilities.

Answer: D

Choice A defines the redundancy method, choice B defines the method of alternative routing, choice C defines the method of long-haul network diversity, and choice D defines diverse routing.

161. The responsibilities of a disaster recovery relocation team include:

A. obtaining, packaging and shipping media and records to the recovery facilities, as well as establishing and overseeing an offsite storage schedule.
B. locating a recovery site if one has not been predetermined and coordinating the transport of company employees to the recovery site.
C. managing the relocation project and conducting a more detailed assessment of the damage to the facilities and equipment.
D. coordinating the process of moving from the hot site to a new location or to the restored original location.

Answer: D

Choice A describes an offsite storage team, choice B defines a transportation team, and choice C defines a salvage team.

162. Which of the following findings would an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?

A. There are three individuals with a key to enter the area.
B. Paper documents also are stored in the offsite vault.
C. Data files, which are stored in the vault, are synchronized.
D. The offsite vault is located in a separate facility.

Answer: C

Choice A is incorrect because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties. Choice B is not correct because the IS auditor would not be concerned whether paper documents are stored in the offsite vault. In fact, paper documents, such as procedural documents and a copy of the contingency plan, most likely would be stored in the offsite vault, and the location of the vault is important, but not as important as the files being synchronized.

163. Which of the following functions, if performed by scheduling and operations personnel, would be in conflict with a policy requiring a proper segregation of duties?

A. Job submission
B. Resource management

C. Code correction
D. Output distribution

Answer: C

Code correction is a responsibility of the programming staff and should not be the responsibility of the scheduling and operations staff.

164. Which of the following facilitates program maintenance?

A. More cohesive and loosely coupled programs
B. Less cohesive and loosely coupled programs
C. More cohesive and strongly coupled programs
D. Less cohesive and strongly coupled programs

Answer: A

Cohesion refers to the performance of a single dedicated function by each program. Coupling refers to the independence of the comparable units. Loosely coupled units, when the program code is changed, will reduce the probability of affecting other program units. More cohesive and loosely coupled units are best for maintenance.

165. During an audit of the tape management system at a data center, an IS auditor discovered that parameters are set to bypass or ignore the labels written on tape header records. The IS auditor also determined that effective staging and job setup procedures were in place. In this situation, the IS auditor should conclude that the:

A. tape headers should be manually logged and checked by the operators.
B. staging and job setup procedures are not appropriate compensating controls.
C. staging and job setup procedures compensate for the tape label control weakness.
D. tape management system parameters must be set to check all labels.

Answer: C

Compensating controls are an important part of a control structure. They are considered adequate if they help to achieve the control objective and are cost-effective. In this situation the IS auditor is most likely to conclude that staging and job setup procedures compensate for the tape label control weakness.

166. Compensating controls are intended to:

A. reduce the risk of an existing or potential control weakness.
B. predict potential problems before they occur.
C. remedy problems discovered by detective controls.
D. report errors or omissions.

Answer: A

Compensating controls are intended to reduce the risk of an existing or potential control weakness. Choices B, C and D are characteristics of preventive, corrective and detective controls respectively.

167. A distinction that can be made between compliance testing and substantive testing is that compliance testing tests:

A. details, while substantive testing tests procedures.
B. controls, while substantive testing tests details.
C. plans, while substantive testing tests procedures.
D. for regulatory requirements, while substantive testing tests validations.

Answer: B

Compliance testing involves determining whether controls exist as designed whereas substantive testing relates to detailed testing of transactions/procedures. Compliance testing does not involve testing of plans. Regulatory requirements are not by themselves tested directly in compliance testing, but controls in place to ensure regulatory compliance are checked.

168. When an IS auditor obtains a list of current users with access to a WAN/LAN and verifies that those listed are active associates, the IS auditor is performing a:

A. compliance test.
B. substantive test.
C. statistical sample.
D. risk assessment.

Answer: A

Compliance tests determine if controls are being applied in accordance with management policies and procedures. In this case, verifying that only active associates are present provides reasonable assurance that a control is in place and can be relied upon. Choice B, substantive tests, relates to quantitative reviews, such as balances and transactions and their accuracy. Choice C does not relate since all current user records were verified, while choice D is part of a risk-based audit approach.

169. The use of coding standards is encouraged by IS auditors because they:

A. define access control tables.
B. detail program documentation.
C. standardize dataflow diagram methodology.
D. ensure compliance with field naming conventions.

Answer: D

Compliance with field-naming conventions ensures that ongoing program maintenance can be carried out by different programmers, and that quality controls are facilitated. Access control tables, program documentation and data flow diagram techniques normally would not be included in coding standards. An IS auditor has to be aware of such standards and their components so that they know where to look for information and why such standards are important.

170. During a review of a large data center an IS auditor observed computer operators acting as backup tape librarians and security administrators. Which of these situations would be MOST critical to report?

A. Computer operators acting as tape librarians
B. Computer operators acting as security administrators
C. Computer operators acting as a tape librarian and security administrator
D. It is not necessary to report any of these situations.

Answer: B

Computer operators should not be given security administrator access. Computer operators acting as security administrators could manipulate the security system to give themselves access. The access could be used to set up fictitious accounts and to eliminate any record of it from the log. Computer operators in large data centers are often called upon to act as tape librarians. As long as the operator cannot manipulate the system logging, it is acceptable for the librarian to track what has taken place.

171. Which of the following is widely accepted as one of the critical components in networking management?

A. Configuration management
B. Topological mappings
C. Application of monitoring tools
D. Proxy server trouble shooting

Answer: A

Configuration management is widely accepted as one of the key components of any network, since it establishes how the network will function both internally and externally. It also deals with the management of configuration and monitoring performance. Topological mappings provide outlines of the components of the network and its connectivity. Application monitoring is not essential and proxy server trouble shooting is used for trouble shooting purposes.

172. Connection-oriented protocols in the TCP/IP suite are implemented in the:

A. transport layer.
B. application layer.
C. physical layer.
D. network layer.

Answer: A

Connection-oriented protocols provide reliability of the service provided to the higher layer. It is the responsibility of such protocols in the transport layer to enhance the quality of service provided by the network layer. The application layer is concerned with applications that are closer to the user. Reliable transport of packets by connection-oriented protocols is transparent to this layer. The physical layer transmits only raw bits of data. The network layer routes packets based on information provided by the transport layer protocol.

173. Which of the following should be in place to protect the purchaser of an application package in the event that the vendor ceases to trade?

A. Source code held in escrow.
B. Object code held by a trusted third party.
C. Contractual obligation for software maintenance.
D. Adequate training for internal programming staff.

Answer: A

Contractual obligations may not be enforceable if the vendor ceases to trade. Training is irrelevant, as programmers cannot maintain an application unless source code is available. Thus, having object code available also is not an adequate solution. Only ensuring that the source code can be obtained in the event that the vendor cannot provide support will protect the purchaser.

174. Requiring passwords to be changed on a regular basis, assigning a new one-time password when a user forgets his/hers, and requiring users not to write down their passwords are all examples of:

A. audit objectives.
B. audit procedures.
C. controls objectives.
D. control procedures.

Answer: D

Control procedures are practices established by management to achieve specific objectives (control objectives, choice C). The above examples are all control procedures intended to achieve the control objective of ensuring compliance with policies, procedures and standards. Choices A and B refer to the audit process that is used to verify the effectiveness and adequacy of the control procedures

175. The BEST time to perform a control self-assessment involving line management, line staff and the audit department is at the time of:

A. compliance testing.
B. the preliminary survey.
C. substantive testing.
D. the preparation of the audit report.

Answer: B

Control self-assessment is a process in which the auditor can get the auditees together, understand the business process, define the controls and generate an assessment of how well the controls are working. This is accomplished ideally during the preliminary data gathering phase. Choices A, C, D are audit steps that are performed after a control self-assessment has been completed.

176. In which of the following phases of the system development life cycle (SDLC) is it the MOST important for the IS auditor to participate?

A. Design
B. Testing
C. Programming
D. Implementation

Answer: A

Controls should be considered in the design phase and included in the system. The cost of building controls into a system will be minimized if they are included in the initial design.

177. Creation of an electronic signature:

A. encrypts the message.
B. verifies where the message came from.
C. cannot be compromised when using a private key.
D. cannot be used with e-mail systems.

Answer: B

Creation of an electronic signature does not in itself encrypt the message or secure it from compromise. It only verifies the message's origination.

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

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

Answer: A

CSA is predicated on the review of high-risk areas that either need immediate attention, or a more thorough review at a later date. Answer B is incorrect because CSA requires the involvement of both auditors and line management. What occurs is that the internal audit function shifts some of the control monitoring responsibilities to the functional areas. Answer C is incorrect because CSA is not a replacement for traditional audits. CSA is not intended to replace audit's responsibilities, but to enhance them. Answer D is incorrect because CSA does not allow management to relinquish its responsibility for control.

179. The FIRST step in data classification is to:

A. establish ownership.
B. perform a criticality analysis.
C. define access rules.
D. create a data dictionary.

Answer: A

Data classification is necessary to define access rules based on a need-to-do and need-to-know basis. The data owner is responsible for defining the access rules are, hence establishment of ownership is the first step in data classification. The other choices are incorrect. A criticality analysis is required for protection of data, which takes input from data classification. Access definition is complete after data classification and input for a data dictionary is prepared from the data classification process.

180. Which of the following logical access exposures involves changing data before, or as it is entered into the computer?

A. Data diddling
B. Trojan horse
C. Worm
D. Salami technique

Answer: A

Data diddling involves changing data before, or as it is entered into the computer. A trojan horse involves unauthorized changes to a computer program. A worm is a destructive program that destroys data. The salami technique is a program modification that slices off small amounts of money from a computerized transaction.

181. Data edits are an example of:

A. preventive controls.
B. detective controls.
C. corrective controls.
D. compensating controls.

Answer: A

Data edits are preventive controls since they are used in a program before data is processed, thus preventing the processing of data containing errors.

182. Data flow diagrams are used by IS auditors to:

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

Answer: C

Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of data. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

183. Which of the following integrity tests examines the accuracy, completeness, consistency and authorization of data?

A. Data
B. Relational
C. Domain
D. Referential

Answer: A

Data integrity testing examines the accuracy, completeness, consistency and authorization of data. Relational integrity testing detects modification to sensitive data by the use of control totals. Domain integrity testing verifies that data conforms to specifications. Referential integrity testing ensures that data exists in its parent or original file before it exists in the child or another file.

184. Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?

A. Intrusion detection systems
B. Data mining techniques
C. Firewalls
D. Packet filtering routers

Answer: B

Data mining is a technique to detect trends or patterns of transactions or data. If the historical pattern of charges against a credit card account is changed than it is a flag that the transaction may have resulted from a fraudulent use of the card.

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

A. data owners.
B. programmers.

C. system analysts.
D. librarians.

Answer: A

Data owners are responsible for the use of data. Written authorization for users to gain access to computerized information should be provided by the data owners. Security administration with the owners approval sets up access rules stipulating which users or group of users are authorized to access data or files and the level of authorized access (read or update).

186. When an organization's network is connected to an external network in an Internet client-server model not under that organization's control, security becomes a concern. In providing adequate security in this environment, which of the following assurance levels is LEAST important?

A. Server and client authentication
B. Data integrity
C. Data recovery
D. Data confidentiality

Answer: C

Data recovery, as a corrective action, occurs after a total network failure (denial of service) and therefore is least important in assuring security in a networked environment. The other choices are proactive in nature and directly impact network security. Server and client authentication provides a way of verifying that the server bring communicating with is a valid server, and the server needs to know that the clients are in fact valid client machines. Data integrity is required for verifying that the data received over the network has not been modified during its transmission, and data confidentiality is required for protecting information sent over the network from eavesdropping.

187. Controls designed to ensure that unauthorized changes are not made to information residing in a computer file are known as:

A. data security controls.
B. implementation controls.
C. program security controls.
D. computer operations controls.

Answer: A

Data security controls are the controls that ensure data integrity, not accuracy. None of the other controls listed ensure data integrity.

188. A data warehouse is:

A. object orientated.
B. subject orientated.
C. departmental specific.
D. a volatile databases.

Answer: B

Data warehouses are subject oriented. The data warehouse is meant to help make decisions when the function(s) to be affected by the decision transgress across departments within an organization. They are nonvolatile. Object orientation and volatility are irrelevant to a data warehouse system.

189. Online banking transactions are being posted to the database when processing suddenly comes to a halt. The integrity of the transaction processing is best ensured by:

A. database integrity checks.
B. validation checks.
C. input controls.
D. database commits and rollbacks.

Answer: D

Database commits ensure the data are saved to disk while the transaction processing is underway or complete. Rollback ensures that the processing already completed is reversed back and the data already processed are not saved to the disk in the event of the failure of the completion of the transaction processing. All other options do not ensure integrity while processing is underway.

190. Which of the following controls would be MOST effective in ensuring that production source code and object code are synchronized?

A. Release-to-release source and object comparison reports
B. Library control software restricting changes to source code
C. Restricted access to source code and object code
D. Date and time-stamp reviews of source and object code

Answer: D

Date and time stamp reviews of source and object code would ensure that source code, which has been compiled matches the production object code. This is the most effective way to ensure that the approved production source code is compiled and is the one being used.

191. 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:

A. rules.
B. decision trees.
C. semantic nets.
D. data flow diagrams.

Answer: B

Decision trees use questionnaires to lead a user through a series of choices until a conclusion is reached. Rules refer to the expression of declarative knowledge through the use of if-then relationships. Semantic nets consist of a graph in which nodes represent physical or conceptual objects and the arcs describe the relationship between the nodes. Semantic nets resemble a data flow diagram and make use of an inheritance mechanism to prevent duplication of data.

192. Which of the following line media would provide the BEST security for a telecommunication network?

A. Broad band network digital transmission
B. Baseband network
C. Dial-up
D. Dedicated lines

Answer: D

Dedicated lines are set apart for a particular user or organization. Since there is no sharing of lines or intermediate entry points, the risk of interception or disruption of telecommunications messages is lower.

193. When performing an audit of access rights, an IS auditor should be suspicious of which of the following if allocated to a computer operator?

A. READ access to data
B. DELETE access to transaction data files
C. Logged READ/EXECUTE access to programs
D. UPDATE access to job control language/script files

Answer: B

Deletion of transaction data files should be a function of the application support team, not operations staff. Read access to production data is a normal requirement of a computer operator, as well as logged access to programs and access to JCL in order to control job execution.

194. A company disposing of personal computers that once were used to store confidential data should first:

A. demagnetize the hard disk.
B. low-level format the hard disk.
C. delete all data contained on the hard disk.
D. defragment the data contained on the hard disk.

Answer: A

Demagnetizing the hard disk is the best way to ensure that confidential data once stored on the hard disk cannot be recovered. Low-level formatting destroys the file allocation table not the data and the data could be reconstructed with the appropriate software. Deleting data merely removes its reference in the file allocation table and the data can be recovered. Defragmenting is an efficient procedure and does not remove data.

195. To share data in a multivendor network environment, it is essential to implement program-to-program communication. With respect to program-to-program communication features that can be implemented in this environment, which of the following makes implementation and maintenance difficult?

A. User isolation
B. Controlled remote access
C. Transparent remote access
D. The network environments

Answer: D

Depending on the complexity of the network environment, implementation of program-to-program communication features becomes progressively more difficult. It is possible to implement program-to-program communication to isolate a user in the multi-vendor network. program-to-program communication can be implemented to control and monitor the files that a user can transfer between systems, and the remote program-to-program will be transparent to the end user. All of these are security features.

196. The responsibility for designing, implementing and maintaining a system of internal control lies with:

A. the IS auditor.
B. management.
C. the external auditor.
D. the programming staff.

Answer: B

Designing, implementing and maintaining a system of internal controls, including the prevention and detection of fraud is the responsibility of management. The IS auditor assesses the risks, and performs tests to detect irregularities created by weaknesses in the structure of internal controls.

197. The use of statistical sampling procedures helps minimize:

A. sampling risk.
B. detection risk.
C. inherent risk.
D. control risk.

Answer: B

Detection risk is the risk that the IS auditor uses an inadequate test procedure and concludes that material errors do not exist, when in fact they do. Using statistical sampling, an IS auditor can quantify how closely the sample should represent the population and quantify the probability of error. Sampling risk is the risk that incorrect assumptions will be made about the characteristics of a population from which a sample is selected. Assuming there are no related compensating controls, inherent risk is the risk that an error exists, which could be material or significant when combined with other errors found

during the audit. Statistical sampling will not minimize this. Control risk is the risk that a material error exists, which will not be prevented or detected on a timely basis by the system of internal controls. This cannot be minimized using statistical sampling.

198. Detection risk refers to:

A. concluding that material errors do not exist, when in fact they do.
B. controls that fail to detect an error.
C. controls that detect high-risk errors.
D. detecting an error but failing to report it.

Answer: A

Detection risk refers to the risk that an IS auditor may use an inadequate test procedure and conclude that no material error exists when in fact errors do exist.

199. The FIRST step in developing a business continuity plan (BCP) is to:

A. classify the importance of systems.
B. establish a disaster recovery strategy.
C. determine the critical recovery time period.
D. perform a risk ranking.

Answer: A

Determining the classification of systems is the foremost step in a BCP exercise. Without determining the classification of systems other steps cannot be performed. Choices B, C and D are carried out later in the process.

200. Which of the following would be the LEAST helpful in restoring service from an incident currently underway?

A. Developing a database repository of past incidents and actions to facilitate future corrective actions
B. Declaring the incident, which not only helps to carry out corrective measures, but also improves the awareness level
C. Developing a detailed operations plan that outlines specific actions to be taken to recover from an incident
D. Establishing multidisciplinary teams consisting of executive management, security staff, information systems staff, legal counsel, public relations, etc., to carry out the response.

Answer: A

Developing a database repository of past incidents and actions to facilitate future corrective actions would be of least value in restoring service from an incident currently underway. The creation of a detailed operations plan, a multidisciplinary team and the declaration of incidents are all necessary parts of having an incident response capability, which must be carried out immediately before or during the incident to handle it properly.

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

A. Digital signatures
B. Asymmetric cryptography
C. Digital certificates
D. Message authentication code

Answer: C

Digital certificates are issued by a trusted third party. The message sender attaches the certificate rather than the public key and can verify authenticity with the certificate repository. Asymmetric cryptography is vulnerable to a man-in-the-middle attack. Digital certificates are used for confidentiality. Message authentication code is used for message integrity verification.

202. Digital signatures require the:

A. signer to have a public key and the receiver to have a private key.
B. signer to have a private key and the receiver to have a public key.
C. signer and receiver to have a public key.
D. signer and receiver to have a private key.

Answer: B

Digital signatures are intended to verify to a recipient the integrity of the data and the identity of the sender. The digital signature standard is a public key algorithm. This requires the signer to have a private key, and the receiver to have a public key.

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

A. confidentiality.
B. integrity.
C. availability.
D. timeliness.

Answer: B

Digital signatures provide integrity because the digital signature of a signed message (file, mail, document, etc.) changes every time a single bit of the document changes, thus, a signed document cannot be altered. Depending on the mechanism chosen to implement a digital signature, the mechanism might be able to ensure data confidentiality or even timeliness, but this is not assured. Availability is not related to digital signatures.

204. Disaster recovery planning addresses the:

A. technological aspect of business continuity planning.
B. operational piece of business continuity planning.
C. functional aspect of business continuity planning.
D. overall coordination of business continuity planning.

Answer: A

Disaster recovery planning is the technological aspect of business continuity planning. Business resumption planning addresses the operational part of business continuity planning.

205. Which of the following methods of providing telecommunication continuity involves routing traffic through split- or duplicate-cable facilities?

A. Diverse routing
B. Alternative routing
C. Redundancy
D. Long haul network diversity

Answer: A

Diverse routing is a method of providing telecommunication continuity that involves routing traffic through split or duplicate cable facilities. Alternative routing is accomplished via alternative media such as copper cable or wire optics, redundancy involves the use of excess capacity and long haul network diversity is a service provided by vendors to allow access to diverse long distance networks.

206. The method of routing traffic through split cable facilities or duplicate cable facilities is called:

A. alternative routing.
B. diverse routing.
C. redundancy.
D. circular routing.

Answer: B

Diverse routing is the method of routing traffic through split cable facilities or duplicate cable facilities, which can be accomplished with different/duplicate cable sheaths. Alternative routing is the method of

routing information via an alternative medium like copper cable or fiber optics. Redundancy involves providing extra capacity, with an option to use such excess capacity in the event the primary transmission capability is not available. Circular routing is the logical path of a message in a communication network based on a series of gates at the physical network layer in the open system interconnection.

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

A. alternative routing.
B. diverse routing.
C. long-haul network diversity.
D. last mile circuit protection.

Answer: B

Diverse routing routes traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and therefore subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. This type of access is time-consuming and costly. Alternative routing is a method of routing information via an alternate medium such as copper cable or fiber optics. This involves use of different networks, circuits or end points should the normal network be unavailable. Long-haul network diversity is a diverse long-distance network utilizing T-1 circuits among the major long-distance carriers. It ensures long-distance access should any one carrier experience a network failure. Last mile circuit protection is a redundant combination of local carrier T-1s, microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local carrier routing also is utilized.

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

A. address of the domain server.
B. resolution service for the name/address.
C. IP addresses for the Internet.
D. domain name system.

Answer: C

DNS is utilized primarily on the Internet for resolution of the name/address of the web site. It is an Internet service that translates domain names into IP addresses. As names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time a domain name is used, a DNS service must translate the name into the corresponding IP address. The DNS system has its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

209. A decision support system (DSS):

A. is aimed at solving highly structured problems.
B. combines the use of models with nontraditional data access and retrieval functions.
C. emphasizes flexibility in the decision making approach of users.
D. supports only structured decision-making tasks.

Answer: C

DSS emphasizes flexibility in the decision-making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions and supports semistructured decision-making tasks.

210. To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

A. during data preparation.
B. in transit to the computer.
C. between related computer runs.
D. during the return of the data to the user department.

Answer: A

During data preparation is the best answer because it establishes control at the earliest point.

211. Which of the following steps would an IS auditor normally perform FIRST in a data center security review?

A. Evaluate physical access test results.
B. Determine the risks/threats to the data center site.
C. Review business continuity procedures.
D. Test for evidence of physical access at suspect locations.

Answer: B

During planning, the IS auditor should get an overview of the functions being audited and evaluate the audit and business risks. Choices A and D are part of the audit fieldwork process that occurs subsequent to this planning and preparation. Choice C is not part of a security review.

212. During which of the following phases in systems development would user acceptance test plans normally be prepared?

A. Feasibility study
B. Requirements definition
C. Implementation planning
D. Post-implementation review

Answer: B

During requirements definition, the project team will be working with the users to define their precise objectives and functional needs. At this time, the users should be working with the team to consider and document how the system functionality can be tested to ensure it meets their stated needs. The feasibility study is too early for such detailed user involvement and the implementation planning and post-implementation review phases are too late. The IS auditor should know at what point user testing should be planned in order to ensure it is most effective and efficient.

213. Which of the following is MOST likely to occur when a system development project is in the middle of the programming/coding phase?

A. Unit tests
B. Stress tests
C. Regression tests
D. Acceptance tests

Answer: A

During the programming phase, the development team should have mechanisms in place to ensure that coding is being developed to standard and is working correctly. Unit tests are key elements of that process in that they ensure that individual programs are working correctly. They would normally be supported by code reviews. Stress tests, regression tests and acceptance testing would normally occur later in the development and testing phases. As part of the process of assessing compliance with quality processes, IS auditors should verify that such reviews are undertaken.

214. When auditing the requirements phase of a system development project, an IS auditor would:

A. assess the adequacy of audit trails.
B. identify and determine the criticality of the need.
C. verify cost justifications and anticipated benefits.
D. ensure that control specifications have been defined.

Answer: D

During the requirements phase the IS auditor should verify the detailed requirements definition document. The IS auditor would identify and determine the criticality of the need and verify all cost justifications/benefits during the feasibility phase. The assessment of the adequacy of audit trails would take place during the detailed design and programming phase.

215. Information requirement definitions, feasibility studies and user requirements are significant considerations when:

A. defining and managing service levels.
B. identifying IT solutions.
C. managing changes.
D. assessing internal IT control.

Answer: B

Each of the items listed is a step in identifying potential processes to supply information. Feasibility studies typically are not used to define service levels, manage changes to current systems or assess IT controls. The combination should point directly to satisfying a problem.

216. E-cash is a form of electronic money that:

A. can be used over any computer network.
B. utilizes reusable e-cash coins to make payments.
C. does not require the use of an Internet digital bank.
D. contains unique serial numbering to track the identity of the buyer.

Answer: A

E-cash is a form of electronic money that can be sent from any computer to any other computer using any network, including the Internet. E-cash uses coins that can be used only once, after which they are taken out of circulation. These coins are anonymous and carry no traceable information. Each transaction in which e-cash is used requires the participation of an Internet connected digital bank.

217. A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

A. Establishing an inter-networked system of client servers with suppliers for increased efficiencies
B. Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing
C. Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format
D. Reengineering the existing processing and redesigning the existing system

Answer: C

EDI is the best answer. Properly implemented (e.g., agreements with trading partners transaction standards, controls over network security mechanisms in conjunction with application controls) EDI is best suited to identify and follow up on errors more quickly, given reduced opportunities for review and authorization.

218. The impact of EDI on internal controls will be:

A. that fewer opportunities for review and authorization will exist.
B. an inherent authentication.
C. a proper distribution of EDI transactions while in the possession of third parties.
D. that IPF management will have increased responsibilities over data center controls.

Answer: A

EDI promotes a more efficient paperless environment, but at the same time, less human intervention makes it more difficult for reviewing and authorizing. Choice B is incorrect since the interaction between parties is electronic there is no inherent authentication occurring. Computerized data can look the same no matter what the source and does not include any distinguishing human element or signature. Choice C is incorrect because this is a security risk associated with EDI. Choice D is incorrect because there are relatively few, if any, additional data center controls associated with the implementation of EDI applications. Instead, more control will need to be exercised by the user's application system to replace manual controls, such as site reviews of documents. More emphasis will need to be placed on control over data transmission (network management controls).

219. Electronic signatures can prevent messages from being:

A. suppressed.
B. repudiated.
C. disclosed.
D. copied.

Answer: B

Electronic signatures provide a receipt of the transaction ensuring that the entities that participated in that transaction cannot repudiate their commitments. An electronic signature does not prevent messages from being suppressed, disclosed or copied.

220. Electromagnetic emissions from a terminal represent an exposure because they:

A. affect noise pollution.
B. disrupt processor functions.
C. produce dangerous levels of electric current.
D. can be detected and displayed.

Answer: D

Emissions can be detected by sophisticated equipment and displayed, thus giving access to data to unauthorized persons. They should not cause disruption of CPUs or effect noise pollution.

221. The PRIMARY purpose of audit trails is to:

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

Answer: B

"Enabling audit trails helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system. The objective of enabling software to provide audit trails is not to improve system efficiency, since it often involves additional processing which may in fact reduce response time for users. Enabling audit trails does involve storage and thus occupies disk space. Choice D is also a valid reason
however, it is not the primary reason"

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

A. Inheritance
B. Dynamic warehousing
C. Encapsulation
D. Polymorphism

Answer: C

Encapsulation is a property of objects, which prevents accessing either properties or methods, that have not been previously defined as public. This means that any implementation of the behavior of an object

is not accessible. An object defines a communication interface with the exterior and only whatever belongs to that interface can be accessed.

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

A. encapsulation.
B. wrapping.
C. transform.
D. encryption.

Answer: A

Encapsulation or tunneling is a technique used to carry the traffic of one protocol over a network that does not support that protocol directly. The original packet is wrapped in another packet. The other choices are not security technique specific for VPNs.

224. Which of the following provides the GREATEST assurance of message authenticity?

A. The pre-hash code is derived mathematically from the message being sent.
B. The pre-hash code is encrypted using the sender's private key.
C. Encryption of the pre-hash code and the message using the secret key.
D. Sender attains the recipient's public key and verifies the authenticity of its digital certificate with a certificate authority.

Answer: B

Encrypting the pre-hash code using the sender's private key provides assurance of the authenticity of the message. Mathematically deriving the pre-hash code provides integrity to the message. Encrypting the pre-hash code and the message using the secret key provides confidentiality.

225. The BEST defense against network eavesdropping is:

A. encryption.
B. moving the defense perimeter outward.
C. reducing the amplitude of the communication signal.
D. masking the signal with noise.

Answer: A

Encryption is the best choice in this situation and generally protects information from eavesdroppers. Encrypted strings, with a discernible pattern, can be captured by a sniffer. This means that due care should be taken even with encryption. Moving the defense perimeter outward would entail additional cost as the security coverage would enlarge. Reducing the amplitude of the communication signal would result in attenuation of the signal and the recipient would not receive the information properly. Masking with noise would cause signal distortion and therefore distortion in the information received that is not desirable.

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

A. encryption.
B. callback modems.
C. message authentication.
D. dedicated leased lines.

Answer: A

Encryption of data is the most secure method. The other methods are less secure, with leased lines being possibly the least secure method.

227. Which of the following is the MOST effective technique for providing security during data transmission?

A. Communication log
B. Systems software log
C. Encryption
D. Standard protocol

Answer: C

Encryption provides security for data during transmission. The other choices do not provide protection during data transmission.

228. To develop a successful business continuity plan, end user involvement is critical during which of the following phases?

A. Business recovery strategy
B. Detailed plan development
C. Business impact analysis
D. Testing and maintenance

Answer: C

End user involvement is critical in the business impact analysis phase. During this phase the current operations of the business needs to be understood and the impact on the business of various disasters must be evaluated. End users are the appropriate persons to provide relevant information for these tasks. Inadequate end user involvement in this stage could result in inadequate understanding of business priorities and the plan not meeting the requirements of the organization.

229. An organization is experiencing a growing backlog of undeveloped applications. As part of a plan to eliminate this backlog, end-user computing with prototyping, supported by the acquisition of an interactive application generator system is being introduced. Which of the following areas is MOST critical to the ultimate success of this venture?

A. Data control
B. Systems analysis
C. Systems programming
D. Application programming

Answer: B

"End-user computing tools, such as prototyping systems and interactive application generator systems, handle many of the technical aspects of the system design process
however, end users are still required to have adequate skills to design a system efficiently. These skills are often attributable to systems analysts that understand efficient methods of data flow. Therefore, the end user should be familiar with systems analysis to make this venture successful."

230. In addition to the backup considerations for all systems, which of the following is an important consideration in providing backup for online systems?

A. Maintaining system software parameters
B. Ensuring periodic dumps of transaction logs
C. Ensuring grandfather-father-son file backups
D. Maintaining important data at an off-site location

Answer: B

Ensuring periodic dumps of transaction logs is the only safe way of preserving timely historical data. The volume of activity usually associated with an online system makes other more traditional methods of backup impractical.

231. The purpose for requiring source code escrow in a contractual agreement is to:

A. ensure the source code is available if the vendor ceases to exist.
B. permit customization of the software to meet specified business requirements.
C. review the source code for adequacy of controls.
D. ensure the vendor has complied with legal requirements.

Answer: A

Ensuring that source code is available if the vendor ceases to exist is the major reason for requiring source code escrow. Choices B, C and D are not applicable because source code escrow is not used for these purposes.

232. An IS auditor, in evaluating proposed biometric control devices reviews the false rejection rates (FRRs), false acceptance rates (FARs) and equal error rates (ERRs) of three different devices. The IS auditor should recommend acquiring the device having the:

A. least ERR.
B. most ERR.
C. least FRR but most FAR.
D. least FAR but most FRR.

Answer: A

Equal error rate is the percent of times the false rejection and acceptance are equal. The lower the overall measure, the more effective the biometric. Neither a higher false rejection rate nor false acceptance rate is desirable.

233. Which of the following is the MOST effective control over visitor access to a data center?

A. Visitors are escorted.
B. Visitor badges are required.
C. Visitors sign in.
D. Visitors are spot-checked by operators.

Answer: A

Escorting visitors will provide the best assurance that visitors have permission to access the data processing facility. Choices B and C are not reliable controls. Choice D is incorrect because visitors should be accompanied at all times while they are on the premises, not only when they are in the data processing facility.

234. When selecting software, which of the following business and technical issues is the MOST important to be considered?

A. Vendor reputation
B. Requirements of the organization
C. Cost factors
D. Installed base

Answer: B

Establishing the requirements of the organization is a task that should be completed early in the process. Cost factors are a part of the analysis in the evaluation of software alternatives. A vendor's reputation and the installed base become important only after the requirements are met.

235. Which of the following normally would be the MOST reliable evidence for an auditor?

A. A confirmation letter received from a third party verifying an account balance
B. Assurance from line management that an application is working as designed
C. Trend data obtained from World Wide Web (Internet) sources
D. Ratio analysis developed by the IS auditor from reports supplied by line management

Answer: A

Evidence obtained from independent third parties almost always is considered to be the most reliable. Answers B, C and D would not be considered as reliable.

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

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

Answer: D

Evidence obtained from outside sources is usually more reliable than that obtained from within the organization. Confirmation letters received from outside parties, such as those used to verify accounts receivable balances, are usually highly reliable. Testing performed by an auditor may not be reliable if the auditor did not have a good understanding of the technical area under review.

237. 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?

A. Differential reporting
B. False positive reporting
C. False negative reporting
D. Less detail reporting

Answer: C

False negative reporting on weaknesses means the control weaknesses in the network are not identified and hence may not be addressed, leaving the network vulnerable to attack. False positive is one in which the controls are in place, but are evaluated as weak, which should prompt a rechecking of the controls. Less detail reporting and differential reporting functions provided by these tools compare scan results over a period of time.

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

A. Copper wire
B. Twisted pair
C. Fiber-optic cables
D. Coaxial cables

Answer: C

Fiber-optic cables have proven to be more secure than the other media. Satellite transmission and copper wire can be violated with inexpensive equipment. Coaxial cable also can be violated more easily than other transmission media.

239. Confidential data residing on a PC is BEST protected by:

A. a password.
B. file encryption.
C. removable diskettes.
D. a key operated power source.

Answer: B

File encryption is the best means of protecting confidential data in a PC. A key-operated power source, password or removable diskettes will only restrict access, and the data will still be viewable using electronic eavesdropping techniques. Only encryption provides confidentiality. A password also may not be the best method of protection since passwords can be compromised. Removable diskettes do provide some security for information if they are locked away so only authorized individuals can gain access. However, if obtained by unauthorized individuals, information can be accessed easily. A key-operated power source can be bypassed by obtaining power from another source.

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

A. Unauthorized access from outside the organization
B. Unauthorized access from within the organization

C. A delay in Internet connectivity
D. A delay in downloading using file transfer protocol (FTP)

Answer: A

Firewalls are meant to prevent outsiders from gaining access to an organization's computer systems through the Internet gateway. They form a barrier with the outside world, but are not intended to address access by internal users, and are more likely to cause delays than address such concerns.

241. An IS auditor needs to link his/her microcomputer to a mainframe system that uses binary synchronous data communications with block data transmission. However, the IS auditor's microcomputer, as presently configured, is capable of only asynchronous ASCII character data communications. Which of the following must be added to the IS auditor's computer to enable it to communicate with the mainframe system?

A. Buffer capacity and parallel port
B. Network controller and buffer capacity
C. Parallel port and protocol conversion
D. Protocol conversion and buffer capability

Answer: D

For the IS auditor's microcomputer to communicate with the mainframe, the IS Auditor must use a protocol converter to convert the asynchronous and synchronous transmission. Additionally, the message must be spooled to the buffer to compensate for different rates of data flow.

242. Which of the following should concern an IS auditor when reviewing security in a client-server environment?

A. Data is protected by an encryption technique.
B. Diskless workstations prevent unauthorized access.
C. Ability of users to access and modify the database directly.
D. Disabling floppy drives on the users machines.

Answer: C

For the purpose of data security in a client-server environment, an IS auditor should be concerned with the users ability to access and modify a database directly. This could affect the integrity of the data in the database. Data protected by encryption aids in securing the data. Diskless workstations prevent copying of data into local disks and thus helps to maintain the integrity and confidentiality of data. Disabling floppy drives is a physical access control, which helps to maintain the confidentiality of data by preventing it from being copied onto a disk.

243. Transmitting redundant information with each character or frame to facilitate detection and correction of errors is called:

A. feedback error control.
B. block sum check.
C. forward error control.
D. cyclic redundancy check.

Answer: C

Forward error control involves transmitting additional redundant information with each character or frame to facilitate detection and correction of errors. In feedback error control, only enough additional information is transmitted so the receiver can identify that an error has occurred. Choices B and D are both error detection methods but not error correction methods. Block sum check is an extension of parity check wherein an additional set of parity bits is computed for a block of characters. A cyclic redundancy check is a technique wherein a single set of check digits is generated for each frame transmitted, based on the contents of the frame.

244. The MAJOR concern for an IS auditor when reviewing an organization's business process reengineering (BRP) efforts is:

A. cost overrun of the project.
B. employees resistance to change.
C. key controls may be removed from a business process.
D. lack of documentation of new processes.

Answer: C

From an IS audit point of view, the main concern would be that controls might be eliminated. All other choices are concerns in a business process reengineering project, but the major concern would be related to the adequacy of controls.

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

A. information assets are over protected.
B. a basic level of protection is applied regardless of asset value.
C. appropriate levels of protection are applied to information assets.
D. an equal proportion of resources are devoted to protecting all information assets.

Answer: C

Full risk assessment determines the level of protection most appropriate to a given level of risk, while the baseline approach merely applies a standard set of protection regardless of risk. There is a cost advantage in not over protecting information. However, an even bigger advantage is making sure that no information assets are over or under protected. The risk assessment approach will ensure an appropriate level of protection is applied commensurate with the level of risk and asset value, and therefore, considers asset value. The baseline approach allows more resources to be directed towards the assets at greater risk rather than equally directing resources to all assets.

246. Which of the following is a measure of the size of an information system based on the number and complexity of a system's inputs, outputs and files?

A. Program evaluation review technique (PERT)
B. Rapid application development (RAD)
C. Function point analysis (FPA)
D. Critical path method (CPM)

Answer: C

Function point analysis is a measure of the size of an information system based on the number and complexity of the inputs, outputs and files that a user sees and interacts with. Function points are used in a manner analogous to lines of code as a measure of software productivity, quality and other attributes. PERT is a network management technique used in both the planning and control of projects. RAD is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality. CPM is used by network management techniques, such as PERT, in computing a critical path.

247. Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

A. Function point analysis
B. PERT chart
C. Rapid application development
D. Object-oriented system development

Answer: B

Function point analysis is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries, logical internal file, etc. While this will help determine the size of individual activities, it will not assist in determining project duration since there are many over-lapping tasks. A PERT chart will help determine project duration once all the activities and the work involved in the activities are known. Rapid application development is a methodology that enables organizations to develop strategically important systems

faster while reducing development costs and maintaining quality, and object-oriented system development is the process of solution specification and modeling.

248. Functional acknowledgements are used:

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

Answer: A

Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and therefore can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

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

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

Answer: A

Functionality is the set of attributes that bears on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs. Choice B refers to portability, choice C refers to reliability and choice D refers to efficiency.

250. To identify the value of inventory that has been kept for more than eight weeks, an IS auditor would MOST likely use:

A. test data.
B. statistical sampling.
C. an integrated test facility.
D. generalized audit software.

Answer: D

Generalized audit software will facilitate reviewing the entire inventory file to look for those items that meet the selection criteria. Generalized audit software provides direct access to data and provides for features of computation, stratification, etc. Test data are used to verify programs, but will not confirm anything about the transactions in question. The use of statistical sampling methods are not intended to select specific conditions, but are to select on a random basis from a file. In this case the IS auditor would want to check all of the items that meet the criteria and not just a sample of them. An integrated test facility allows the IS auditor to test transactions through the production system.

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

A. Warm site
B. Mobile site
C. Hot site
D. Cold site

Answer: D

Generally a cold site is contracted for a longer period at a lower cost. Since it requires more time to make a cold site operational, it is used generally for noncritical applications. A warm site is generally available at a medium cost, requires less time to become operational and is suitable for sensitive operations. A mobile site is a vehicle ready with all necessary computer equipment and it can be moved to any cold or warm site depending upon the need. The need for a mobile site depends upon the scale of

operations and a hot site is contracted for a shorter time period at a higher cost and is better suited for recovery of vital and critical applications.

252. Which of the following is intended to detect the loss or duplication of input?

A. Hash totals
B. Check digits
C. Echo checks
D. Transaction codes

Answer: A

Hash totals are the result of totaling specified fields in a series of transactions or records. If a later summation does not result in the same number, then records have either been lost, entered or transmitted incorrectly, or duplicated.

253. A large chain of shops with 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?

A. Offsite storage of daily backups
B. Alternative standby processor onsite
C. Installation of duplex communication links
D. Alternative standby processor at another network node

Answer: D

Having an alternative standby processor at another network node would be the best. The unavailability of the central communications processor would disrupt all access to the banking network resulting in the disruption of operations for all of the shops. This could be caused by failure of equipment, power or communications. Offsite storage of backups would not help since EFT tends to be an online process and offsite storage will not replace the dysfunctional processor. The provision of an alternate processor onsite would be fine if it were an equipment problem, but would not help if the outage were caused by power, for example. Installation of duplex communication links would be most appropriate if it were only the communication link that failed.

254. An advantage of the use of hot sites as a backup alternative is that:

A. the costs associated with hot sites are low.
B. hot sites can be used for an extended amount of time.
C. hot sites can be made ready for operation within a short period of time.
D. they do not require that equipment and systems software be compatible with the primary site.

Answer: C

Hot sites can be made ready for operation normally within hours. However, the use of hot sites is expensive, should not be considered as a long-term solution and does require that equipment and systems software be compatible with the primary installation being backed up.

255. Which of the following is a role of an IS steering committee?

A. Initiate computer applications.
B. Ensure efficient use of data processing resources.
C. Prepare and monitor system implementation plans.
D. Review the performance of the systems department.

Answer: B

Ideally an IS steering committee should consist of members from all significant business areas in an organization. Their goal is to review and act upon all requests for new system needs in accordance with the corporate mission and objectives. To this end, it is the responsibility of the committee to ensure the efficient use of data processing resources, set the priorities, examine costs and provide support for various projects.

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

A. A cost-benefits analysis of methods for securing the applications
B. Identification of network applications to be externally accessed
C. Identification of vulnerabilities associated with network applications to be externally accessed
D. Creation of an applications traffic matrix showing protection methods

Answer: B

Identification of the applications required across the network should be identified first. After identification, depending on the physical location of these applications in the network and the network model, the person in-charge will be able to understand the need and possible ways of controlling access to these applications. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step. Having identified the applications, the next step is to identify vulnerabilities (weaknesses) associated with the network applications. The next step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

257. When developing a risk management program, the FIRST activity to be performed is a/an:

A. threats assessment.
B. classification of data.
C. inventory of assets.
D. criticality analysis.

Answer: C

Identification of the assets to be protected is the first step in the development of a risk management program. A listing of the threats that can affect the performance of these assets and criticality analysis are later steps in the process. Data classification is required for defining access controls, and in criticality analysis.

258. Birth date and marriage date items were switched while entering data. Which of the following data validation checks could detect this?

A. Logical relationship
B. Sequence
C. Reasonableness
D. Validity

Answer: A

If a particular condition is true, then one or more additional conditions or data input relationships may be required to be true and then the input may be considered as valid. The date of marriage has to follow date of birth plus a certain period. A logical relationship check would be helpful in detecting this data entry error. A sequence check would look for an ascending or descending series of entries. A reasonableness check is used to match input data to predetermined reasonable limits and a validity check would validate data in accordance with predetermined criteria.

259. If a database is restored using before-image dumps, where should the process be restarted following an interruption?

A. Before the last transaction
B. After the last transaction
C. The first transaction after the latest checkpoint
D. The last transaction before the latest checkpoint

Answer: A

If before images are used, the last transaction in the dump will not have updated the database prior to the dump being taken. The last transaction will not have updated the database and must be reprocessed. Program checkpoints are irrelevant in this situation.

260. Which of the following represents the GREATEST risk created by a reciprocal agreement for disaster recovery made between two companies?

A. Developments may result in hardware and software incompatibility.
B. Resources may not be available when needed.
C. The recovery plan cannot be tested.
D. The security infrastructures in each company may be different.

Answer: A

If one organization updates its hardware and software configuration, it may mean that it is no longer compatible with the systems of the other party in the agreement. This may mean that each company is unable to use the facilities at the other company to recover their processing following a disaster. Resources being unavailable when needed are an intrinsic risk in any reciprocal agreement, but this is a contractual matter and is not the greatest risk. The plan can be tested by paper-based walk-throughs and, possibly, by agreement between the companies. The difference in security infrastructures, while a risk, is not insurmountable.

261. 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?

A. Customers are widely dispersed geographically, but not the certificate authorities.
B. Customers can make their transactions from any computer or mobile device.
C. The certificate authority has several data processing subcenters to administrate certificates.
D. The organization is the owner of the certificate authority.

Answer: D

If the certificate authority belongs to the same organization, this would generate a conflict of interest. If a customer wanted to repudiate a transaction, he/she could allege that there exists an unlawful agreement between the parties generating the certificates, because of the shared interests. If a customer wanted to repudiate a transaction, he/she could believe that there exists a bribery between the parties to generate the certificates, as there exist shared interests. The other options are not weaknesses.

262. An IS auditor is assigned to help design the data security aspects of an application under development. Which of the following provides the MOST reasonable assurance that corporate assets are protected when the application is certified for production?

A. A review conducted by the internal auditor
B. A review conducted by the assigned IS auditor
C. Specifications by the user on the depth and content of the review
D. An independent review conducted by another equally experienced IS auditor

Answer: D

If the IS auditor assigned to the development process actually contributes to the design of the system, then true independence has been compromised. Therefore, to insure an independent review of the system, a different IS auditor should review the system prior to production or within a reasonable time frame after implementation.

263. Which of the following controls would BEST detect intrusion?

A. User ids and user privileges are granted through authorized procedures.
B. Automatic logoff is used when a workstation is inactive for a particular period of time.
C. Automatic logoff of the system after a specified number of unsuccessful attempts.
D. Unsuccessful logon attempts are monitored by the security administrator.

Answer: D

IIntrusion is detected by the active monitoring and review of unsuccessful logons. User ids and the granting of user privileges defines a policy, not a control. Automatic logoff is a method of preventing access on inactive terminals and is not a detective control. Unsuccessful attempts to log on is a method for preventing intrusion, not detecting.

264. A database administrator is responsible for:

A. maintaining the access security of data residing on the computers.
B. implementing database definition controls.
C. granting access rights to users.
D. defining system's data structure.

Answer: B

Implementing database definition controls is one of the primary functions of the database administrator. Maintaining access security of data and granting access rights to users is the responsibility of the data owner and the security administrator. Defining a system's data structure is the responsibility of the systems analyst.

265. In a data warehouse, data quality is achieved by:

A. cleansing.
B. restructuring.
C. source data credibility.
D. transformation.

Answer: C

In a data warehouse system the quality of data depends on the quality of the originating source. Choices A, B and D relate to the composition of a data warehouse and do not affect data quality. Restructuring, transformation and cleansing all relate to reorganization of existing data within the database.

266. Which of the following is the MOST important function to be performed by IS management when a service has been outsource?

A. Ensuring that invoices are paid to the provider
B. Participating in systems design with the provider
C. Renegotiating the provider's fees
D. Monitoring the outsourcing provider's performance

Answer: D

In an outsourcing environment, the company is dependent on the performance of the service provider. Therefore, it is critical the outsourcing provider's performance be monitored to ensure that services are delivered to the company as required. Payment of invoices is a finance function, which would be done per contractual requirements. Participating in systems design is a by-product of monitoring the outsourcing provider's performance, while renegotiating fees is usually a one-time activity.

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

A. Integrity
B. Availability
C. Completeness
D. Confidentiality

Answer: B

In case of a disruption in service, one of the key functions of network performance monitoring tools is to ensure that the information has remained unaltered. It is a function of the security monitoring to assure confidentiality by using such tools as encryption. However, the most important aspect of network performance is assuring the ongoing dependence on connectivity to run the business. Therefore, the characteristic that benefits the most from network monitoring is availability.

268. IS auditors, in performing detailed network assessments and access control reviews should FIRST:

A. determine the points of entry.
B. evaluate users access authorization.
C. assess users identification and authorization.
D. evaluate the domain-controlling server configuration.

Answer: A

In performing detailed network assessments and access control reviews IS auditors should first determine the points of entry to the system and accordingly review the points of entry for appropriate controls. Evaluation of user access authorization, assessment of user identification and authorization and evaluation of the domain-controlling server configuration are all implementation issues for appropriate controls for the points of entry.

269. While designing the business continuity plan (BCP) for an airline reservation system, the MOST appropriate method of data transfer/back up at an offsite location would be:

A. shadow file processing.
B. electronic vaulting.
C. hard-disk mirroring.
D. hot-site provisioning.

Answer: A

In shadow file processing exact duplicates of the files are maintained at the same site or at a remote site. The two files are processed concurrently. This is used for critical data files, such as airline booking systems. Electronic vaulting electronically transmits data either to direct access storage, an optical disc or any other storage medium. This is a method used by banks. Hard-disk mirroring provides redundancy in case the primary hard disk fails. All transactions and operations are done on two hard disks in the same server. A hot site is an alternate site ready to take over business operations within a few hours of any business interruption and is not a method for backing up data.

270. When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

A. There could be a question with regards to the legal jurisdiction.
B. Having a provider abroad will cause excesive costs in future audits.
C. The auditing process will be difficult because of the distances.
D. There could be different auditing norms.

Answer: A

In the funds transfer process, when the processing scheme is centralized in a different country, there could be legal issues of jurisdiction that might affect the right to perform a review in the other country. The other choices, though possible, are not as relevant as the issue of legal jurisdiction.

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

A. Router configuration and rules
B. Design of the internal network
C. Updates to the router system software
D. Audit testing and review techniques

Answer: A

Inadequate router configuration and rules would lead to an exposure to denial-of-service attacks. Choices B and C would be lesser contributors. Choice D is incorrect because audit testing and review techniques are applied after the fact.

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

A. include the finding in the final report because the IS auditor is responsible for an accurate report of all findings.
B. not include the finding in the final report because the audit report should include only unresolved findings.

C. not include the finding in the final report because corrective action can be verified by the IS auditor during the audit.
D. include the finding in the closing meeting for discussion purposes only.

Answer: A

Including the finding in the final report is a generally accepted audit practice. If an action is taken after the audit started and before it ended, the audit report should identify the finding and describe the corrective action taken. An audit report should reflect the situation, as it existed at the start of the audit. All corrective actions taken by the auditee should be reported in writing.

273. IS auditors who have participated in the development of an application system might have their independence impaired if they:

A. perform an application development review.
B. recommend control and other system enhancements.
C. perform an independent evaluation of the application after its implementation.
D. are involved actively in the design and implementation of the application system.

Answer: D

Independence may be impaired if the auditor becomes involved actively in the design and implementation of the application system. For example, if the auditor becomes a decision-making member of the project team, the auditor's ability to perform an independent application development review of the application system is impaired. The auditor may recommend control and other system enhancements, perform an application development review and perform an independent evaluation of the application after its implementation without impairing independence.

274. An IS auditor is assigned to perform a post implementation review of an application system. Which of the following situations may have impaired the independence of the IS auditor? The IS auditor:

A. implemented a specific control during the development of the application system.
B. designed an embedded audit module exclusively for auditing the application system.
C. participated as a member of the application system project team, but did not have operational responsibilities.
D.provided consulting advice concerning application system best practices.

Answer: A

Independence may be impaired if the IS auditor is, or has been, actively involved in the development, acquisition and implementation of the application system. Choices B and C are situations that do not impair the IS auditor's independence. Choice D is incorrect because the IS auditor's independence is not impaired by providing advice on known best practices.

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

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

Answer: D

Independence should be continually assessed by the auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests and prior job assignments and responsibilities. The fact that the employee has worked in IS for many years may not in itself ensure credibility. The audit department's needs should be defined and any candidate should be evaluated against those requirements. In addition, the length of service will not ensure technical competency, and evaluating an individual's qualifications based on the age of the individual is not a good criterion and is illegal in many parts of the world.

276. An IS auditor conducting an access controls 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:

A. exposure is greater since information is available to unauthorized users.
B. operating efficiency is enhanced since anyone can print any report, any time.
C. operating procedures are more effective since information is easily available.
D. user friendliness and flexibility is facilitated since there is a smooth flow of information among users.

Answer: A

Information in all its forms needs to be protected from unauthorized access. Unrestricted access to the report option results in an exposure. Efficiency and effectiveness are not relevant factors in this situation. Greater control over reports will not be accomplished since reports need not be in a printed form only. Information could be transmitted outside as electronic files without printing as print options allow for printing in an electronic form as well.

277. An IS auditor should be able to identify and evaluate various types of risks and their potential effects. Which of the following risks is associated with authorized program exits (trap doors)?

A. Inherent
B. Detection
C. Audit
D. Error

Answer: A

Inherent risk is the susceptibility of an area or process to an error that could be material. Exits out of an authorized program are an inherent risk as they provide a flexibility for inserting code to modify or add functionality. The exits (trap doors) also permit insertion of unauthorized code. Detection risk (choice B) is the risk that IS auditor's substantive procedures will not detect an error which could be material, indivually or in combination with other errors. Audit risk (choice C) is the risk of giving an incorrect audit opinion, while error risk (choice D) is the risk of errors occuring in the area being audited.

278. Passwords should be:

A. assigned by the security administrator.
B. changed every 30 days at the discretion of the user.
C. reused often to ensure the user does not forget the password.
D. displayed on the screen so that the user can ensure that it has been entered properly.

Answer: A

Initial password assignment should be done discretely by the security administrator. Passwords should be changed often (e.g., every 30 days), however, changing should not be voluntary. It should be required by the system. Systems should not permit previous passwords(s) to be used again. Old passwords may have been compromised and would thus permit unauthorized access. Passwords should not be displayed in any form.

279. Which of the following would not prevent the loss of an asset but would assist in recovery by transferring part of the risk to a third party?

A. Full system backups
B. Insurance
C. Testing
D. Business impact analysis

Answer: B

Insurance assists by involving a third party in sharing the risks. In case of the destruction of an asset, the third party would compensate for the loss based on the contract. This would assist in reinstating the asset to the pre-disaster condition. A business impact analysis (BIA) is the first step in developing a business continuity plan. This step would assist in the classification of assets based on risk and would not assist in either preventing a disaster or reinstating an asset to a pre-disaster condition. Backups would

assist in recovering a system in case of a disaster but do not necessarily involve a third party. Testing of the plan would help to ensure that the business continuity plan works as intended, but testing would not reinstate an asset to a pre-disaster condition.

280. A control for a company that wants to prevent virus-infected programs (or other type of unauthorized modified programs) would be to:

A. utilize integrity checkers.
B. verify program's lengths.
C. backup the source and object code.
D. implement segregation of duties.

Answer: A

Integrity checkers (such as the ones included in many antivirus programs or freeware, like tripwire) compute for each selected program some type of hash, checksum or cyclic redundancy check (CRC), then store this number in a database file. Before each execution of the program, the checker recomputes the hash or checksum and compares it to the value stored in the database. If the values do not match, the program is not executed thus detecting a possible virus or modified program. Verifying a progam's length is not practical, and some virus do not affect the length of infected programs. A backup of source and object code does not help detect a modified program. Segregation of duties is useful to minimize risk, however, it does not detect a modified program.

281. Which of the following is the MOST effective type of antivirus software?

A. Scanners
B. Active monitors
C. Integrity checkers
D. Vaccines

Answer: C

"Integrity checkers compute a binary number on a known virus-free program that is then stored in a database file. The number is called a cyclical redundancy check (CRC). When that program is called to execute, the checker computes the CRC on the program about to be executed and compares it to the number in the database. A match means no infection
a mismatch means that a change in the program has occurred. A change in the program could mean a virus. Scanners look for sequences of bits called signatures that are typical of virus programs. They examine memory, disk boot sectors, executables and command files for bit patterns that match a known virus. Scanners, therefore, need to be updated periodically to remain effective. Active monitors interpret DOS and ROM basic input-output system (BIOS) calls, looking for virus-like actions. Active monitors can be annoying because they cannot distinguish between a user request and a program or virus request. As a result, users are asked to confirm actions like formatting a disk or deleting a file or set of files. Vaccines are known to be good antivirus software. However, they also need to be updated periodically to remain effective."

282. Testing the connection of two or more system components that pass information from one area to another is:

A. pilot testing.
B. parallel testing
C. interface testing.
D. regression testing.

Answer: C

Interface testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. Pilot testing is a preliminary test that focuses on specific and predetermined aspects of a system and is not meant to replace other methods. Parallel testing is the process of feeding test data into two systems-the modified system and an alternative system-and comparing the results. Regression testing is the process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing is the same as the data used in the original test.

283. Which of the following are data file controls?

A. Internal and external labeling
B. Limit check and logical relationship checks
C. Total items and hash totals
D. Report distribution procedures

Answer: A

Internal and external labeling are controls to ensure that only authorized processing affects stored data. Limit checks and logical relationship checks are validation and editing controls. Total items and hash totals are batch controls and report distribution procedures are output controls.

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

A. Traffic analysis
B. Masquerading
C. Denial of service
D. E-mail spoofing

Answer: A

Internet security threats/vulnerabilities are divided into passive and active attacks. Examples of passive attacks are: network analysis, eavesdropping and traffic analysis. Active attacks include: brute-force attack, masquerading, packet replay, message modification, unauthorized access through the Internet or web-based services, denial of service, dial-in penetration attacks, e-mail bombing and spamming, and e-mail spoofing.

285. Which of the following Internet security threats could compromise integrity?

A. Theft of data from the client
B. Exposure of network configuration information
C. A trojan horse browser
D. Eavesdropping on the net

Answer: C

Internet security threats/vulnerabilities to integrity include a trojan horse found in client browser software, which could modify user data, memory and messages. The other options compromise confidentiality.

286. IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that:

A. a substantive test would be too costly.
B. the control environment is poor.
C. inherent risk is low.
D. control risks are within the acceptable limits.

Answer: D

IS auditors perform tests of controls (compliance testing) to assess whether control risks are within acceptable limits. The results of the compliance testing would influence the IS auditor's decisions as to the extent of tests of balance (substantive testing). If compliance testing confirms that the control risks are within an acceptable level, then the extent of substantive testing would be reduced. During the testing phase of an audit, an IS auditor does not know whether the controls identified operate effectively. Tests of controls, therefore, evaluate whether specific, material controls are, in fact reliable. Performing test of controls may conclude that the control environment is poor, but it is not the objective of compliance testing. Inherent risks cannot be determined by performing a test of controls.

287. The IS department of an organization wants to ensure that the computer files, used in the information processing facility, are backed up adequately to allow for proper recovery. This is a/an:

A. control procedure.

B. control objective.
C. corrective control.
D. operational control.

Answer: B

IS control objectives specify the minimum set of controls to ensure efficiency and effectiveness in the operations and functions within an organization. Control procedures are developed to provide reasonable assurance that specific objectives will be achieved. A corrective control is a category of controls, which aims to minimizing the threat and/or remedy problems that were not prevented or were not initially detected. Operational controls address the day-to-day operational functions and activities, and aid in ensuring that the operations are meeting the desired business objectives.

288. Which of the following reports should an IS auditor use to check compliance with a service level agreement (SLA) requirement for uptime?

A. Utilization reports
B. Hardware error reports
C. System logs
D. Availability reports

Answer: D

IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes. Utilization reports document the use of computer equipment, and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating correction action. System logs are a recording of the system's activities.

289. Various standards have emerged to assist IS organizations in achieving an operational environment that is predictable, measurable and repeatable. The standard that provides the definition of the characteristics and the associated quality evaluation process to be used when specifying the requirements for and evaluating the quality of software products throughout their life cycle is:

A. ISO 9001.
B. ISO 9002.
C. ISO 9126.
D. ISO 9003.

Answer: C

ISO 9126 focuses on the end result of good software processes, i.e., the quality of the actual software product. ISO 9001 contains guidelines about design, development, production, installation or servicing. ISO 9002 contains guidelines about production, installation or servicing, and ISO 9003 contains guidelines for final inspection and testing.

290. To help mitigate the effects of a denial of service attack, which mechanism can an Internet service provider (ISP) use to identify Internet protocol (IP) packets from unauthorized sources?

A. Inbound traffic filtering
B. Rate limiting
C. Reverse address lookup
D. Network performance monitoring

Answer: A

ISPs serve user organizations with pre-assigned IP addresses. Inbound traffic filtering can filter out IP packets that do not conform to the pre-assigned IP address range. Rate limiting involves limiting the occurrences of certain types of TCP/IP packets according to predefined specifications. It is used to identify excess packets. Reverse address lookup determines if the source address is an IP packet of the true address of the computer (host) that is actually sending the packet. It would identify address substitution, but would not initially identify that it was an unauthorized source. Network performance monitoring is a way to monitor system performance for potential intrusions on a real-time basis. It could help identify unusual traffic volumes.

291. An organization is moving its application maintenance in-house from an outside source. Which of the following should be the main concern of an IS auditor?

A. Regression testing
B. Job scheduling
C. User manuals
D. Change control procedures

Answer: D

It is essential for the maintenance and control of software that change control procedures be in place. Regression testing is done after changes are made to the software, and since the software already is being used, the job schedule must be in place and may be reviewed later. This change does not affect user manuals and any associated risks.

292. The phases and deliverables of a systems development life cycle (SDLC) project should be determined:

A. during the initial planning stages of the project.
B. after early planning has been completed, but before work has begun.
C. through out the work stages based on risks and exposures.
D. only after all risks and exposures have been identified and the IS auditor has recommended appropriate controls.

Answer: A

It is extremely important that the project be planned properly and that the specific phases and deliverables be identified during the early stages of the project.

293. An IS auditor performing a review of the IS department discovers that formal project approval procedures do not exist. In the absence of these procedures the IS manager has been arbitrarily approving projects that can be completed in a short duration and referring other more complicated projects to higher levels of management for approval. The IS auditor should recommend as a FIRST course of action that:

A. users participate in the review and approval process.
B. formal approval procedures be adopted and documented.
C. projects be referred to appropriate levels of management for approval.
D. the IS manager's job description be changed to include approval authority.

Answer: B

It is imperative that formal written approval procedures be established to set accountability. This is true of both the IS manager and higher levels of management. Choices A, C and D would be subsequent recommendations once authority has been established.

294. In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, an IS auditor should:

A. identify and assess the risk assessment process used by management.
B. identify information assets and the underlying systems.
C. disclose the threats and impacts to management.
D. identify and evaluate the existing controls.

Answer: D

It is important for an IS auditor to identify and evaluate the existing controls and security once the potential threats and possible impacts are identified. Upon completion of an audit an IS auditor should describe and discuss with management the threats and potential impacts on the assets.

295. Disaster recovery planning for a company's computer system usually focuses on:

A. operations turnover procedures.

B. strategic long-range planning.
C. the probability that a disaster will occur.
D. alternative procedures to process transactions.

Answer: D

It is important that disaster recovery identify alternative processes that can be put in place while the system is not available.

296. During which phase of a system development process should an IS auditor first raise the issue of application controls?

A. Construction
B. System design
C. Acceptance testing
D. Functional specification

Answer: D

It is important that IS auditors raise control concerns as early as possible. Frequently, the requirement for controls is not clearly specific when developing the functional specifications. The IS auditor should ensure that the business areas specify their requirement for control at that stage. The construction phase of the project is often too late for the identification of the controls, since this may require that changes be made in the design. Controls should be designed in at the system design stage, but the types of controls should have been identified as part of the functional specification. The acceptance testing stage is too late to identify controls, since this can require major changes to the system.

297. When reviewing a system development project at the project initiation stage, an IS auditor finds that the project team is following the organization's quality manual. To meet critical deadlines the project team proposes to fast track the validation and verification processes, commencing some elements before the previous deliverable is signed off. Under these circumstances, the IS auditor would MOST likely:

A. report this as a critical finding to senior management.
B. accept that different quality processes can be adopted for each project.
C. report to IS management the team's failure to follow quality procedures.
D. report the risks associated with fast tracking to the project steering committee.

Answer: D

It is important that quality processes are appropriate to individual projects. Attempts to apply inappropriate processes will often find their abandonment under pressure. A fast-tracking process is an acceptable option under certain circumstances. However, it is important that the project steering committee is informed of the risks associated with this (i.e., possibility of rework if changes are required).

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

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

Answer: A

It is important that there be an offsite storage location for IS files and that it be in a location not subject to the same risks as the primary data center. The other choices are all issues that must be considered when establishing the offsite location, but they are not as critical as the location selection.

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

A. central processing site after running the application system.
B. central processing site during the running of the application system.
C. remote processing site after transmission to the central processing site.

D. remote processing site prior to transmission of the data to the central processing site.

Answer: D

It is important the data entered from a remote site be edited and validated prior to transmission to the central processing site.

300. An IS steering committee should:

A. include a mix of members from different departments and staff levels.
B. ensure that IS security policies and procedures have been executed properly.
C. have formal terms of reference and maintain minutes of its meetings.
D. be briefed about new trends and products at each meeting by a vendor.

Answer: C

It is important to keep detailed steering committee minutes to document the decisions and activities of the IS steering committee, and the board of directors should be informed on a timely basis. Choice A is incorrect because only senior management, or high staff levels should be members of this committee because of its strategic mission. Choice B is not a responsibility of this committee but the responsibility of the security administrator. Choice D is incorrect because a vendor should be invited to meetings only when appropriate.

301. The implementation of cost-effective controls in an automated system is ultimately the responsibility of the:

A. system administrator.
B. quality assurance function.
C. business unit management.
D. chief of internal audit.

Answer: C

It is the business unit management's responsibility to implement cost effective controls in an automated system. They are the best group in an organization to know which information assets need to be secured in terms of availability, confidentiality and integrity. System administrators take care of services related to the system requirements of the user management group. The quality assurance function addresses the overall quality of the systems. The audit group will assess or examine the compliance level of the controls with written policies, procedures or practices.

302. Which of the following alternative business recovery strategies would be LEAST appropriate for an organization with a large database and online communications network environment?

A. Hot site
B. Cold site
C. Reciprocal agreement
D. Dual information processing facilities

Answer: C

It is unlikely that reciprocal agreements could be made to accommodate sophisticated environments, i.e., databases with large communications networks. Even if a compatible alternate facility could be located, it would be unlikely that there would be sufficient capacity available to accommodate foreign systems and provide the necessary security and integrity. Further, a cold-site arrangement could be appropriate, if plans to convert the cold site to a hot site could be executed rapidly enough to accommodate critical processing.

303. When a new system is to be implemented within a short time frame, it is MOST important to:

A. finish writing user manuals.
B. perform user acceptance testing.
C. add last-minute enhancements to functionalities.
D. ensure that code has been documented and reviewed.

Answer: B

It would be most important to complete the user acceptance testing so as to ensure that the system, which is to be implemented is working correctly. The completion of the user manuals is similar to the performance of code reviews. If time is tight, the last thing one would want to do is add another enhancement. It would be necessary to freeze the code and complete the testing, then make any other changes as future enhancements. It would be appropriate to have the code documented and reviewed, but unless the acceptance testing is completed, there is no guarantee that the system will work correctly and meet user requirements.

304. The corporate office of a company having branches worldwide, developed a control self-assessment program (CSA) for all its offices. Which of the following is the MOST important requirement for a successful CSA?

A. Skills of the workshop facilitator
B. Simplicity of the questionnaire
C. Support from the audit department
D. Involvement of line managers

Answer: D

Key to the success of a control self-assessment program is the support and involvement of the management and staff responsible for the process being assessed. All other options are essential for CSA to be successful, however in the absence of active involvement from those responsible, the other choices will not result in a successful CSA.

305. To make an electronic funds transfer (EFT), one employee enters the amount field and another employee reenters the same data again, before the money is transferred. The control adopted by the organization in this case is:

A. sequence check.
B. key verification.
C. check digit.
D. completeness check.

Answer: B

Key verification is a process in which keying-in is repeated by a separate individual using a machine that compares the original entry to the repeated entry. Sequence check refers to the continuity in serial numbers within the number range on documents. A check digit is a numeric value that has been calculated mathematically and added to data to ensure that the original data have not been altered or an incorrect but valid value substituted. Completeness checks ensure that all the characters required for a field have been input.

306. Which of the following data entry controls provides the GREATEST assurance that the data is entered correctly?

A. Using key verification
B. Segregating the data entry function from data entry verification
C. Maintaining a log/record detailing the time, date, employee's initials/user id and progress of various data preparation and verification tasks
D. Adding check digits

Answer: A

Key verification or one-to-one verification will yield the highest degree of confidence that data entered is error free. However, this could be impractical for large amounts of data. The segregation of the data entry function from data entry verification is an additional data entry control but does not address accuracy. Maintaining a log/record detailing the time, date, employee's initials/user ID and progress of various data preparation and verification tasks, provides an audit trail. A check digit is added to data to ensure that original data have not been altered. If a check digit is wrongly keyed, this would lead to accepting incorrect data but would only apply to those data elements having a check digit.

307. The most common reason for the failure of information systems to meet the needs of users is that:

A. user needs are constantly changing.
B. the growth of user requirements was forecast inaccurately.
C. the hardware system limits the number of concurrent users.
D. user participation in defining the system's requirements was inadequate.

Answer: D

Lack of adequate user involvement, especially in the systems requirements phase, will usually result in a system that does not address the needs of the user fully or adequately. Only users can define what their needs are and, therefore, what the system should accomplish.

308. LANs:

A. protect against virus infection.
B. protect against improper disclosure of data.
C. provide program integrity from unauthorized changes.
D. provide central storage for a group of users.

Answer: D

LANs facilitate the storage and retrieval of programs and data used by a group of people. They do not facilitate or provide protection against the other items listed in this question.

309. A PING command is used to measure:

A. attenuation.
B. throughput.
C. delay distortion.
D. latency.

Answer: D

"Latency, which is measured using a &quot
Ping&quot
command, represents the delay that a message/packet will have in traveling from source to destination. A decrease in amplitude as a signal propagates through a transmission medium is called attenuation. Throughput, which is the quantity of work per unit of time, is measured in bytes per second. Delay distortion represents delay in transmission because the rate of propagation of a signal along a transmission line varies with the frequency."

310. Which of the following exposures could be caused by a line-grabbing technique?

A. Unauthorized data access
B. Excessive CPU cycle usage
C. Lockout of terminal polling
D. Multiplexor control dysfunction

Answer: A

Line grabbing will enable eavesdropping, thus allowing unauthorized data access. It will not necessarily cause multiplexor dysfunction, excessive CPU usage or lockout of terminal polling.

311. A debugging tool, which reports on the sequence of steps executed by a program, is called a/an:

A. output analyzer.
B. memory dump.
C. compiler.
D. logic path monitor.

Answer: D

Logic path monitors report on the sequence of steps executed by a program. This provides the programmer with clues to logic errors, if any, in the program. An output analyzer checks the results of a

program for accuracy by comparing the expected results with the actual results. A memory dump provides a picture of the content of a computer's internal memory at any point of time, often when the program aborted, thus providing information on inconsistencies in data or parameter values. Though compilers have some potential to provide feedback to a programmer, they are not generally considered a debugging tool.

312. The BEST overall quantitative measure of the performance of biometric control devices is:

A. false rejection rate.
B. false acceptance rate.
C. equal error rate.
D. estimated error rate.

Answer: C

Low equal error rate (EER) is a combination of the low false rejection rate and the low false acceptance rate. EER, expressed as a percentage, is a measure of the number of times that the false rejection and false acceptance are equal. A low EER is the measure of the more effective biometrics control device. Low false rejection rates or low false acceptance rates alone do not measure the efficiency of the device. Estimated error rate is non-existing and hence irrelevant.

313. Which of the following would be the LEAST important aspect of a business continuity plan?

A. Redundant facilities
B. Relocation procedures
C. Adequate insurance coverage
D. Current and available business continuity manual

Answer: C

Maintaining adequate insurance coverage is important to the overall financial recovery of the organization, but it is not as important as providing facilities for processing recovery. The underlying purpose of business continuity planning is the resumption of business operations. As such, business recovery plans include procedures developed to accommodate systems, user and network recovery strategies.

314. Which of the following tasks is normally performed by a clerk in the control group?

A. Maintenance of an error log
B. Authorization of transactions
C. Control of noninformation systems assets
D. Origination of changes to master files

Answer: A

Maintaining an error log is the only task identified that a control group clerk normally would perform.

315. Which of the following is the MOST important objective of data protection?

A. Identifying persons who need access to information
B. Ensuring the integrity of information
C. Denying or authorizing access to the IS system
D. Monitoring logical accesses

Answer: B

Maintaining data integrity is the most important objective of data security. This is a necessity if an organization is to continue as a viable and successful enterprise. The other choices are important techniques for achieving the objective of data integrity.

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

A. security administrator.

B. systems administrator.
C. data and systems owners.
D. systems operations group.

Answer: C

Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.

317. Which of the following would be considered a business risk?

A. Former employees
B. Part-time and temporary personnel
C. Loss of competitive edge
D. Hackers

Answer: C

Many organizations, especially service firms such as banks, savings and loans and investment firms, need credibility and public trust to maintain a competitive edge. A security violation can severely damage this credibility, resulting in the loss of business and prestige. Loss of credibility is a risk. The other choices are threats. Former employees, who left on unfavorable terms, are potential logical or physical access violators. Part-time and temporary personnel often have a great deal of physical access and may well be competent in computing. Hackers are typically attempting to test the limits of access restrictions to prove their ability to overcome the obstacles. Although they usually do not access a computer with the intent of destruction, this is quite often the result.

318. An independent software program that connects two otherwise separate applications sharing computing resources across heterogeneous technologies is known as:

A. middleware.
B. firmware.
C. application software.
D. embedded systems.

Answer: A

Middleware is independent software that connects two otherwise separate applications sharing computing resources across heterogeneous technologies. Firmware is software (programs or data) that has been written onto read-only memory (ROM). It is a memory chip with embedded program code that holds its content when power is turned off. Firmware is a combination of software and hardware. Application software are programs that addresses an organization's processes and functions as opposed to system software which enables the computer to function. Embedded systems are built-in modules for a specific purpose, for example SCARF.

319. The interface that allows access to lower or higher level network services is called:

A. firmware.
B. middleware.
C. X.25 interface.
D. utilities.

Answer: B

Middleware, a class of software employed by client server applications, provides services, such as, identification, authentication, directories and security. It facilitates client-server connections over the network and allows client applications to access and update remote databases and mainframe files. Firmware consists of memory chips with embedded program code, that hold their content when the power is turned off. X.25 interface is the interface between data terminal equipment and data circuit terminating equipment for terminals operating in the packet mode on some public data networks.

Utilities are system software used to perform system maintenance and routines that are required during normal processing, such as sorting or backup.

320. Which of the following would an IS auditor place LEAST reliance on when determining management's effectiveness in communicating information systems policies to appropriate personnel?

A. Interviews with user and IS personnel
B. Minutes of IS steering committee meetings
C. User department systems and procedures manuals
D.Information processing facilities operations and procedures manuals

Answer: B

Minutes of IS steering committee meetings are not objective measures of the effectiveness of management. They generally represent the views of management, not staff, and thus may not indicate how effective policies have been communicated to appropriate personnel.

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

A. Daily backup
B. Offsite storage
C. Mirroring
D. Periodic testing

Answer: C

Mirroring of critical elements is a tool that facilitates immediate recoverability. Daily backup implies that it is reasonable for restoration to take place within a number of hours but not immediately. Offsite storage and periodic testing of systems do not of themselves support continuous availability.

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

A. The recipient uses his/her private key to decrypt the secret key.
B. The encrypted pre-hash code and the message are encrypted using a secret key.
C. The encrypted pre-hash code is derived mathematically from the message to be sent.
D. The recipient uses the sender's public key, verified with a certificate authority, to decrypt the pre-hash code.

Answer: D

Most encrypted transactions today use a combination of private keys, public keys, secret keys, hash functions and digital certificates to achieve confidentiality, message integrity and nonrepudiation by either sender or recipient. The recipient uses the sender's public key to decrypt the pre-hash code into a post-hash code which when equaling the pre-hash code verifies the identity of the sender and that the message has not been changed in route and would provide the greatest assurance. Each sender and recipient has a private key, known only to him/her and a public key, which can be known by anyone. Each encryption/decryption process requires at least one public key and one private key and both must be from the same party. A single secret key is used to encrypt the message, because secret key encryption requires less processing power than using public and private keys. A digital certificate, signed by a certificate authority, validates senders' and recipients' public keys.

323. Naming conventions for system resources are important for access control because they:

A. ensure that resource names are not ambiguous.
B. reduce the number of rules required to adequately protect resources.
C. ensure that user access to resources is clearly and uniquely identified.
D. ensure that internationally recognized names are used to protect resources.

Answer: B

Naming conventions for system resources are important for efficient administration of security controls. The conventions can be structured so that resources beginning with the same high-level qualifier can be governed by one or more generic rules. This reduces the number of rules required to adequately protect

resources, which in turn facilitates security administration and maintenance efforts. Reducing the number of rules required to protect resources allows for the grouping of resources and files by application, which makes it easier to provide access. Ensuring that resource names are not ambiguous can not be achieved through the use of naming conventions. Ensuring the clear and unique identification of user access to resources is handled by access control rules, not naming conventions. Internationally recognized names are not required to control access to resources. It tends to be based on how each organization wants to identify its resources.

324. An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

A. Availability of online network documentation
B. Support of terminal access to remote hosts
C. Handling file transfer between hosts and inter-user communications
D. Performance management, audit and control

Answer: A

Network operating system user features include online availability of network documentation. Other features would be user access to various resources of network hosts, user authorization to access particular resources and the network and host computers to be used without special user actions or commands. Choices B, C and D are examples of network operating systems functions among which the following are included: supporting terminal access to remote hosts, handling file transfer between hosts, and inter-user communications.

325. The review of router access control lists should be conducted during a/an:

A. environmental review.
B. network security review.
C. business continuity review.
D. data integrity review.

Answer: B

Network security reviews include reviewing router access control lists, port scanning, internal and external connections to the system, etc. Environmental reviews, business continuity reviews and data integrity reviews do not require a review of the router access control lists.

326. Neural networks are effective in detecting fraud because they can:

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

Answer: C

Neural networks can be used to attack problems that require consideration of numerous input variables, They are capable of capturing relationships and patterns often missed by other statistical methods. Neural networks will not discover new trends. They are inherently nonlinear and make no assumption about the shape of any curve relating variables to the output. Neural networks will not work well at solving problems for which sufficiently large and general sets of training data are not obtainable.

327. A manufacturer has been purchasing materials and supplies for its business through an e-commerce application. Which of the following should this manufacturer rely on to prove that the transactions were actually made?

A. Reputation
B. Authentication
C. Encryption
D. Nonrepudiation

Answer: D

Nonrepudiation may ensure that a transaction is enforceable. It involves creating proof of the origin or delivery of data to protect the sender against false denial by the recipient of the data's receipt, or vice versa. Choice A is incorrect because the company's reputation would not, of itself, prove a deal was made via the Internet. Choice B is not correct as authentication controls are necessary to establish the identification of all parties to a communication. Choice C is incorrect since encryption may protect the data transmitted over the Internet, but may not prove that the transactions were made.

328. Which of the following message services provides the strongest protection that a specific action has occurred?

A. Proof of delivery
B. Nonrepudiation
C. Proof of submission
D. Message origin authentication

Answer: B

Nonrepudiation services provide evidence that a specific action occurred. Nonrepudiation services are similar to their weaker proof counterparts (i.e., proof of submission, proof of delivery, and message origin authentication), however, nonrepudiation provides stronger protection because the proof can be demonstrated to a third party. Digital signatures are used to provide nonrepudiation. Message origination authentication will only confirm the source of the message and does not confirm the specific action that has been completed.

329. The database administrator has recently informed you of the decision to disable certain normalization controls in the database management system (DBMS) software to provide users with increased query performance. This will MOST likely increase the risk of:

A. loss of audit trails.
B. redundancy of data.
C. loss of data integrity.
D. unauthorized access to data.

Answer: B

Normalization is the removal of redundant data elements from the database structure. Disabling features of normalization in relational databases will increase the likelihood of data redundancy. Audit trails are a feature of DBMS software that can be lost by not enabling them. These are not connected to normalization controls. The integrity of data is not affected directly by disabling normalization controls. Access to data is set through defining user rights and controlling access to information, and is not affected by normalization controls.

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

A. IS department.
B. security committee.
C. security administrator.
D. board of directors.

Answer: D

Normally the designing of an information systems security policy is the responsibility of top management or the board of directors. The IS department is responsible for the execution of the policy, having no authority in framing the policy. The security committee also functions within the broad security policy framed by the board of directors. The security administrator is responsible for implementing, monitoring and enforcing the security rules that management has established and authorized.

331. Which of the following should be of MOST concern to an IS auditor?

A. Lack of reporting of a successful attack on the network
B. Failure to notify police of an attempted intrusion
C. Lack of periodic examination of access rights
D. Lack of notification to the public of an intrusion

Answer: A

Not reporting an intrusion is equivalent to an IS auditor hiding a malicious intrusion, which would be a professional mistake. Although notification to the police may be required and the lack of a periodic examination of access rights might be a concern, they do not represent as big a concern as the failure to report the attack. Reporting to the public is not a requirement and is dependent on the organization's desire or lack thereof to make the intrusion known.

332. Which of the following audit techniques would an IS auditor place the MOST reliance on when determining whether an employee practices good preventive and detective security measures?

A. Observation
B. Detail testing
C. Compliance testing
D. Risk assessment

Answer: A

Observation is considered to be the best test to ensure that an employee understands and practices good preventive and detective security.

333. Which of the following is MOST important to have provided for in a disaster recovery plan?

A. Backup of compiled object programs
B. Reciprocal processing agreement
C. Phone contact list
D. Supply of special forms

Answer: A

Of the choices, a backup of compiled object programs is the most important in a successful recovery. A reciprocal processing agreement is not as important, because alternative equipment can be found after a disaster occurs. A phone contact list may aid in the immediate aftermath, as would an accessible supply of special forms, but neither is as important as having access to required programs.

334. An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:

A. hardware configuration.
B. access control software.
C. ownership of intellectual property.
D. application development methodology.

Answer: C

Of the choices, the hardware and access control software generally is irrelevant as long as the functionality, availability and security can be affected, which would be a specific contractual obligation. Similarly, the development methodology should be of no real concern. The contract must, however, specify who owns the intellectual property (i.e., information being processed, application programs). Ownership of intellectual property will have a significant cost and is a key aspect to be defined in an outsourcing contract.

335. An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

A. reverse engineering.
B. prototyping.
C. software reuse.
D. reengineering.

Answer: D

Old (legacy) systems that have been corrected, adapted and enhanced extensively require reengineering to continue to be maintainable. Reengineering is a rebuilding activity to incorporate new technologies into existing systems. Using program language statements, reverse engineering involves reversing a

program's machine code into the source code in which it was written to identify malicious content in a program such as a virus, or to adapt a program written for use with one processor for use with a differently designed processor. Prototyping is development of a system through controlled trial and error. Software reuse is the process of planning, analyzing and using previously developed software components. The reusable components are integrated into the current software product systematically.

336. Which of the following is the FIRST step in a business process reengineering (BPR) project?

A. Defining the areas to be reviewed
B. Developing a project plan
C. Understanding the process under review
D. Reengineering and streamlining the process under review

Answer: A

On the basis of the evaluation of the entire business process, correctly defining the areas to be reviewed is the first step in a BPR project. On the basis of the definition of the areas to be reviewed, the project plan is developed. Understanding the process under review is important, but the subject of the review must be defined first. Thereafter, the process can be reengineered, streamlined, implemented and monitored for continuous improvement.

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

A. facilitate the ability to reuse modules.
B. improve system performance.
C. enhance control effectiveness.
D. speed up the system development life cycle.

Answer: A

One of the major benefits of object-oriented design and development is the ability to reuse modules. The other options do not normally benefit from the object-oriented technique.

338. A disaster recovery plan (DRP) for an organization should:

A. reduce the length of the recovery time and the cost of recovery.
B. increase the length of the recovery time and the cost of recovery.
C. reduce the duration of the recovery time and increase the cost of recovery.
D. not affect the recovery time nor the cost of recovery.

Answer: A

One of the objectives of a DRP is to reduce both the duration and cost of recovering from a disaster. DRP would increase the cost of operations before and after the disaster occurs, but should reduce the time to return to normal operations and the cost that could result from a disaster.

339. Which of the following would be of MOST concern to an IS auditor reviewing a VPN implementation? Computers on the network that are located:

A. on the enterprise's facilities.
B. at the backup site.
C. in employees' homes.
D. at the enterprise's remote offices.

Answer: C

One risk of a VPN implementation is the chance of allowing high-risk computers onto the enterprise's network. All machines that are allowed onto the virtual network should be subject to the same security policy. Home computers are least subject to the corporate security policies and hence are high-risk computers. Once a computer is hacked and "owned", any network that trusts that computer is at risk. Implementation and adherence to corporate security policy is easier when all computers on the network are on the enterprise's campus. Internally to an enterprise's physical network, there should be security policies in place to detect and halt an outside attack that uses an internal machine as a staging platform. Computers at the back up site are subject to the corporate security policy. Hence, not high-risk

computers. Computers on the network that are at the enterprise's remote offices, perhaps with different IS and security employees who have different ideas about security are more risky than choices A and B, but obviously less risky than home computers.

340. Which of the following reports is a measure of telecommunication transmissions and determines whether transmissions are completed accurately?

A. Online monitor reports
B. Downtime reports
C. Help desk reports
D. Response time reports

Answer: A

"Online monitors measure telecommunication transmissions and determine whether transmissions are completed accurately. Downtime reports track the availability of telecommunication lines and circuits help desk reports handle problems occurring in the normal course of operations and response time reports identify the time it takes for a command entered at a terminal to be answered by the computer."

341. Which of the following development methods uses a prototype that can be updated continually to meet changing user or business requirements?

A. Data-oriented development (DOD)
B. Object-oriented development (OOD)
C. Business process reengineering (BPR)
D. Rapid application development (RAD)

Answer: D

Only RAD uses prototyping as its core development tool. OOD and DOD use continuously developing models, and BPR attempts to convert an existing business process rather than make dynamic changes.

342. Which of the following procedures would BEST determine whether adequate recovery/restart procedures exist?

A. Reviewing program code
B. Reviewing operations documentation
C. Turning off the UPS, then the power
D. Reviewing program documentation

Answer: B

Operations documentation should contain recovery/restart procedures, so operations can return to normal processing in a timely manner. Turning off the UPS and then turning off the power might create a situation for recovery and restart, but the negative effect on operations would prove this method to be undesirable. The review of program code and documentation generally does not provide evidence regarding recovery/restart procedures.

343. Which of the following imaging technologies captures handwriting from a preprinted form and converts it into an electronic format?

A. Magnetic ink character recognition (MICR)
B. Intelligent voice recognition (IVR)
C. Bar code recognition (BCR)
D. Optical character recognition (OCR)

Answer: D

Optical character recognition (choice D) is used for capturing handwritten data from forms and converting the data to an electronic format. MICR is a specialized ink used on checks (cheques) for the identification of the instrument, and it is used in reader sorter units present in bank clearinghouses. Intelligent voice recognition is not an imaging technology and bar code readers read the bar codes which identify a specific item (product).

344. A probable advantage to an organization that has outsourced its data processing services is that:

A. needed IS expertise can be obtained from the outside.
B. greater control can be exercised over processing.
C. processing priorities can be established and enforced internally.
D. greater user involvement is required to communicate user needs.

Answer: A

Outsourcing is a contractual arrangement whereby the organization relinquishes control over part or all of the information processing to an external party. This is frequently done to acquire additional resources or expertise that is not obtainable from inside the organization.

345. The act that describes a computer intruder capturing a stream of data packets and inserting these packets into the network as if it were another genuine message stream is called:

A. eavesdropping.
B. message modification.
C. a brute-force attack.
D. packet replay.

Answer: D

Packet replay is a combination of passive and active modes of attack. This form of attack is particularly effective when the receiving end of the communication channel is automated and acts on the receipt and interpretation of information packets without human intervention.

346. When implementing and application software package, which of the following presents the GREATEST risk?

A. Uncontrolled multiple software versions
B. Source programs that are not synchronized with object code
C. Incorrectly set parameters
D. Programming errors

Answer: C

Parameters that are not set correctly would be the greatest concern when implementing an application software package. The other choices, though important, are a concern of the provider, not the organization that is implementing the software itself.

347. Which of the following is a check (control) for completeness?

A. Check digits
B. Parity bits
C. One-for-one checking
D. Prerecorded input

Answer: B

Parity bits are used to check for completeness of data transmissions. Choice A is incorrect because check digits are a control check for accuracy. Choice C is incorrect because in one-for-one checking, individual documents are matched to a detailed listing of documents processed by the computer, but do not ensure that all documents have been received for processing. Choice D (prerecorded input) is a data file control for which selected information fields are preprinted on blank input forms to reduce the chance of input errors.

348. Which of the following database administrator (DBA) activities is unlikely to be recorded on detective control logs?

A. Deletion of a record
B. Change of a password
C. Disclosure of a password

D. Changes to access rights

Answer: C

Password disclosure will not be detected by any database or system log. Password change activities may be recorded on the system log within the access control software. Database activities will be recorded on the appropriate database log.

349. An Internet-based attack using password sniffing can:

A. enable one party to act as if they are another party.
B. cause modification to the contents of certain transactions.
C. be used to gain access to systems containing proprietary information.
D. result in major problems with billing systems and transaction processing agreements.

Answer: C

Password sniffing attacks can be used to gain access to systems on which proprietary information is stored. Spoofing attacks can be used to enable one party to act as if they are another party. Data modification attacks can be used to modify the contents of certain transactions. Repudiation of transactions can cause major problems with billing systems and transaction processing agreements.

350. An IS auditor doing penetration testing during an audit of Internet connections would:

A. evaluate configurations.
B. examine security settings.
C. ensure virus-scanning software is in use.
D. use tools and techniques that are available to a hacker.

Answer: D

Penetration testing is a technique used to mimic an experienced hacker attacking a live site by using tools and techniques available to a hacker. The other choices are procedures that an IS auditor would consider undertaking during an audit of Internet connections, but are not aspects of penetration testing techniques.

351. After a full operational contingency test, the IS auditor performs a review of the recovery steps and concludes that the elapsed time until the technological environment and systems were actually functioning, exceeded the required critical recovery time. Which of the following should the auditor recommend?

A. Perform an integral review of the recovery tasks.
B. Broaden the processing capacity to gain recovery time.
C. Make improvements in the facility's circulation structure.
D. Increase the amount of human resources involved in the recovery.

Answer: A

Performing an exhaustive review of the recovery tasks would be appropriate to identify the way these tasks were performed, the time allocated to each of the steps required to accomplish recovery, and determine where adjustments can be made. Choices B, C, and D could be actions after the described review has been completed.

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

A. Audit log procedures
B. Table link/reference checks
C. Query/table access time checks
D. Rollback and rollforward database features

Answer: B

Performing table link/reference checks serve to detect table linking errors (completeness and accuracy of the contents of the database) and thus provide the greatest assurance of database integrity. Audit log

procedures enable recording of all events that have been identified and help in tracing the events. However, they only point to the event and do not ensure completeness or accuracy of the contents of the database. Querying/monitoring table access time checks help designers improve database performance, but not integrity. Rollback and rollforward database features ensure recovery from an abnormal disruption. They assure the integrity of the transaction that was being processed at the time of disruption, but do not provide assurance on the integrity of the contents of the database.

353. Which of the following is a strength of the program evaluation review technique (PERT) over other techniques? PERT:

A. considers different scenarios for planning and control projects.
B. allows the user to input program and system parameters.
C. tests system maintenance processes accurately.
D. estimates costs of system projects.

Answer: A

PERT considers different scenarios for planning and controlling projects. Three time estimates, optimistic, pessimistic and most likely are used to create a level of uncertainty in the estimation of the time for individual activities.

354. Which of the following provides nonrepudiation services for e-commerce transactions?

A. Public key infrastructure (PKI)
B. Data encryption standard (DES)
C. Message authentication code (MAC)
D. Personal identification number (PIN)

Answer: A

PKI is the administrative infrastructure for digital certificates and encryption key-pairs. The tests of an acceptable digital signature are: it is unique to the person using it, it is capable of verification, it is under the sole control of the person using it and it is linked to data in such a manner that if data are changed, the digital signature is invalidated. PKI meets these tests. The data encryption standard (DES) is the most common private-key cryptographic system. DES does not address non-repudiation. A MAC is a cryptographic value calculated by passing an entire message through a cipher system. The sender attaches the MAC before transmission and the receiver recalculates the MAC and compares it to the sent MAC. If the two MACs are not equal, this indicates that the message has been altered during transmission. It has nothing to do with non-repudiation. A PIN is a type of password, a secret number assigned to an individual which, in conjunction with some other means of identification serves to verify the authenticity of the individual.

355. Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

A. Power line conditioners
B. A surge protective device
C. An alternative power supply
D. An interruptible power supply

Answer: A

Power line conditioners are used to compensate for peaks and valleys in the power supply and reduce peaks in the power flow to what is needed by the machine. Any valleys are removed by power stored in the equipment. Surge protection devices protect against high voltage bursts. Alternative power supplies are intended for computer equipment running for longer periods and normally are coupled with other devices such as an uninterruptible power supply (UPS) to compensate for the power loss until the alternate power supply becomes available. An interruptible power supply would cause the equipment to come down whenever there was a power failure.

356. The BEST method of proving the accuracy of a system tax calculation is by:

A. detailed visual review and analysis of the source code of the calculation programs.
B. recreating program logic using generalized audit software to calculate monthly totals.

C. preparing simulated transactions for processing and comparing the results to predetermined results.
D. automatic flowcharting and analysis of the source code of the calculation programs.

Answer: C

Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

357. Which of the following is an IS control objective?

A. Output reports are locked in a safe place.
B. Duplicate transactions do not occur.
C. System backup/recovery procedures are updated periodically.
D. System design and development meet users' requirements.

Answer: B

Preventing duplicate transactions is a control objective. Having output reports locked in a safe place is an internal accounting control system, backup/recovery procedures are an operational control, and system design and development meeting user requirement is an administrative control.

358. Which of the following would be of the LEAST value to an IS auditor attempting to gain an understanding of an organization's IT process?

A. IT planning documents with deliverables and performance results
B. Policies and procedures relating to planning, managing, monitoring and reporting on performance
C. Prior audit reports
D. Reports of IT functional activities

Answer: C

Prior audit reports would be of least value because they provide historical and therefore not current information about areas of control weaknesses. Each of the other choices provides information useful for gaining an understanding of the process.

359. Which of the following ensures completeness and accuracy of accumulated data?

A. Processing control procedures
B. Data file control procedures
C. Output controls
D. Application controls

Answer: A

Processing controls ensure the completeness and accuracy of accumulated data, for example, editing and run-to-run totals. Data file control procedures ensure that only authorized processing occurs to stored data, for example transaction logs. Output controls ensure that data delivered to users will be presented, formatted and delivered in a consistent and secure manner, for example report distribution. Application controls are a general terminology composing all kinds of controls used in an application.

360. A goal of processing controls is to ensure that:

A. the data are delivered without compromised confidentiality.
B. all transactions are authorized.
C. accumulated data are accurate and complete through authorized routines.
D. only authorized individuals perform sensitive functions.

Answer: C

Processing controls include reconciliation of file totals, reasonableness verification, programmed checks, etc. Data delivered without compromised confidentiality is an output control goal. Having all transactions

authorized and having only authorized individuals perform sensitive functions are input control objectives.

361. Which of the following information valuation methods is LEAST likely to be used during a security review?

A. Processing cost
B. Replacement cost
C. Unavailability cost
D. Disclosure cost

Answer: A

Processing cost reflects the cost incurred for the data processing efforts, but does not take into account other factors like opportunity cost. Choices B, C and D are quite relevant to security. Replacement cost is the typical utilitarian view (most preferred for insurance purposes) that talks about the resources needed to reproduce the lost asset, in this case, the information. Unavailability cost is the effect on the business of information loss by way of lost revenue or lost opportunity. Disclosure cost relates to the intangible (and generally heavy) price that organization will have to pay if the information is compromised and reaches the hands where it should not be.

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

A. Application programmers are implementing changes to production programs.
B. Application programmers are implementing changes to test programs.
C. Operations support staff are implementing changes to batch schedules.
D. Database administrators are implementing changes to data structures.

Answer: A

"Production programs are used for processing an enterprise's data. It is imperative that controls on changes to production programs be stringent. Lack of control in this area could result in application programs being modified to manipulate the data. Application programmers are required to implement changes to test programs. These are used only in development and do not directly impact the live processing of data. Operations support staff implementing changes to batch schedules will affect the scheduling of the batches only
this does not impact the live data. Database administrators are required to implement changes to data structures. This is required for reorganization of the database to allow for additions, modifications or deletions of fields or tables in the database."

363. The FIRST task an IS auditor should complete when performing an audit in an unfamiliar area is to:

A. design the audit programs for each system or function involved.
B. develop a set of compliance tests and substantive tests.
C. gather background information pertinent to the new audit.
D. assign human and economical resources.

Answer: C

Proper planning is the necessary first step in performing effective audits. The IS auditor's first task should be to gather background information, such as business sector, applied benchmarks, specific trends and regulatory and legal requirements. This will allow the auditor to better understand what to audit. After gathering initial information, the auditor would then identify the audit subject and audit objectives, define the scope, establish the information systems and functions involved, and identify the needed resources.

364. A network diagnostic tool that monitors and records network information is a/an:

A. online monitor.
B. downtime report.
C. help desk report.
D. protocol analyzer.

Answer: D

Protocol analyzers are network diagnostic tools that monitor and record network information from packets traveling in the link to which the analyzer is attached. Online monitors (choice A) measure telecommunications transmissions and determine whether transmissions were accurate and complete. Downtime reports (choice B) track the availability of telecommunication lines and circuits. Help desk reports (choice C) are prepared by the help desk, which is staffed or supported by IS technical support personnel trained to handle problems occurring during the course of IS operations.

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

A. both the key used to encrypt and decrypt the data are public.
B. the key used to encrypt is private, but the key used to decrypt the data is public.
C. the key used to encrypt is public, but the key used to decrypt the data is private.
D. both the key used to encrypt and decrypt the data are private.

Answer: C

Public key encryption, also known as asymmetric key cryptography, uses a public key to encrypt the message and a private key to decrypt it.

366. Without causing a conflict of interest, a duty compatible with those of a security administrator would be:

A. quality assurance.
B. application programming.
C. systems programming.
D. data entry.

Answer: A

Quality assurance could be an additional responsibility of the security administrator. The security administrator, being responsible for application programming, systems programming or data entry, would not provide an adequate segregation of duties since he/she would be in a position to openly introduce fraudulent or malicious code or data causing damage to the organization.

367. Which of the following functions would be acceptable for the security administrator to perform in addition to his/her normal functions?

A. Systems analyst
B. Quality assurance
C. Computer operator
D. Systems programmer

Answer: B

Quality assurance duties could be performed by the security administrator and not cause a conflict with respect to segregation of duties. They deal in different aspects of IS with little overlap. The systems analyst function could potentially allow the security administrator to obtain knowledge, which in turn could be used to bypass security procedures. The computer operations function could allow the security administrator to bypass or deactivate security procedures. The systems programmer function could allow the security administrator to bypass or deactivate security procedures for their own benefit.

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

A. Quality of the metadata
B. Speed of the transactions
C. Volatility of the data
D. Vulnerability of the system

Answer: A

Quality of the metadata is the most important element in the design of a data warehouse. A data warehouse is a copy of transaction data specifically structured for query and analysis. Metadata aims to

provide a table of contents to the information stored in the data warehouse. Companies that have built warehouses believe that the metadata is the most important component of the warehouse.

369. Which of the following is a management technique that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality?

A. Function point analysis
B. Critical path methodology
C. Rapid application development
D. Program evaluation review technique

Answer: C

Rapid application development is a management technique that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality. Program evaluation review technique (PERT) and critical path methodology (CPM) are both planning and control techniques, while function point analysis is used for estimating the complexity of developing business applications.

370. Which of the following business recovery strategies would require the least expenditure of funds?

A. Warm site facility
B. Empty shell facility
C. Hot site subscription
D. Reciprocal agreement

Answer: D

Reciprocal agreements are the least expensive because they usually rely on a gentlemen's agreement between two firms. However, while they are the least expensive, they also are the least reliable and often unenforceable at the time of need.

371. Which of the following independent duties is traditionally performed by the data control group?

A. Access to data
B. Authorization tables
C. Custody of assets
D. Reconciliation

Answer: D

Reconciliation is a responsibility performed by the data control group, with the use of control totals and balancing sheets. This type of independent verification increases the level of confidence that the application has run successfully and the data are in proper balance. Access to data are controls provided by a combination of physical and logical security in both the user area and the information processing facility. Authorization tables are built by the IS department, based on the authorization forms provided by the data owners. Custody of assets must be determined and assigned appropriately. The data ownership usually is assigned to a particular user department, and duties should be specific and written. The owner of the data has responsibility for determining authorization levels required to provide adequate security, while the data security administration group is often responsible for implementing and enforcing the security system.

372. Which of the following is a practice that should be incorporated into the plan for testing disaster recovery procedures?

A. Invite client participation.
B. Involve all technical staff.
C. Rotate recovery managers.
D. Install locally stored backup.

Answer: C

Recovery managers should be rotated to ensure the experience of the recovery plan is spread. Clients may be involved but not necessarily in every case. Not all technical staff should be involved in each test. Remote or offsite backup should always be used.

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

A. Restricting operator access and maintaining audit trails
B. Monitoring and reviewing system engineering activity
C. Providing network redundancy
D. Establishing physical barriers to the data transmitted over the network

Answer: C

Redundancy, by building some form of duplication into the network components, such as a link, a router, a switch to prevent loss, delays, or data duplication is a control over component communication failure or error. Other related controls are loop/echo checks to detect line errors, parity checks, error correction codes and sequence checks. Choices A, B and D are communication network controls.

374. A referential integrity constraint consists of:

A. ensuring the integrity of transaction processing.
B. ensuring that data are updated through triggers.
C. ensuring controlled user updates to database.
D. rules for designing tables and queries.

Answer: B

Referential integrity constraints ensure that a change in a primary key of one table is automatically updated in a matching foreign key of other tables. This is done using triggers.

375. IS management has recently informed the IS auditor of its decision to disable certain referential integrity controls in the payroll system to provide users with a faster report generator. This will MOST likely increase the risk of:

A. data entry by unauthorized users.
B. a nonexistent employee being paid.
C. an employee receiving an unauthorized raise.
D. duplicate data entry by authorized users.

Answer: B

Referential integrity controls prevent the occurrence of unmatched foreign key values. Given that a nonexistent employee does not appear in the employees' table, it will never have a corresponding entry in the salary payments table. The other choices cannot be detected by referential integrity controls.

376. An organization wants to enforce data integrity principles and achieve faster performance/execution in a database application. Which of the following design principles should be applied?

A. User (customized) triggers
B. Data validation at the front end
C. Data validation at the back end
D. Referential integrity

Answer: D

Referential integrity should be implemented at the time of the design of the database to provide a faster execution mechanism. All other options are implemented at the application coding stage.

377. What data should be used for regression testing?

A. Different data than used in the previous test
B. The most current production data
C. The data used in previous tests
D. Data produced by a test data generator

Answer: C

Regression testing ensures that changes or corrections in a program have not introduced new errors. Therefore, this would be achieved only if the data used for regression testing are the same as the data used in previous tests.

378. Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. ensure the employee maintains a quality of life, which will lead to greater productivity.
B. reduce the opportunity for an employee to commit an improper or illegal act.
C. provide proper cross training for another employee.
D. eliminate the potential disruption caused when an employee takes vacation one day at a time.

Answer: B

Required vacations/holidays of a week or more duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions. This reduces the opportunity to commit improper or illegal acts, and during this time it may be possible to discover any fraudulent activity that was taking place. Choices A, C and D all could be organizational benefits from a mandatory vacation policy, but not the reason why it is established.

379. During an audit, an IS auditor learns that lengthy and complex passwords are required to reach the network via modem. These passwords were established by an outside provider. The communications software allows users to select a "remember password" option. What should the IS auditor's PRIMARY recommendation be?

A. Disable the save password option and have users record them elsewhere.
B. Request that the provider change the dial-in password to a group password.
C. Establish and enforce a process to have users change their passwords.
D. Allow users to change their passwords to something less complex.

Answer: C

Requiring users to change their passwords is a user account management process. Passwords are a form of shared secrets, useful only if they are secret. Having users select something memorable is preferable to having it saved on the machine. Disabling the save password option, would minimize the ease or access by unauthorized persons with access to the hardware. However, having users write their passwords down or included in a file on their machine defeats the purpose of having a complex password. Requesting the provider to change the password to a group password would decrease the usefulness of the audit trail and therefore the ability to hold individual users accountable. Allowing users to change their passwords is a better suggestion. However, if users are not forced to do this on a periodic basis, this also defeats the purpose.

380. Which of the following MUST exist to ensure the viability of a duplicate information processing facility?

A. The site is near the primary site to ensure quick and efficient recovery.
B. The site contains the most advanced hardware available.
C. The workload of the primary site is monitored to ensure adequate backup is available.
D. The hardware is tested when it is installed to ensure it is working properly.

Answer: C

Resource availability must be assured. The workload of the site must be monitored to ensure that availability for emergency backup use is not impaired. The site chosen should not be subject to the same natural disaster as the primary site. In addition, a reasonable compatibility of hardware/software must exist to serve as a basis for backup. The latest or newest hardware may not adequately serve this need. Testing the hardware when the site is established is essential, but regular testing of the actual backup data is necessary to ensure the operation will continue to perform as planned.

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

A. System access log files
B. Enabled access control software parameters
C. Logs of access control violations
D. System configuration files for control options used

Answer: D

Review of system configuration files for control options used would show which users have access to the privileged supervisory state. Both systems access log files and logs of access violations are detective in nature. Access control software is run under the operating system.

382. During a post-implementation review of an enterprise resource management system, an IS auditor would MOST likely:

A. review access control configuration.
B. evaluate interface testing.
C. review detailed design documentation.
D. evaluate system testing.

Answer: A

Reviewing access control configuration would be first task performed to determine whether security has been mapped appropriately in the system. Since a post-implementation review is done after user acceptance testing and actual implementation, one would not engage in interface testing or detailed design documentation. Evaluating interface testing would be part of the implementation process. The issue of reviewing detailed design documentation is not generally relevant to an enterprise resource management system since these are usually vendor packages with user manuals. System testing should be performed before final user sign off.

383. Which of the following audit procedures would an IS auditor be LEAST likely to include in a security audit?

A. Review the effectiveness and utilization of assets.
B. Test to determine that access to assets is adequate.
C. Validate physical, environmental and logical access policies per job profiles.
D. Evaluate asset safeguards and procedures that prevent unauthorized access to the assets.

Answer: A

Reviewing the effectiveness and utilization of assets is not within the purview of a security audit. Security audits primarily focus on the evaluation of the policies and procedures that ensure the confidentiality, integrity and availability of data. During an audit of security the IS auditor would normally review access to assets, and validate the physical and environmental controls to the extent necessary to satisfy the audit requirements. The IS auditor would also review logical access policies and compare them to job profiles to ensure that excessive access has not been granted. The review also would include an evaluation of asset safeguards and procedures to prevent unauthorized access to assets.

384. When performing a general controls review, an IS auditor checks the relative location of the computer room inside the building. What potential threat is the IS auditor trying to identify?

A. Social engineering
B. Windstorm
C. Earthquake
D. Flooding

Answer: D

Rooms located on higher floors are less likely to flood than the ground floor. There is no more or less chance of damage from social engineering, wind or earthquake.

385. To prevent an organization's computer systems from becoming part of a distributed denial-of-service attack, IP packets containing addresses that are listed as unroutable can be isolated by:

A. establishing outbound traffic filtering.
B. enabling broadcast blocking.
C. limiting allowable services.
D. network performance monitoring.

Answer: A

Routers programmed with outbound traffic filtering, drop outbound packets that contain addresses from other than the user's organization, including source addresses that can not be routed. Broadcast blocking can be done by filtering routers or firewalls. When programmed, IP packets coming from the Internet and using an address that broadcasts to every computer on the destination organization's network can be dropped. Firewalls and filtering routers can be programmed to limit services not allowed by policy and can help prevent use of the company's systems. However, this will not isolate packets that can not be routed. Network performance monitoring is a way to monitor system performance for potential intrusions on a real-time basis and could help identify unusual traffic volumes.

386. Which of the following is a control to detect an unauthorized change in a production environment?

A. Denying programmers access to production data.
B. Requiring change request to include benefits and costs.
C. Periodically comparing control and current object and source programs.
D. Establishing procedures for emergency changes.

Answer: C

Running the code comparison program on the control and current object and source programs allows for the detection of unauthorized changes in the production environment. Choices A, B and D are preventive controls that are effective as long as they are being applied consistently.

387. Which of the following types of controls is designed to provide the ability to verify data and record values through the stages of application processing?

A. Range checks
B. Run-to-run totals
C. Limit checks on calculated amounts
D. Exception reports

Answer: B

Run-to-run totals provide the ability to verify data values through the stages of application processing. Run-to-run total verification ensures that data read into the computer was accepted and then applied to the updating process.

388. Following a reorganization of a company's legacy database, it was discovered that records were accidentally deleted. Which of the following controls would have MOST effectively detected this occurrence?

A. Range check
B. Table lookups
C. Run-to-run totals
D. One-for-one checking

Answer: C

Run-to-run totals would have been an effective detective control over processing in this situation. Table lookups and range checks are used for data validation before input, or as close to the point of origination as possible. One-for-one checking is time consuming and therefore less effective.

389. Security administration procedures require read-only access to:

A. access control tables.
B. security log files.
C. logging options.
D. user profiles.

Answer: B

Security administration procedures require read-only access to security log files to ensure that, once generated, the logs are not modified. Logs provide evidence and track suspicious transactions and activities. Security administration procedures require write access, to access control tables to manage and update the privileges according to authorized business requirements. Logging options require write access to allow the administrator to update the way the transactions and user activities are monitored, captured, stored, processed and reported.

390. Of the following who is MOST likely to be responsible for network security operations?

A. Users
B. Security administrators
C. Line managers
D. Security officers

Answer: B

Security administrators generally are responsible for day-to-day network security operations and also overall network performance. This may include managing user accounts, implementing security patches and other related system software upgrades, writing scripts for routinely archiving log files to a centralized secured server set up for this purpose, and managing the systems workload to maintain performance within acceptable thresholds.

391. Sales orders are automatically numbered sequentially at each of a retailer's multiple outlets. Small orders are processed directly at the outlets, with large orders sent to a central production facility. The MOST appropriate control to ensure that all orders transmitted to production are received and processed would be to:

A. send and reconcile transaction counts and totals.
B. have data transmitted back to the local site for comparison.
C. compare data communications protocols with parity checking.
D. track and account for the numerical sequence of sales orders at the production facility.

Answer: A

Sending and reconciling transaction totals not only ensures that the orders were received, but also processed by the central production location. Transmission back to the local site confirms that the central location received it, but not that they have actually processed it. Tracking and accounting for the numerical sequence only confirms what orders are on hand, and not whether they actually have been completed. The use of parity checking would only confirm that the order was not changed during transmission.

392. IS auditors reviewing access control should review data classification to ensure that encryption parameters are classified as:

A. sensitive.
B. confidential.
C. critical.
D. private.

Answer: A

Sensitive applies to information that requires special precautions to assure the integrity of the information, by protecting it from unauthorized modification or deletion, hence, encryption parameters should be classified as sensitive. Confidential applies to the most sensitive business information that is intended strictly for use within an organization. Critical applies to information that is an important to the organization's business objectives. Private applies to personal information that is intended for use within an organization.

393. The information that requires special precaution to ensure integrity is termed?

A. Public data

B. Private data
C. Personal data
D. Sensitive data

Answer: D

Sensitive data applies to information that requires special precaution to ensure its integrity. It represents information that requires a higher than normal assurance of accuracy and completeness. Public data applies to data that can be accessed by the public but should be updated/deleted only by authorized personnel. Private data applies to personnel information that is intended for use within the organization. Personal data is not a common data classification term.

394. An IS auditor performing an independent classification of systems should consider a situation where functions could be performed manually at a tolerable cost for an extended period of time as:

A. critical.
B. vital.
C. sensitive.
D. noncritical.

Answer: C

Sensitive functions are best described as those that can be performed manually at a tolerable cost for an extended period of time. Critical functions are those that cannot be performed unless they are replaced by identical capabilities and cannot be replaced by manual methods. Vital functions refer to those that can be performed manually but only for a brief period of time. This is associated with lower costs of disruption than critical functions. Noncritical functions may be interrupted for an extended period of time, at little or no cost to the company, and require little time or cost to restore.

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

A. Analyzer
B. Administration console
C. User interface
D. Sensor

Answer: D

Sensors are responsible for collecting data. Analyzers receive input from sensors and determine intrusive activity. An administration console and a user interface are components of an IDS.

396. The general ledger setup function in an enterprise resource package (ERP) allows for setting accounting periods. Access to this function has been permitted to users in finance, the warehouse and order entry. The MOST likely reason for such broad access is the:

A. need to change accounting periods on a regular basis..
B. requirement to post entries for a closed accounting period.
C. lack of policies and procedures for the proper segregation of duties.
D. need to create/modify the chart of accounts and its allocations.

Answer: C

Setting of accounting periods is one of the critical activities of the finance function. Granting access to this function to the personnel in the warehouse and order entry could be because of a lack of proper policies and procedures for the adequate segregation of duties. Accounting periods should not be changed at regular intervals, but established permanently. The requirement to post entries for a closed accounting period is a risk. If necessary this should be done by someone in the finance or accounting area. The need to create/modify the chart of accounts and its allocations is the responsibility of the finance department and is not a function that should be performed by warehouse or order entry personnel.

397. An IS auditor observed that some data entry operators leave their computers in the midst of data entry without logging off. Which of the following controls should be suggested to prevent unauthorized access?

A. Encryption
B. Switch off the computer when leaving
C. Password control
D. Screen saver password

Answer: D

Since data entry operators have to attend to other assignments in the midst of data entry and the nature of the assignments are such that they do not logoff the computer, screen saver password is the only effective control to guard against unauthorized access. Encryption does not prevent access to the computer, it only guards against disclosure of the confidential contents of the files. Switching off the computer without properly shutting it down is not advisable. Password control takes place when logging on to anapplication and is not effective in this scenario.

398. Which of the following fire suppressant systems would an IS auditor expect to find when conducting an audit of an unmanned computer center?

A. Carbon dioxide
B. Halon
C. Dry-pipe sprinkler
D. Wet-pipe sprinkler

Answer: A

Since fire cannot burn in carbon dioxide, it is an effective suppressant. However, in a manned operation, the release of this gas is likely to result in fatalities so automatic release is inadvisable, if not illegal, and manual release delays the suppression of the fire. Where an installation is unmanned, carbon dioxide can be released automatically should a fire be detected. Halon gas may be released automatically, as it is breathable by humans and will suppress a fire. However, since it has an adverse affect on the earth's ozone layer, its use is discouraged and, in many countries, banned. Dry-pipe sprinklers, which fill with water only when the fire is detected, are considered an appropriate option in manned installations but are not necessary when people are not present. Wet-pipe sprinklers, which are filled with water at all times, are not a viable option for a computer installation due to the risk of leaks.

399. The PRIMARY objective of a business continuity and disaster recovery plan should be to:

A. safeguard critical IS assets.
B. provide for continuity of operations.
C. minimize the loss to an organization.
D. protect human life.

Answer: D

Since human life is invaluable, the main priority of any business continuity and disaster recovery plan should be to protect people. All other priorities are important but are secondary objectives of a business continuity and disaster recovery plan.

400. What type of transmission requires modems?

A. Encrypted
B. Digital
C. Analog
D. Modulated

Answer: C

Since most communication switches are analog, modems are required to convert data from digital to analog.

401. Which of the following is the MOST effective control procedure for security of a stand-alone small business computer environment?

A. Supervision of computer usage
B. Daily management review of the trouble log
C. Storage of computer media in a locked cabinet
D. Independent review of an application system design

Answer: A

Since small stand-alone business computer environments normally lack basic controls such as access control software and a strict segregation of duties, strong compensating controls should be applied. In this situation, supervision of computer usage must be relied upon. This takes the form of monitoring office activity, reviewing key control reports, and sampling employee work to ensure it is appropriate and authorized.

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

A. Transaction authorization
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

Answer: A

Since the interaction between parties is electronic, there is no inherent authentication occurring, therefore, transaction authorization is the greatest risk. Choices B and D are examples of risks, but the impact is not as great as that of unauthorized transactions. Transmission delays may terminate the process or hold the line until the normal time for processing has elapsed, however there will be no loss of data.

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

A. test data to validate data input.
B. test data to determine system sort capabilities.
C. generalized audit software to search for address field duplications.
D. generalized audit software to search for account field duplications.

Answer: C

Since the name is not the same (due to name variations), one method to detect duplications would be to compare other common fields, such as addresses. Subsequent review to determine common customer names at these addresses could then be conducted. Searching for duplicate account numbers would not likely find duplications since customers would most likely have different account numbers for each variation. Test data would not be useful to detect the extent of any data characteristic, but simply to determine how the data were processed.

404. A control log basic to a real-time application system is a(n):

A. audit log.
B. console log.
C. terminal log.
D. transaction log.

Answer: D

Since this is a real-time system the answer is a transaction log. If the system failed, significant costs would be incurred to reenter transaction data if a transaction log were not maintained. A transaction log also permits operations personnel to determine which transactions have been posted, and this helps to decrease recovery time when system failures occur.

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

A. Encryption
B. Sniffing
C. Spoofing
D. A signed document cannot be altered.

Answer: B

Sniffing is an attack that can be used to capture sensitive pieces of information (password), passing through the network. Encryption is a method of scrambling information to prevent unauthorized individuals from understanding the transmission. Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication. Data destruction is erasing information or removing it from its original location.

406. The process of using interpersonal communication skills to get unauthorized access to company assets is called:

A. wire tapping.
B. trap doors.
C. war dialing.
D. social engineering.

Answer: D

Social engineering is a term that describes a nontechnical kind of intrusion that relies heavily on human interaction and often involves tricking other people into breaking normal security procedures. Wire tapping is a technique used for getting the signals transmitted over cables without disturbing the flow between the source and destination. Trap doors are a deliberately left break in the software source code by programmers to enable the insertion of additional debugging code. The trap door may be used later for some unwanted purposes. War dialing involves trying out all the published phone numbers of the company to find one that is connected to a modem and subsequently using that as an entry point into the corporate databases.

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

A. social engineering.
B. sniffers.
C. backdoors.
D. trojan horses.

Answer: A

Social engineering is based on the divulgence of private information through dialogues, interviews, inquiries, etc., in which a user may be indiscreet regarding his or other's personal data. A sniffer is a computer tool to monitor the traffic in networks. Backdoors are computer programs left by hackers to exploit vulnerabilities. Trojan horses are computer programs that pretend to supplant a real program, thus, the functionality of the program is not authorized and is usually malicious in nature.

408. If the decision has been made to acquire software rather than develop it internally, this decision is normally made during the:

A. requirements definition phase of the project.
B. feasibility study phase of the project.
C. detailed design phase of the project.
D. programming phase of the project.

Answer: B

Software acquisition is not a phase in what is regarded as the standard system development life cycle. However, if a decision is made to acquire rather than develop software, this process should occur after the requirements definition phase and a decision is normally made in the feasibility study phase.

409. The secure socket layer (SSL) protocol addresses the confidentiality of a message through:

A. symmetric encryption.
B. message authentication code.
C. hash function.
D. digital signature certificates.

Answer: A

SSL uses a symmetric key for message encryption. A message authentication code is used for ensuring data integrity. Hash function is used for generating a message digest. It does not use public key encryption for message encryption. Digital signature certificates are used by SSL for server authentication.

410. Which of the following represents the MOST pervasive control over application development?

A. IS auditors
B. Standard development methodologies
C. Extensive acceptance testing
D. Quality assurance groups

Answer: B

Standard development methodologies will provide consistency for all systems utilized in the company. They also assist the IS auditor by providing a standard with which to measure the adequacy of a system.

411. With regard to sampling it can be said that:

A. sampling is generally applicable when the population relates to an intangible or undocumented control.
B. if an auditor knows internal controls are strong, the confidence coefficient may be lowered.
C. attribute sampling would help prevent excessive sampling of an attribute by stopping an audit test at the earliest possible moment.
D. variable sampling is a technique to estimate the rate of occurrence of a given control or set of related controls.

Answer: B

Statistical sampling quantifies how closely the sample should represent the population, usually as a percentage. If the auditor knows internal controls are strong, the confidence coefficient may be lowered. Sampling generally is applicable when the population relates to a tangible or documented control. Choice C is a description of stop-or-go sampling. Choice D is a definition of attribute sampling.

412. Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

A. has been approved by line management.
B. does not vary from the IS department's preliminary budget.
C. complies with procurement procedures.
D. supports the business objectives of the organization.

,

Strategic planning sets corporate or department objectives into motion. Both long-term and short-term strategic plans should be consistent with the organization's broader plans and business objectives for attaining these goals. Answer A is incorrect since line management prepared the plans.

413. Which of the following goals would you expect to find in an organization's strategic plan?

A. Test a new accounting package.
B. Perform an evaluation of information technology needs.
C. Implement a new project planning system within the next 12 months.
D. Become the supplier of choice within a given time period for the product offered.

Answer: D

Strategic planning sets corporate or departmental objectives into motion. Comprehensive planning helps ensure an effective and efficient organization. Strategic planning is time and project oriented, but also must address and help determine priorities to meet business needs. Long- and short-range plans should be consistent with the organization's broader plans for attaining their goals. Choice D represents a business objective that is intended to focus the overall direction of the business and would thus be a part of the organization's strategic plan. The other choices are project oriented and do not address business objectives.

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

A. strategic plans.
B. IS policies.
C. IS procedures.
D. standards and guidelines.

Answer: A

Strategic plans provide the basis for ensuring that the enterprise meets its goals and objectives. Involvement of senior management is critical to ensuring that the plan adequately addresses the established goals and objectives. IS policies, procedures, standards and guidelines are all structured to support the overall strategic plan.

415. Which of the following would an IS auditor expect to find in a console log?

A. Names of system users
B. Shift supervisor identification
C. System errors
D. Data edit errors

Answer: C

System errors are the only ones that you would expect to find in the console log.

416. Which of the following is the MOST effective means of determining which controls are functioning properly in an operating system?

A. Consulting with the vendor
B. Reviewing the vendor installation guide
C. Consulting with the system programmer
D. Reviewing the system generation parameters

Answer: D

System generation parameters determine how a system runs, the physical configuration and its

417. Analysis of which of the following would MOST likely enable the IS auditor to determine if a non-approved program attempted to access sensitive data?

A. Abnormal job termination reports
B. Operator problem reports
C. System logs
D. Operator work schedules

Answer: C

System logs are automated reports that identify most of the activities performed on the computer. Many programs have been developed which analyze the system log to report on specifically defined items. Abnormal job termination reports identify application jobs that were terminated before successful completion. Operator problem reports are used by operators to log computer operations problems and their solutions. Operator work schedules are maintained by IS management to assist in human resource planning.

418. A tax calculation program maintains several hundred tax rates. The BEST control to ensure that tax rates entered into the program are accurate is:

A. an independent review of the transaction listing.
B. a programmed edit check to prevent entry of invalid data.
C. programmed reasonableness checks with 20 percent data entry range.
D. a visual verification of data entered by the processing department.

Answer: A

Tax rates represent critical data that will be used in numerous calculations and should be independently verified by someone other than the entry person before they are used in processing. Choices B and C are programmed controls that are useful for preventing gross errors, that is, errors such as an added zero or alpha instead of a numeric. A tax table must be 100 percent accurate, not just readable. Choice D will allow the data entry person to check input accuracy, but it is not sufficient.

419. An advantage of using sanitized live transactions in test data is that:

A. all transaction types will be included.
B. every error condition is likely to be tested.
C. no special routines are required to assess the results.
D. test transactions are representative of live processing.

Answer: D

"Test date will be representative of live processing
however, it is unlikely that all transaction types or error conditions will be tested in this way."

420. Good quality software is BEST achieved:

A. through thorough testing.
B. by finding and quickly correcting programming errors.
C. determining the amount of testing by the available time and budget.
D. by applying well-defined processes and structured reviews throughout the project.

Answer: D

Testing can point to quality deficiencies, However, it cannot by itself fix them. Corrective action at this point in the project is expensive. While it is necessary to detect and correct program errors, the bigger return comes from detecting defects as they occur in upstream phases, such as requirements and design. Choice C is representative of the most common mistake when applying quality management to a software project. It is seen as overhead, instead early removal of defects has a substantial payback. Rework is actually the largest cost driver on most software projects. Choice D represents the core of achieving quality, that is, following a well defined consistent process and effectively reviewing key deliverables.

421. Which of the following user profiles should be of MOST concern to the IS auditor, when performing an audit of an EFT system?

A. Three users with the ability to capture and verifiy their own messages
B. Five users with the ability to capturr and send their own messages
C. Five users with the ability to verificy other users and to send of their own messages
D. Three users with the ability to capture and verifiy the messages of other users and to send their own messages

Answer: A

The ability by one individual to capture and verify messages represents an inadequate segregation, since messages can be taken as correct and as if they had already been verified.

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

A. The alternate facility will be available until the original information processing facility is restored.

B. User management was involved in the identification of critical systems and their associated critical recovery times.
C. Copies of the plan are kept at the homes of key decision making personnel.
D. Feedback to management assuring them that the business continuity plans are indeed workable and that the procedures are current.

Answer: A

The alternate facility should be made available until the original site is restored to provide the greatest assurance of recovery after a disaster. Without this assurance, the plan will not be successful. All other choices ensure prioritization or the execution of the plan.

423. Which of the following types of firewalls provide the GREATEST degree and granularity of control?

A. Screening router
B. Packet filter
C. Application gateway
D. Circuit gateway

Answer: C

The application gateway is similar to a circuit gateway, but it has specific proxies for each service. To be able to handle web services it has an HTTP proxy, which acts as an intermediary between externals and internals, but specifically for HTTP. This means that it not only checks the packet IP addresses (layer 3) and the ports it is directed to (in this case port 80, layer 4), it also checks every http command (layer 5 and 7). Therefore, it works in a more detailed (granularity) way than the others. Screening router and packet filter (choices A and B) basically work at the protocol, service and/or port level. This means that they analyze packets from layers 3 and 4 (not from higher levels). A circuit-gateway (choice D) is based on a proxy or program that acts as an intermediary between external and internal accesses. This means that, during an external access, instead of opening a single connection to the internal server, two connections are established-one from the external to the proxy (which conforms the circuit-gateway) and one from the proxy to the internal. Layers 3 and 4 (IP and TCP) and some general features from higher protocols are used to perform these tasks.

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

A. System analysis
B. Authorization of access to data
C. Application programming
D. Data administration

Answer: B

The application owner is responsible for authorizing access to data. Application development and programming are functions of the IS department. Similarly, system analysis should be performed by qualified persons in IS who have knowledge of IS and user requirements. Data administration is a specialized function related to database management systems and should be performed by qualified database administrators.

425. Which of the following is the PRIMARY reason for involving an IS auditor in the definition of a system's requirements?

A. Post-application reviews do not need to be performed.
B. Total budgeted system development costs can be reduced.
C. It is costly to institute controls after a system becomes operational.
D. The extent of user involvement in design activities is reduced.

Answer: C

The assurance of adequate controls is the primary reason for an IS auditor's involvement in the requirements definition process. The fact that these controls can be designed into the system as opposed

to being retrofitted brings cost savings to the overall cost of the system. Therefore, this is a basic justification for involving the IS auditor in the system development process.

426. The primary purpose of an audit charter is to:

A. document the audit process used by the enterprise.
B. formally document the audit department's plan of action.
C. document a code of professional conduct for the auditor.
D. describe the authority and responsibilities of the audit department.

Answer: D

The audit charter typically sets out the role and responsibility of the internal audit department. It should state management's objectives for and delegation of authority to the audit department. It is rarely changed and does not contain the audit plan or audit process which is usually part of annual audit planning, nor does it describe a code of professional conduct since such conduct is set by the profession and not by management.

427. An IS auditor performing a telecommunication access control review should be concerned PRIMARILY with the:

A. maintenance of access logs of usage of various system resources.
B. authorization and authentication of the user prior to granting access to system resources.
C. adequate protection of stored data on servers by encryption or other means.
D. accountability system and the ability to identify any terminal accessing system resources.

Answer: B

The authorization and authentication of users is the most significant aspect in a telecommunications access control review as it is a preventive control. Weak controls at this level can affect all other aspects. The maintenance of access logs of usage of system resources is a detective control. The adequate protection of data being transmitted to and from servers by encryption or other means is a method of protecting information during transmission and is not an access issue. The accountability system and the ability to identify any terminal accessing system resources deal with controlling access through the identification of a terminal.

428. In regard to moving an application program from the test environment to the production environment, the BEST control would be provided by having the:

A. application programmer copy the source program and compiled object module to the production libraries.
B. as paul says,
C. production control group compile the object module to the production libraries using the source program in the test environment.
D. production control group copy the source program to the production libraries and then compile the program.

Answer: D

The best control would be provided by having the production control group copy the source program to the production libraries and then compile the program.

429. Confidential data stored on a laptop is BEST protected by:

A. storage on optical disks.
B. logon ID and password.
C. data encryption.
D. physical locks.

Answer: C

The best protection for confidential data stored on a laptop is data encryption. Data, if not encrypted, would be accessible to anyone who has access to the disks. Logon ID and password are not the best protection because a stand-alone laptop, depending on the operating system, may not need an ID and

password to begin a session, and it is relatively easy to bypass security controls on laptops to gain access to the operating system. Physical locks prevent physical theft only.

430. Which of the following would be the BEST population to take a sample from when testing program changes?

A. Test library listings
B. Source program listings
C. Program change requests
D. Production library listings

Answer: D

The best source from which to draw any sample or test of system information is the automated system. The production libraries represent executables that are approved and authorized to process organizational data. Source program listings would be time intensive. Program change requests are the documents used to initiate change. There is no guarantee that the request has been completed for all changes. Test library listings do not represent the approved and authorized executables.

431. 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:

A. payroll reports should be compared to input forms.
B. gross payroll should be recalculated manually.
C. checks (cheques) should be compared to input forms.
D. checks (cheques) should be reconciled with output reports.

Answer: A

The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the input (payroll reports). Hence, comparing payroll reports with input forms is the best mechanism of verifying data accuracy. Recalculating gross payroll manually would only verify whether the processing is correct and not the data accuracy of inputs. Comparing checks to input forms is not feasible as checks have the processed information and input forms have the input data. Reconciling checks with output reports only confirms that checks have been issued as per output reports.

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

A. Overwriting the tapes
B. Initializing the tape labels
C. Degaussing the tapes
D. Erasing the tapes

Answer: C

The best way to handle obsolete magnetic tapes is to degauss them. This action leaves a very low residue of magnetic induction, essentially erasing the data from the tapes. Overwriting or erasing the tapes may cause magnetic errors but would not remove the data completely. Initializing the tape labels would not remove the data that follows the label.

433. Business continuity/disaster recovery is PRIMARILY the responsibility of:

A. IS management.
B. business unit managers.
C. the security administrator.
D. the board of directors.

Answer: D

The board of directors is primarily and ultimately responsible for business continuity/disaster recovery. They are entrusted with safeguarding both the assets of the company and the viability of the company.

Business continuity/disaster recovery planning is not an isolated activity, it must be consistant with and support the overall plan of the organization. IS management and business unit managers are responsible for the continuity/recovery of their respective functions, not responsble for the organization as a whole. The security adminitrator is responsible for implementing, monitoring and enforcing security policies established and authorized by management.

434. An advantage in using a bottom-up versus a top-down approach to software testing is that:

A. interface errors are detected earlier.
B. confidence in the system is achieved earlier.
C. errors in critical modules are detected earlier.
D. major functions and processing are tested earlier.

Answer: C

The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and works upwards until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing is the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices in this question all refer to advantages of a top-down approach which follows the opposite path, either in depth-first or breadth-first search order.

435. During an audit of an enterprise that is dedicated to e-commerce, the IS manager states that digital signatures are used in the establishment of its commercial relations. To substantiate this, the IS auditor must prove that which of the following is used?

A. A biometric, digitalized and encrypted parameter with the customer's public key
B. A hash of the data that is transmitted and encrypted with the customer's private key
C. A hash of the data that is transmitted and encrypted with the customer's public key
D. The customer's scanned signature, encrypted with the customer's public key

Answer: C

The calculation of a hash or digest of the data that is transmitted and its encryption requires the public key of the client (receiver) and is called a signature of the message or digital signature. The receiver performs the same process and then compares the received hash once it has been decrypted with his/her private key, with the hash that he/she calculates with the received data. If they are the same, the conclusion would be that there is integrity in the data that has arrived and the origin is authenticated.

436. Which of the following manages the digital certificate life cycle to ensure adequate security and controls exist in digital signature applications related to e-commerce?

A. Registration authority
B. Certification authority
C. Certification relocation list
D. Certification practice statement

Answer: B

The certification authority (CA) maintains a directory of digital certificates for the reference of those receiving them. It manages the certificate life cycle, including certificate directory maintenance and certificate revocation list maintenance and publication. Choice A is not correct because a registration authority is an optional entity that is responsibile for the administrative tasks associated with registering the end entity that is the subject of the certificate issued by the CA. Choice C is incorrect since a CRL is an instrument for checking the continued validity of the certificates for which the CA has responsibility. Choice D is incorrect because a certification practice statement is a detailed set of rules governing the certificate authority's operations.

437. Which of the following IS functions may be performed by the same individual, without compromising on control or violating segregation of duties?

A. Job control analyst and applications programmer
B. Mainframe operator and system programmer

C. Change/problem and quality control administrator
D. Applications and system programmer

Answer: C

The change/problem and quality control administrator are two compatible functions that would not compromise control or violate segregation of duties. The other functions listed, if combined, would result in compromising control.

438. In a web server, a common gateway interface (CGI) is MOST often used as a(n):

A. consistent way for transferring data to the application program and back to the user.
B. computer graphics imaging method for movies and TV.
C. graphic user interface for web design.
D. interface to access the private gateway domain.

Answer: A

The common gateway interface (CGI) is a standard way for a web server to pass a user's request to an application program and to move data back and forth to the user. When the user requests a web page (for example, by clicking on a highlighted word or entering a web site address), the server sends back the requested page. However, when a user fills out a form on a web page and sends it in, it usually needs to be processed by an application program. The web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method, or convention for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the web's HTTP protocol.

439. A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses the team should:

A. compute the amortization of the related assets.
B. calculate a return on investment (ROI).
C. apply a qualitative approach.
D. spend the time needed to define exactly the loss amount.

Answer: C

The common practice, when it is difficult to calculate the financial losses, is to take a qualitative approach, in which the manager affected by the risk defines the financial loss in terms of a weighted factor (e.g., 1 is a very low impact to the business and 5 is a very high impact). A ROI is computed when there is a predictable savings or revenues, which can be compared to the investment needed to realize the revenues. Amortization is used in a profit and loss statement, not in computing potential losses. Spending the time needed to define exactly the total amount is normally a wrong approach. If it has been difficult to estimate potential losses (e.g., losses derived from erosion of public image due to a hack attack) that situation is not likely to change, and at the end of the day, you will arrive with a not well-supported evaluation.

440. Receiving an EDI transaction and passing it through the communications interface stage usually requires:

A. translating and unbundling transactions.
B. routing verification procedures.
C. passing data to the appropriate application system.
D. creating a point of receipt audit log.

Answer: B

The communications interface stage requires routing verification procedures. EDI or ANSI X12 is a standard that must be interpreted by an application for transactions to be processed and then to be invoiced, paid and sent, whether they are for merchandise or services. There is no point in sending and receiving EDI transactions if they cannot be processed by an internal system. Unpacking transactions and recording audit logs are both important elements that help follow business rules and establish controls, but are not part of the communications interface stage.

441. If an application program is modified and proper system maintenance procedures are in place, which of the following should be tested? The:

A. integrity of the database
B. access controls for the applications programmer
C. complete program, including any interface systems
D. segment of the program containing the revised code

Answer: C

The complete program with all interfaces needs to be tested to determine the full impact of a change to program code. Usually the more complex the program, the more testing required.

442. Sign-on procedures include the creation of a unique user ID and password. However, an IS auditor discovers that in many cases the user name and password are the same. The BEST control to mitigate this risk is to:

A. change the company's security policy.
B. educate users about the risk of weak passwords.
C. build in validations to prevent this during user creation and password change.
D. require a periodic review of matching user ID and passwords for detection and correction.

Answer: C

The compromise of the password is the highest risk. The best control is a preventive control through validation at the time the password is created or changed. Changing the company's security policy and educating users about the risk of weak passwords only provides information to users, but does little to enforce this control. Requiring a periodic review of matching user ID and passwords for detection and ensuring correction is a detective control.

443. What is a risk associated with attempting to control physical access to sensitive areas, such as computer rooms, through card keys, locks, etc.?

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

Answer: A

The concept of piggybacking compromises all physical control established. Choice B would be of minimal concern in a disaster recovery environment. Items in choice C are not easily duplicated. Regarding choice D, technology is constantly changing but card keys have existed for some time and appear to be a viable option for the foreseeable future.

444. Which of the following is the MOST important consideration when developing a business continuity plan for a bank?

A. Antivirus software
B. Naming standards
C. Customer balance list
D. Password policy

Answer: C

The customer balance list provides a basis for providing minimum service in case of short time non-availability of branch computers. Antivirus software, password policy and naming standards are preventive controls and are not required for business continuity planning.

445. Which of the following controls will detect MOST effectively the presence of bursts of errors in network transmissions?

A. Parity check

B. Echo check
C. Block sum check
D. Cyclic redundancy check

Answer: D

The cyclic redundancy check (CRC) can check for a block of transmitted data. The workstations generate the CRC and transmit it with the data. The receiving workstation computes a CRC and compares it to the transmitted CRC. If both of them are equal, then the block is assumed error free. In this case (such as in parity error or echo check), multiple errors can be detected. In general, CRC can detect all single-bit and bubble-bit errors. Parity check also (known as vertical redundancy check) involves adding a bit-known as the parity bit-to each character during transmission. In this case, where there is a presence of bursts of errors (i.e., impulsing noise during high transmission rates), it has a reliability of approximately 50 percent. In higher transmission rates, this limitation is significant. Echo checks detect line errors by retransmitting data back to the sending device for comparison with the original transmission.

446. Which of the following would be the LEAST likely indication that complete or selected outsourcing of IS functions should be considered?

A. The applications development backlog is greater than three years.
B. It takes one year to develop and implement a high-priority system.
C. More than 60 percent of programming costs are spent on system maintenance.
D. Duplicate information systems functions exist at two sites.

Answer: B

The development and implementation of a high-priority system typically would take from one year to 18 months. Having it take one year would not be an indicator that outsourcing would improve the development time. Choices A, C and D would all be indicators that outsourcing selected IS functions may be warranted.

447. A dry-pipe fire extinguisher system is a system that uses:

A. water, but in which water does not enter the pipes until a fire has been detected.
B. water, but in which the pipes are coated with special watertight sealants.
C. carbon dioxide instead of water.
D. halon instead of water.

Answer: A

The dry-pipe sprinkler is an effective and environmentally friendly method of suppressing fire. Water sprinklers, with an automatic power shutoff system, can be set to automatic release without threat to life. Sprinklers must be dry-pipe to prevent the risk of leakage. Halon or carbon dioxide also are used to extinguish fire, but are not used through a dry pipe.

448. The primary role of an IS auditor during the system design phase of an application development project is to:

A. advise on specific and detailed control procedures.
B. ensure the design accurately reflects the requirement.
C. ensure all necessary controls are included in the initial design.
D. advise the development manager on adherence to the schedule.

Answer: C

The duty of the IS auditor is to ensure that required controls are included. Unless specifically present as a consultant, the IS auditor should not be involved in detailed designs. During the design phase, the IS auditor's primary role is to ensure controls are included. Unless there is any potential slippage to report, the IS auditor is not concerned with project control at this stage.

449. In a risk-based audit approach, an IS auditor, in addition to risk, would be influenced by:

A. the availability of CAATs.

B. management's representation.
C. organizational structure and job responsibilities.
D. the existence of internal and operational controls

Answer: D

The existence of internal and operational controls will have a bearing on the IS auditor's approach to the audit. In a risk-based approach the IS auditor is not just relying on risk, but also on internal and operational controls as well as knowledge of the company and the business. This type of risk assessment decision can help relate the cost-benefit analysis of the control to the known risk, allowing practical choices. The nature of available testing techniques and management's representations, have little impact on the risk-based audit approach. Although organizational structure and job responsibilities need to be considered, they are not directly considered unless they impact internal and operational controls.

450. The extent to which data will be collected during an IS audit should be determined, based on the:

A. availability of critical and required information.
B. auditor's familiarity with the circumstances.
C. auditee's ability to find relevant evidence.
D. purpose and scope of the audit being done.

Answer: D

The extent to which data will be collected during an IS audit should be related directly to the scope and purpose of the audit. An audit with a narrow purpose and scope would result most likely in less data collection, than an audit with a wider purpose and scope. The scope of an IS audit should not be constrained by the ease of obtaining the information or by the auditor's familiarity with the area being audited. Collecting all the required evidence is a required element of an IS audit and the scope of the audit should not be limited by the auditee's ability to find relevant evidence.

451. Which of the following would be a MAJOR disadvantage of using prototyping as a systems development methodology?

A. User expectations of project timescales may be overly optimistic.
B. Effective change control and management is impossible to implement.
C. User participation in day-to-day project management may be too extensive.
D. Users usually are not sufficiently knowledgeable to assist in system development.

Answer: A

The fact that prototyping involves demonstrating various external elements of a completed project to users, such as screen layouts and printed reports, may cause a user to believe that the project is closer to completion than it actually is (that underlying programmed processes are also completed). This may result in users having unrealistic expectations of project delivery. Change control may be more difficult, but is certainly not impossible. Users are unlikely to be involved in day-to-day project management, and the whole point of prototyping is that users do usually have sufficient knowledge to assist in system development.

452. When implementing continuous monitoring systems an IS auditor's first step is to identify:

A. reasonable target thresholds.
B. high-risk areas within the organization.
C. the location and format of output files.
D. applications that provide the highest potential payback.

Answer: B

The first and most critical step in the process is to identify high-risk areas within the organization. Business department managers and senior executives are in the best positions to offer insight as to these areas. Once potential areas of implementation have been identified, an assessment of potential impact should be completed to identify applications that provide the highest potential payback to the organization. At this point tests and reasonable target thresholds should be determined prior to programming. During systems development the location and format of the output files generated by the monitoring programs should be defined.

453. When auditing the proposed acquisition of a new computer system, the IS auditor should FIRST establish that:

A. a clear business case has been approved by management.
B. corporate security standards will be met.
C. users will be involved in the implementation plan.
D. the new system will meet all required user functionality.

Answer: A

The first concern of the IS auditor should be to establish that the proposal meets the needs of the business, and this should be established by a clear business case. Although compliance with security standards is essential, as are meeting the needs of the users and having users involved in the implementation process, it is too early in the procurement process for these to be the IS auditor's first concern.

454. In a risk-based audit approach an IS auditor should FIRST complete a/an:

A. inherent risk assessment.
B. control risk assessment.
C. test of control assessment.
D. substantive test assessment.

Answer: A

The first step in a risk-based audit approach is to gather information about the business and industry so as to evaluate the inherent risks. After completing the assessment of the inherent risks the next step would be to complete an assessment of the internal control structure. The controls would then be tested and on the basis of the test results, substantive tests would be carried out and assessed.

455. Which of the following audit procedures would an IS auditor normally perform FIRST when reviewing an organization's systems development methodology?

A. Determine procedural adequacy.
B. Analyze procedural effectiveness.
C. Evaluate level of compliance with procedures.
D. Compare established standards to observed procedures.

Answer: D

The first step should be to establish that the entity being audited meets best practice. The adequacy of the procedures observed should follow confirmation that they meet best practice. Effectiveness analysis will follow establishment of standards. Compliance tests will follow establishment of standards.

456. Which of the following is the MOST fundamental step in effectively preventing a virus attack?

A. Executing updated antivirus software in the background on a periodic basis
B. Buying standard antivirus software, which is installed on all servers and workstations
C. Ensuring that all software is checked for a virus in a separate PC before being loaded into the production environment
D. Adopting a comprehensive antivirus policy and communicating it to all users

Answer: D

The formulation of a comprehensive antivirus policy and education of the users are the most fundamental steps in preventing virus attacks. These provide the broad framework and policy from which relevant operating procedures and practices will be developed. If no policy exists, or the policy is not communicated, ineffective ad hoc procedures may be practiced. The other choices are procedures within the overall policy that direct the measures to be adopted to prevent, detect and recover from virus attacks.

457. An enterprise has established a steering committee to oversee its e-business program. The steering committee would MOST likely be involved in the:

A. documentation of requirements.
B. escalation of project issues.
C. design of interface controls.
D. specification of reports.

Answer: B

The function of the steering committee is to ensure the success of the project. If there are factors or issues that potentially could affect planned results, the steering committee should escalate them. Activities such as documentation of requirements, design of interface controls and specification of reports are the responsibility of the project team.

458. An organization provides information to its supply-chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

A. A secure socket layer (SSL) has been implemented for user authentication and remote administration of the firewall.
B. On the basis of changing requirements, firewall policies are updated.
C. Inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
D. The firewall is placed on top of the commercial operating system with all installation options.

Answer: D

The greatest concern when implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that could undermine the security posture of the firewall platform itself. In most circumstances when commercial firewalls are breached, that breach is facilitated by vulnerabilities in the underlying operating system. Keeping all installation options available on the system further increases the risks of vulnerabilities and exploits. Using SSL for firewall administration (choice A) is important, changes in user and supply chain partners' roles and profiles will be dynamic and it is appropriate to maintain the firewall policies daily (choice B), and it is a prudent policy to block all inbound traffic unless permitted (choice C).

459. When a PC that has been used for the storage of confidential data is sold on the open market the:

A. hard disk should be demagnetized.
B. hard disk should be mid-level formatted.s
C. data on the hard disk should be deleted.
D. data on the hard disk should be defragmented.

Answer: A

The hard disk should be demagnetized since this will cause all of the bits to be set to zero thus eliminating any chance of information, which was previously stored on the disk, being retrieved. A mid-level format does not delete information from the hard disk. It only resets the directory pointers. The deletion of data from the disk removes the pointer to the file, but in actual fact leaves the data in place so, with the proper tools, the information can be retrieved. The defragmentation of the disk does not cause information to be deleted, but simply moves it around to make it more efficient to access.

460. As part of the business continuity planning process, which of the following should be identified FIRST in the business impact analysis (BIA)?

A. Organizational risks, such as single point-of-failure and infrastructure risk
B. Threats to critical business processes
C. Critical business processes for ascertaining the priority for recovery
D. Resources required for resumption of business

Answer: C

The identification of the priority for recovering critical business processes should be addressed first. Organizational risks should be identified next followed by the identification of threats to critical business processes. Identification of resources for business resumption will be done after the tasks mentioned.

461. An organization is introducing a single sign-on (SSO) system. Under the SSO system, users will be required to enter only one user ID and password for access to all application systems. Under the SSO system, unauthorized access:

A. is less likely.
B. is more likely.
C. will have a greater impact.
D. will have a smaller impact.

Answer: C

The impact will be greater since the hacker needs to know only one password to gain access to all systems and can, therefore, cause greater mischief than if only the password to one of the systems is known. Less likely would be the correct answer if the single sign-on system were to be introduced with a stronger form of authentication, such as a smart card/challenge response system. There is no indication that the probability of someone attempting to gain access to systems after introduction of single sign-on is greater than before. The impact can only be greater, not smaller, since the access gained is wider.

462. Which of the following is an implementation risk within the process of decision support systems?

A. Management control
B. Semistructured dimensions
C. Inability to specify purpose and usage patterns
D. Changes in decision processes

Answer: C

The inability to specify purpose and usage patterns is a risk that developers need to anticipate while implementing a decision support system (DSS). Choices A, B and D are not risks, but characteristics of a DSS.

463. Which of the following provides the framework for designing and developing logical access controls?

A. Information systems security policy
B. Access control lists
C. Password management
D. System configuration files

Answer: A

The information systems security policy developed and approved by the top management in an organization is the basis upon which logical access control is designed and developed. Access control lists, password management and systems configuration files are all tools for implementing the access controls.

464. An IS auditor recommends that an initial validation control be programmed into a credit card transaction capture application. The initial validation process would MOST likely:

A. check to ensure the type of transaction is valid for that card type.
B. verify the format of the number entered then locate it on the database.
C. ensure that the transaction entered is within the cardholder's credit limit.
D. confirm that the card is not shown as lost or stolen on the master file.

Answer: B

The initial validation should confirm whether the card is valid. This validity is established through the card number and PIN entered by the user. Based on this initial validation, all other validations will proceed. A validation control in data capture will ensure that the data entered is valid (i.e., it can be processed by the system). If the data captured in the initial validation is not valid (if the card number or PIN do not match with the database), then the card will be rejected or captured per the controls in place.

Once initial validation is completed, then other validations specific to the card and cardholder would be performed.

465. In reviewing the IS short-range (tactical) plan, the IS auditor should determine whether:

A. there is an integration of IS and business staffs within projects.
B. there is a clear definition of the IS mission and vision.
C. there is a strategic information technology planning methodology in place.
D. the plan correlates business objectives to IS goals and objectives.

Answer: A

The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan. Choices B, C, and D are areas covered by a strategic plan.

466. Which of the following would contribute MOST to an effective business continuity plan (BCP)? The BCP:

A. document was circulated to all interested parties.
B. planning involved all user departments.
C. was approved by senior management.
D. was audited by an external IS auditor.

Answer: B

The involvement of user departments in the BCP is crucial for the identification of the business processing priorities. The BCP circulation will ensure that the BCP document is received by all users, though essential, this does not contribute significantly to the success of the BCP. A BCP approved by senior management would not ensure the quality of the BCP, nor would an audit necessarily improve the quality of the BCP.

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

A. reasonable assurance that the audit will cover material items.
B. definite assurance that material items will be covered during the audit work.
C. reasonable assurance that all items will be covered by the audit.
D. sufficient assurance that all items will be covered during the audit work.

Answer: A

"The IS auditing guideline on planning the IS audit states, &quot
As assessment of risk should be made to provide reasonable assurance that material items will be adequately covered during the audit work. This assessment should identify areas with relatively high risk of existence of material problems.&quot
Definite assurance that material items will be covered during the audit work is an impractical proposition. Reasonable assurance that all items will be covered during the audit work is not the correct answer as material items need to be covered, not all items."

468. Which of the following processes describes risk assessment? Risk assessment is:

A. subjective.
B. objective.
C. mathematical.
D. statistical.

Answer: A

"The IS auditing guideline on the use of a risk assessment in audit planning states, &quot
All risk assessment methodologies rely on subjective judgments at some point in the process (e.g., for assigning weightings to the various parameters). The IS auditor should identify the subjective decisions required in order to use a particular methodology and consider whether these judgments can be made and validated to an appropriate level of accuracy.&quot
"

469. An IS auditor conducting a review of disaster recovery planning at a financial processing organization has discovered the following:
The existing disaster recovery plan was compiled two years ago by a systems analyst in the organization's IT department using transaction flow projections from the operations department.<li>The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting his 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 their 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. The IS auditor should:

A. take no action as the lack of a current plan is the only significant finding.
B. recommend that the hardware configuration at each site should be identical.
C. perform a review to verify that the second configuration can support live processing.
D. report that the financial expenditure on the alternative site is wasted without an effective plan.

Answer: C

The IS auditor does not have a finding unless it can be shown that the alternative hardware cannot support the live processing system. Even though the primary finding is the lack of a proven and communicated disaster recovery plan, it is essential that this aspect of recovery is included in the audit. Since, if it is found to be inadequate the finding will materially support the overall audit opinion. It is certainly not appropriate to take no action at all, leaving this important factor untested, and unless it is shown that the alternative site is inadequate, there can be no comment on the expenditure (even if this is considered a proper comment for the IS auditor to make). Similarly, there is no need for the configurations to be identical. The alternative site could actually exceed the recovery requirements if it is also used for other work, such as other processing or systems development and testing. The only proper course of action at this point would be to find out if the recovery site can actually cope with a recovery.

470. An IS auditor is reviewing the database administration function to ascertain whether adequate provision has been made for controlling data. The IS auditor should determine that the:

A. function reports to data processing operations.
B. responsibilities of the function are well defined.
C. database administrator is a competent systems programmer.
D. audit software has the capability of efficiently accessing the database.

Answer: B

The IS auditor should determine that the responsibilities of the database administration function are not only well defined but also assure that the database administrator (DBA) reports directly to the IS manager or executive to provide independence, authority and responsibility. The DBA should not report to either data processing operations or systems development management. The DBA need not be a competent systems programmer. Choice D is not as important as choice A.

471. A web-based bookstore has included the customer relationship management (CRM) system in its operations. An IS auditor has been assigned to perform a call center review. Which of the following is the MOST appropriate first step for the IS auditor to take?

A. Review the company's performance since the CRM was implemented.
B. Review the IT strategy.
C. Understand the business focus of the bookstore.
D. Interview salespeople and supervisors.

Answer: C

The IS auditor should first understand the business drivers of the CRM implementation. Choices A, B and D are not appropriate first steps.

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

A. Design further tests of the calculations that are in error.

B. Identify variables that may have caused the test results to be inaccurate.
C. Examine some of the test cases to confirm the results.
D. Document the results and prepare a report of findings, conclusions and recommendations.

Answer: C

The IS auditor should next examine cases where incorrect calculations occurred and confirm the results. After the calculations have been confirmed, further tests can be conducted and reviewed. Report preparation, findings and recommendations would not be made until all results are confirmed.

473. An IS auditor's MAJOR concern as a result of reviewing a business process reengineering (BPR) project should be whether the:

A. newly designed business process has key controls in place.
B. changed process will affect organization structure, finances and personnel.
C. roles for suppliers have been redefined.
D. process has been documented before and after reengineering.

Answer: A

The IS auditor should review the redesigned process, assess the risks, evaluate the controls and recommend the inclusion, if appropriate, of additional controls. Whether the changed process affects organizational structure, finances and personnel, is a concern for the change management team. The redefinition of roles for suppliers is normally outside the scope of a BPR project. Choice D is an important task but not as critical as a strong control environment.

474. An IS auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late-night shift a month as the senior computer operator. The MOST appropriate course of action for the IS auditor is to:

A. advise senior management of the risk involved.
B. agree to work with the security officer on these shifts as a form of preventative control.
C. develop a computer-assisted audit technique to detect instances of abuses of this arrangement.
D. review the system log for each of the late-night shifts to determine whether any irregular actions occurred.

Answer: A

The IS auditor's first and foremost responsibility is to advise senior management of the risk involved in having the security administrator perform an operations function. This is a violation of separation of duties. The IS auditor should not get involved in processing.

475. When reviewing the quality of an IS department's development process, the IS auditor finds that they do not use any formal, documented methodology and standards. The IS auditor's MOST appropriate action would be to:

A. complete the audit and report the finding.
B. investigate and recommend appropriate formal standards.
C. document the informal standards and test for compliance.
D. withdraw and recommend a further audit when standards are implemented.

Answer: C

The IS auditor's first concern would be to ensure that projects are consistently managed. Where it is claimed that an internal standard exists, it is important to ensure that it is operated correctly, even when this means documenting the claimed standards first. Merely reporting the issue as a weakness and closing the audit without findings would not help the organization in any way and investigating formal methodologies may be unnecessary if the existing, informal standards prove to be adequate and effective.

476. Which of the following is the FIRST thing an IS auditor should do after the discovery of a trojan horse program in a computer system?

A. Investigate the author.

B. Remove any underlying threats.
C. Establish compensating controls.
D. Have the offending code removed.

Answer: D

The IS auditor's first duty is to prevent the trojan horse from causing further damage. After removing the offending code, follow up actions would include investigation and recommendations (choices B and C).

477. Once an organization has finished the business process reengineering (BPR) of all its critical operations, the IS auditor would MOST likely focus on a review of:

A. pre-BPR process flowcharts.
B. post-BPR process flowcharts.
C. BPR project plans.
D. continuous improvement and monitoring plans.

Answer: B

The IS auditor's task is to identify and ensure that key controls have been incorporated into the reengineered process. Choice A is incorrect because an IS auditor must review the process as it is today, not as it was in the past. Choices C and D are incorrect because they are steps within a BPR project.

478. Which of the following would an IS auditor consider the MOST relevant to short-term planning for the IS department?

A. Allocating resources
B. Keeping current with technology advances
C. Conducting control self-assessment
D. Evaluating hardware needs

Answer: A

The IS department should specifically consider the manner in which resources are allocated in the short term. Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake. Conducting control self-assessments and evaluating hardware needs are not as critical as allocating resources during short-term planning for the IS department

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

A. Monitoring vendor controlled change control and testing
B. Ensuring a separation of duties within the information's processing environment
C. Approving and monitoring major projects, the status of IS plans and budgets
D. Responsible for liaison between the IS department and the end users

Answer: C

The IS steering committee typically serves as a general review board for major IS projects and should not become involved in routine operations, therefore, one of its functions is to approve and monitor major projects, the status of IS plans and budgets. Vendor change control is an outsourcing issue and should be monitored by IS management. Ensuring a separation of duties within the information's processing environment is an IS management responsibility. Liaison between the IS department and the end users is a function of the individual parties and not a committee.

480. An IS auditor reviewing an organization's IT strategic plan should FIRST review:

A. the existing IT environment.
B. the business plan.
C. the present IT budget.
D. current technology trends.

Answer: B

The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, the IS auditor would first need to familiarize him/herself with the business plan.

481. The key difference between a microwave radio system and a satellite radiolink system is that:

A. microwave uses line-of-sight and satellite uses transponders during transmission.
B. microwave operates through transponders placed on the earth's orbit.
C. satellite uses line-of-sight during transmission.
D. microwave uses fiber optic cables.

Answer: A

The key difference between a microwave radio system and satellite radiolink system is that microwave transmits along the line-of-sight, while a satellite radiolink system operates through transponders placed on the earth's orbit and a microwave radio system operates on land along the line of sight. Both microwave and satellite use electromagnetic radiation and not fiber optic cables for their communication.

482. Which of the following provisions in a contract for external information systems services would an IS auditor consider to be LEAST significant?

A. Ownership of program and files
B. Statement of due care and confidentiality
C. Continued service of outsourcer in the event of a disaster
D. Detailed description of computer hardware used by the vendor

Answer: D

The least significant would be the description of computer hardware. The organization would need to have compatible and sufficient hardware to be considered a viable service provider before contract provisions are reviewed.

483. Of the following, the MAIN purpose for periodically testing offsite backup facilities is to:

A. ensure the integrity of the data in the database.
B. eliminate the need to develop detailed contingency plans.
C. ensure the continued compatibility of the contingency facilities.
D. ensure that program and system documentation remains current.

Answer: C

The main purpose of offsite hardware testing is to ensure the continued compatibility of the contingency facilities. Specific software tools are available to ensure the ongoing integrity of the database. Contingency plans should not be eliminated and program and system documentation should be reviewed continuously for currency.

484. An IS auditor performing an application maintenance audit would review the log of program changes for the:

A. authorization for program changes.
B. creation date of a current object module.
C. number of program changes actually made.
D. creation date of a current source program.

Answer: A

The manual log will most likely contain information on authorized changes to a program. Deliberate, unauthorized changes will not be documented by the responsible party. An automated log, found usually in library management products, and not a change log would most likely contain date information for the source and executable modules.

485. A digital signature contains a message digest to:

A. show if the message has been altered after transmission.

B. define the encryption algorithm.
C. confirm the identity of the originator.
D. enable message transmission in a digital format.

Answer: A

The message digest is calculated and included in a digital signature to prove that the message has not been altered. It should be the same value as a recalculation performed upon receipt. It does not define the algorithm or enable the transmission in digital format and has no effect on the identity of the user, being there to ensure integrity rather than identity.

486. Facilitating telecommunications continuity by providing redundant combinations of local carrier T-1 lines, microwaves and/or coaxial cables to access the local communication loop is:

A. last mile circuit protection.
B. long haul network diversity.
C. diverse routing.
D. alternative routing.

Answer: A

The method of providing telecommunication continuity through the use of many recovery facilities providing redundant combinations of local carrier T-1s, microwave and/or coaxial cable to access the local communication loop in the event of a disaster is called last mile circuit protection. Providing diverse long-distance network availabilty utilizing T-1 circuits among major long-distance carriers is called long haul network diversity. This ensures long-distance access should any one carrier experience a network failure. The method of routing traffic through split cable facilities or duplicate cable facilities is called diverse routing. Alternative routing is the method of routing information via an alternative medium, such as copper cable or fiber optics.

487. Large-scale systems development efforts:

A. are not affected by the use of prototyping tools.
B. can be carried out independent of other organizational practices.
C. require that business requirements be defined before the project begins.
D. require that project phases and deliverables be defined during the duration of the project.

Answer: C

The methodology used should provide for business requirements to be clearly defined before approval of any development, implementation or modification project. The phases and deliverables should be decided during the early planning stages of the project and not throughout its duration. The phases necessary to complete the project depend on its size and the type of tolls being used by the project team (e.g., prototyping tools) In addition, the selected methodology must fit to a particular organization's practices and size.

488. To prevent unauthorized entry to the data maintained in a dial-up fast response system, an IS auditor should recommend:

A. online terminals be placed in restricted areas.
B. online terminals be equipped with key locks.
C. ID cards be required to gain access to online terminals.
D. online access be terminated after three unsuccessful attempts.

Answer: D

The most appropriate control to prevent unauthorized entry is to terminate connection after a specified number of attempts. This will deter access through the guessing of ids and passwords. The other choices are physical controls, which are not effective in deterring unauthorized accesses via the telephone lines.

489. Which of the following controls would be the MOST comprehensive in a remote access network with multiple and diverse subsystems?

A. Proxy server

B. Firewall installation
C. Network administrator
D. Password implementation and administration

Answer: D

The most comprehensive control in this situation is password implementation and administration. While firewall installations are the primary line of defense, they cannot protect all access and, therefore, an element of risk remains. A proxy server is a type of firewall installation and thus the same rules apply. The network administrator may serve as a control, but typically this would not be comprehensive enough to serve on multiple and diverse systems.

490. In planning a software development project, which of the following is the MOST difficult to determine?

A. Project slack times
B. The project's critical path
C. Time and resource requirements for individual tasks
D. Relationships that preclude the start of an activity before others are complete

Answer: C

"The most difficult problem is effectively estimating a project's slack time and/or resource requirements for individual tasks or development activities. This commonly is done through direct software measures (size-oriented SLOC-source lines of code
KLOC-thousand lines of code) or indirect software measures (function points-values for number of user inputs, outputs, inquiries
number of files and interfaces). The other choices are project management methods and techniques employed that are dependent on the effectiveness of methods used in deriving accurate and reliable software development productivity and performance measures."

491. 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?

A. Review software migration records and verify approvals.
B. Identify changes that have occurred and verify approvals.
C. Review change control documentation and verify approvals.
D. Ensure that only appropriate staff can migrate changes into production.

Answer: B

The most effective method is to determine through code comparisons what changes have been made and then verify that they have been approved. Change control records and software migration records may not have all changes listed. Ensuring that only appropriate staff can migrate changes into production is a key control process, but in itself does not verify compliance.

492. When reviewing a system development project an IS auditor would be PRIMARILY concerned with whether:

A. business objectives are achieved.
B. security and control procedures are adequate.
C. the system utilizes the strategic technical infrastructure.
D. development will comply with the approved quality management processes

Answer: A

The most important issue in reviewing system development processes to ensure that business objectives are achieved. A software development project should meet its objectives. Security and control procedures are to be considered as a subset of business objectives, because a well-controlled system that does not meet business needs is of little benefit to the organization.

493. Which of the following audit procedures would MOST likely be used in an audit of a systems development project?

A. Develop test transactions
B. Use code comparison utilities
C. Develop audit software programs
D. Review functional requirements documentation

Answer: D

"The most likely audit procedure in systems development is the review of the functional requirements, since this will indicate what the new system is supposed to provide and how. Based on this documentation other testing may be performed to confirm that the necessary controls and functionality are in place. The development of test transactions also may be performed if necessary however, this would be to assist functional requirements testing. The use of code comparison utilities compares two copies of the source code to identify differences and would normally be used for system maintenance. Audit software programs are normally used to integrate production data, thus it would not be appropriate for a system under development."

494. 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?

A. Virtual private network
B. Dedicated line
C. Leased line
D. Integrated services digital network

Answer: A

The most secure way would be a virtual private network (VPN) using encryption, authentication and tunneling to allow data to travel securely from a private network to the Internet. Choices B, C and D are network connectivity options, which are normally too expensive to be practical for small- to medium-sized organizations.

495. Which of the ISO/OSI model layers provides for routing packets between nodes?

A. Data link
B. Network
C. Transport
D. Session

Answer: B

The network layer switches and routes information (network layer header). Node-to-node data link services are extended across a network by this layer. The network layer provides service for routing packets (units of information at the network layer) between nodes connected through an arbitrary network. The data link layer transmits information as groups-of-bits (logical units called a frame) to adjacent computer systems (node-to-node). The bits in a frame are divided into an address field (media access control MAC 48 bit hardware address), control field, data field and error control field. The transport layer, provides end-to-end data integrity. To ensure reliable delivery, the transport layer builds on the error control mechanisms provided by lower layers. If lower layers do not do an adequate job, the transport layer is the last chance for error recovery. The session layer provides the control structure for communications between applications. It establishes, manages and terminates connections (sessions) between cooperating applications and performs access security checking.

496. The difference between a vulnerability assessment and a penetration test is that a vulnerability assessment:

A. 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.
B. and penetration tests are different names for the same activity.
C. is executed by automated tools, whereas penetration testing is a totally manual process.
D. is executed by commercial tools, whereas penetration testing is executed by public processes.

Answer: A

"The objective of a vulnerability assessment is to find the security holds in the computers and elements analyzed and its intent is not to damage the infrastructure. The intent of penetration testing is to imitate a hacker's activities and determine how far they could go into the network. They are not the same they have different approaches. Vulnerability assessments and penetration testing can be executed both by automated or manual tools or processes and can be executed by commercial or free tools."

497. The objective of IT governance is to ensure that the IT strategy is aligned with the objectives of (the):

A. enterprise.
B. IT.
C. audit.
D. finance.

Answer: A

The objective of IT governance is to ensure that the IT strategy is aligned with the enterprise/business objectives. Choices B, C, D are not the main objectives.

498. Which of the following is an objective of a control self-assessment (CSA) program?

A. Concentration on areas of high risk
B. Replacement of audit responsibilities
C. Completion of control questionnaires
D. Collaborative facilitative workshops

Answer: A

The objectives of CSA programs include education for line management in control responsibility and monitoring and concentration by all on areas of high risk. The objectives of CSA programs include the enhancement of audit responsibilities, not replacement of audit responsibilities. Choices C and D are tools of CSA, not objectives.

499. Which of the following offsite information processing facility conditions would cause an IS auditor the GREATEST concern? The facility

A. is identified clearly on the outside with the company name.
B. is located more than an hour driving distance from the originating site.
C. does not have any windows to let in natural sunlight.
D. entrance is located in the back of the building rather than the front.

Answer: A

The offsite facility should not be easily identified from the outside. Signs identifying the company and the contents of the facility should not be present. This is to prevent intentional sabotage of the offsite facility should the destruction of the originating site be from malicious attack. The offsite facility should not be subject to the same natural disaster that affected the originating site. The offsite facility must also be secured and controlled just as the originating site. This includes adequate physical access controls, such as locked doors, no windows and human surveillance.

500. An organization has been an Internet user for several years and the business plan now calls for initiating e-commerce via web-based transactions. Which of the following will LEAST impact transactions in e-commerce?

A. Encryption is required
B. Timed authentication is required
C. Firewall architecture hides the internal network
D. Traffic is exchanged through the firewall at the application layer only

Answer: C

The only control that does not directly impact the e-commerce transactions is the actual architecture of the firewall and whether or not it hides the internal network. All other options are key requirements for ensuring security transactions in e-commerce. The use of encryption will have an impact on the system

performance as transactions go through the encryption/decryption process. Timed authentication requires that a response is received within a specific amount of time, which will have an effect on system performance. The exchange of traffic will have an effect on system performance.

501. An IS auditor discovers evidence of fraud perpetrated with a manager's user id. The manager had written the password, allocated by the system administrator, inside his/her desk drawer. The IS auditor should conclude that the:

A. manager's assistant perpetrated the fraud.
B. perpetrator cannot be established beyond doubt.
C. fraud must have been perpetrated by the manager.
D. system administrator perpetrated the fraud.

Answer: B

The password control weaknesses means that any of the other three options could be true. Password security would normally identify the perpetrator. In this case, it does not establish guilt beyond doubt.

502. The PRIMARY reason for replacing checks (cheques) with EFT systems in the accounts payable area is to:

A. make the payment process more efficient.
B. comply with international EFT banking standards.
C. decrease the number of paper-based payment forms.
D. reduce the risk of unauthorized changes to payment transactions.

Answer: A

The payment process is more efficient because it involves virtually no manual intervention. This reduces the chance that transcription errors will occur as the information is entered into the accounts payable system. International EFT banking standards do not dictate the form that transactions should take. The decrease in the number of paper-based payment forms makes processing easier, but most companies will accept payment in whichever form the customer is willing to use. The reduction of unauthorized changes to payment transactions is not a major reason for going to EFT.

503. At the end of a simulation of an operational contingency test, the IS auditor performed a review of the recovery process. The IS auditor concluded that the recovery took more than the critical time frame allows. Which of the following actions should the auditor recommend?

A. Widen the physical capacity to accomplish better mobility in a shorter time.
B. Shorten the distance to reach the hot site.
C. Perform an integral review of the recovery tasks.
D. Increase the number of human resources involved in the recovery process.

Answer: C

The performance of an exhaustive review of the recovery tasks would be appropriate to determine time invested in each task and the way each was conducted. This would allow the individual responsible for the test to adjust the time assigned for the recovery tasks. The other choices could be conclusions, once the first analysis was made.

504. Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

A. The use of diskless workstations
B. Periodic checking of hard drives
C. The use of current antivirus software
D. Policies that result in instant dismissal if violated

Answer: B

The periodic checking of hard drives would be the most effective method of identifying illegal software packages loaded to the network. Antivirus software will not necessarily identify illegal software unless the software contains a virus. Diskless workstations act as a preventative control and are not effective since

users could still download software from other than diskless workstations. Policies lay out the rules about loading the software, but will not detect the actual occurrence.

505. An IS auditor reviewing an organization's IS disaster recovery plan should verify that it is:

A. tested every 6 months.
B. regularly reviewed and updated.
C. approved by the chief executive officer (CEO).
D. communicated to every departmental head in the organization.

Answer: B

The plan should be reviewed at appropriate intervals, depending upon the nature of the business and the rate of change of systems and personnel, otherwise it may become out of date and may no longer be effective. The plan must be subjected to regular testing, but the period between tests will again depend on the nature of the organization and the relative importance of IS. Three months or even annually may be appropriate in different circumstances. Although the disaster recovery plan should receive the approval of senior management, it need not be the CEO if another executive officer is equally, or more appropriate. For a purely IS-related plan, the executive responsible for technology may have approved the plan. Similarly, although a business continuity plan is likely to be circulated throughout an organization, the IS disaster recovery plan will usually be a technical document and only relevant to IS and communications staff.

506. In a system development project the purpose of the program and procedure development phase is to:

A. prepare, test and document all programs and manual procedures.
B. document a business or system problem to a level at which management can select a solution.
C. prepare a high-level design of a proposed system solution and present reasons for adopting a solution.
D. expand the general design of an approved solution so that program and procedure writing can begin.

Answer: A

The preparation, testing, and documentation of all computer programs and manual procedures best relate to the program and procedure development phase. Choices B, C and D relate to earlier phases of the system development life cycle.

507. 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 are necessary to restore these files?

A. The previous day's backup file and the current transaction tape
B. The previous day's transaction file and the current transaction tape
C. The current transaction tape and the current hard-copy transaction log
D. The current hard-copy transaction log and the previous day's transaction file

Answer: A

The previous day's backup will be the most current historical backup of activity in the system. The current day's transaction file will contain all of the day's activity. Therefore, the combination of these two files will enable full recovery up to the point of interruption.

508. An IS auditor conducting a review of disaster recovery planning at a financial processing organization has discovered the following:
The existing disaster recovery plan was compiled two years ago by a systems analyst in the organization's IT department using transaction flow projections from the operations department.<li>The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting his 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 their area in the event of a disruptive incident.
The IS auditor's report should recommend that:

A. the deputy CEO be censured for his failure to approve the plan.

B. a board of senior managers be set up to review the existing plan.
C. the existing plan be approved and circulated to all key management and staff.
D. a manager coordinate the creation of a new or revised plan within a defined time limit.

Answer: D

The primary concern is to establish a workable disaster recovery plan, which reflects current processing volumes to protect the organization from any disruptive incident. Censuring the deputy CEO will not achieve this and is generally not within the scope of an IS auditor to recommend. Establishing a board to review the plan, which is two years out of date, may achieve an updated plan, but is not likely to be a speedy operation and issuing the existing plan would be folly without first ensuring that it is workable. The best way to achieve a disaster recovery plan in a short timescale is to make an experienced manager responsible for coordinating the knowledge of other managers into a single, formal document within a defined time limit.

509. The PRIMARY objective of an IS audit function is to:

A. determine whether everyone uses IS resources according to their job description.
B. determine whether information systems safeguard assets, and maintain data integrity.
C. examine books of accounts and relative documentary evidence for the computerized system.
D. determine the ability of the organization to detect fraud.

Answer: B

The primary reason for conducting IS audits is to determine whether a system safeguards assets and maintains data integrity. Examining books of accounts is one of the processes involved in IS audit but it is not the primary purpose. Detecting frauds could be a result of an IS audit but is not the purpose for which an IS audit is performed.

510. 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?

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

Answer: A

The primary responsibility of the IS auditor is to assure that the company assets are being safeguarded. This is true even if the assets do not reside on the immediate premises. Reputable service bureaus will have a well-designed and tested business continuity plan.

511. A MAJOR risk of using single sign-on (SSO) is that it:

A. has a single authentication point.
B. represents a single point of failure.
C. causes an administrative bottleneck.
D. leads to a lockout of valid users.

Answer: A

The primary risk associated with single sign-on is the single authentication point. If a password is compromised, access to many applications can be obtained without further verification. A single point of failure provides a similar redundancy to the single authentication point. However, failure can occur at multiple points, such as, data, process or network. An administrative bottleneck may result when the administration is centralized in a single step entry system. This is therefore an advantage. User lockout can occur with any password authentication system and normally is remedied swiftly by the security administrator resetting the account.

512. In an online transaction processing system, data integrity is maintained by ensuring that a transaction is either completed in its entirety or not at all. This principle of data integrity is known as:

A. isolation.
B. consistency.
C. atomicity.
D. durability.

Answer: C

The principle of atomicity requires that a transaction be completed in its entirety or not at all. If an error or interruption occurs, all changes made up to that point are backed out. Consistency ensures that all integrity conditions in the database be maintained with each transaction. Isolation ensures that each transaction is isolated from other transactions, and hence, each transaction only accesses data that are part of a consistent database state. Durability ensures that when a transaction has been reported back to a user as complete the resultant changes to the database will survive subsequent hardware or software failures.

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

A. confidentiality and integrity.
B. security and nonrepudiation.
C. integrity and nonrepudiation.
D. confidentiality and nonrepudiation.

Answer: C

The process of applying a mathematical algorithm to the data that travels in the network and placing the results of this operation with the hash data is used for controlling data integrity, since any unauthorized modification to this data would result in a be different hash. The application of a digital signature would accomplish the nonrepudiation of the delivery of the message. The term security is a broad concept and not a specific one. In addition to a hash and a digital signature, confidentiality is applied when an encryption process exists.

514. Failure to adequately define or manage the requirements for a system can result in a number of risks. The GREATEST risk is:

A. inadequate user involvement.
B. inadequate allocation of resources.
C. scope creep.
D. an incorrect estimation of the critical path.

Answer: C

The process through which requirements change (scope creep) is considered the greatest risk. Changes in the requirements will impact development schedules/resources. Inadequate user involvement may have been the cause but it is not the resulting risk. Inadequate allocation of resources is a tied to the proficiency of the project manager. The inaccurate estimation of the critical path is not as great a risk as scope creep.

515. In the development of an important application affecting the entire organization, which of the following would be the MOST appropriate project sponsor?

A. The information systems manager
B. A member of executive management
C. An independent management consultant
D. The manager of the key user department

Answer: B

The project sponsor puts his/her name on a project to emphasize its importance to the organization, and to ensure the commitment and cooperation of management. Where the development is both important, and affects the entire organization, the sponsor must be of sufficient corporate standing to require such cooperation. Therefore, a member of the executive team is most appropriate. The manager of a department may not command automatic support from peers, and the IS manager and an independent consultant are inappropriate sponsors of such a development.

516. Which of the following group/individuals should assume overall direction and responsibility for costs and timetables of system development projects?

A. User management
B. Project steering committee
C. Senior management
D. Systems development management

Answer: B

The project steering committee is ultimately responsible for all costs and timetables. User management assumes ownership of the project and the resulting system. Senior management commits to the project and approves the resources necessary to complete the project. System development management provides technical support for the hardware and software environments by developing, installing and operating the requested system.

517. A primary reason for an IS auditor's involvement in the development of a new application system is to ensure that:

A. adequate controls are built into the system.
B. user requirements are satisfied by the system.
C. sufficient hardware is available to process the system.
D. data are being developed for pre-implementation testing of the system.

Answer: A

The provision of controls is the primary reason for audit involvement.

518. Which of the following is LEAST likely to be contained in a digital certificate for the purposes of verification by a trusted third party (TTP)/certification authority (CA)?

A. Name of the TTP/CA
B. Public key of the sender
C. Name of the public key holder
D. Time period for which the key is valid

Answer: C

The public key is stored in the key servers and can be accessed by anyone, and therefore, the holders of the public key are unlikely to be included in the certificate. In addition, the public key holder is not needed for validation of the certificate. The name of the CA is needed for validation of the certificate, since the public key of the CA is needed to verify the public key of the message sender, before it can be used to verify the message. The public key of the sender is needed to verify the message hash, while the time period for which the key is valid is needed to ensure the key is still valid.

519. Which of the following is critical to the selection and acquisition of the correct operating system software?

A. Competitive bids
B. User department approval
C. Hardware-configuration analysis
D. Purchasing department approval

Answer: C

The purchase of operating system software is dependent on the fact that software is compatible with existing hardware. Choices A and D, although important, are not as important as choice C. Users do not normally approve the acquisition of operating systems software.

520. The purpose of debugging programs is to:

A. generate random data that can be used to test programs before implementing them.
B. protect valid changes from being overwritten by other changes during programming.

C. define the program development and maintenance costs to be include in the feasibility study.
D. ensure that abnormal terminations and coding flaws are detected and corrected.

Answer: D

The purpose of debugging programs is to ensure that program abends and coding flaws are detected and corrected before the final program goes into production. There are special tools, such as logic paths monitors, memory dumps and output analyzers, to aid the debugging efforts.

521. Which of the following is the primary purpose for conducting parallel testing?

A. To determine if the system is cost-effective.
B. To enable comprehensive unit and system testing.
C. To highlight errors in the program interfaces with files.
D. To ensure the new system meets user requirements.

Answer: D

The purpose of parallel testing is to ensure the implementation of a new system will meet user requirements. Parallel testing may show that the old system is, in fact, better than the new system, but this is not the primary reason. Unit and system testing will be completed before parallel testing. Errors in program interfaces with files will be tested during system testing.

522. The quality assurance group is typically responsible for:

A. ensuring that the output received from system processing is complete.
B. monitoring the execution of computer processing tasks.
C. ensuring that programs and program changes and documentation adhere to established standards.
D. designing procedures to protect data against accidental disclosure, modification or destruction.

Answer: C

The quality assurance group is typically responsible for ensuring that programs, program changes and documentation adhere to established standards. Choice A is the responsibility of the data control group, choice B is the responsibility of computer operations, and choice D is the responsibility of data security.

523. The PKI element that manages the certificate life cycle, including certificate directory maintenance and certificate revocation list (CRL) maintenance and publication is the:

A. certificate authority.
B. digital certificate.
C. certification practice statement.
D. registration authority.

Answer: D

The registration authority manages the certificate life cycle, including certificate directory maintenance and certificate revocation list (CRL) maintenance and publication. The certificate authority attests, as a trusted provider of the public/private key pairs, to the authenticity of the owner to whom a public/private key pair has been given. The digital certificate is composed of a public key together with identifying information about the owner of the public key. It associates a public key with an individual's identity. Certificates are e-documents digitally signed by a trusted entity containing information on individuals. The process entails the sender digitally signing a document with the digital certificate attached issued by a trusted entity where the receiver relies on the public key that is included in the digital certificate to authenticate the message. The certification practice statement is the governance process for CA operations.

524. Which of the following has the LEAST effect on controlling physical access?

A. Access to the work area is restricted through a swipe card.
B. All physical assets have an identification tag and are properly recorded.
C. Access to the premises is restricted and all visitors authorized for entry.
D. Visitors are issued a pass and escorted in and out by a concerned employee.

Answer: B

The requirement that all physical assets have an identification tag and are recorded properly is an effective procedure for recording and monitoring assets. This is not directly related to physical access control, although they do facilitate implementing physical access controls. The other choices are access controls that control and monitor physical access.

525. An IS auditor should be concerned when a telecommunication analyst:

A. monitors systems performance and tracks problems resulting from program changes.
B. reviews network load requirements in terms of current and future transaction volumes.
C. assesses the impact of the network load on terminal response times and network data transfer rates.
D. recommends network balancing procedures and improvements.

Answer: A

The responsibilities of a telecommunications analyst include reviewing network load requirements in terms of current and future transaction volumes (choice B), assessing the impact of network load or terminal response times and network data transfer rates (choice C) and recommending network balancing procedures and improvements (choice D). Monitoring systems performance and tracking problems as a result of program changes (choice A) would put the analyst in a self-monitoring role.

526. Which of the following LAN physical layouts is subject to total loss if one device fails?

A. Star
B. Bus
C. Ring
D. Completely connected

Answer: C

The ring network is vulnerable to failure if one device fails.

527. Which of the following is a benefit of a risk-based approach to audit planning? Audit:

A. scheduling may be performed months in advance.
B. budgets are more likely to be met by the IS audit staff.
C. staff will be exposed to a variety of technologies.
D. resources are allocated to the areas of highest concern.

Answer: D

The risk-based approach is designed to ensure audit time is spent on the areas of highest risk. The development of an audit schedule is not addressed by a risk-based approach. Audit schedules may be prepared months in advance using various scheduling methods. A risk approach does not have a direct correlation to the audit staff meeting time budgets on a particular audit, nor does it necessarily mean a wider variety of audits will be performed in a given year.

528. The PRIMARY objective of a logical access controls review is to:

A. review access controls provided through software.
B. ensure access is granted per the organization's authorities.
C. walkthrough and assess access provided in the IT environment.
D. provide assurance that computer hardware is protected adequately against abuse.

Answer: B

The scope of a logical access controls review is primarily to determine whether or not access is granted as per the organization's authorizations. Choices A and C relate to procedures of a logical access controls review, rather than objectives. Choice D is relevant to a physical access control review.

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

A. encryption key bits.

B. messages sent.
C. keys.
D. channels used.

Answer: A

The security level of a private key system depends on the number of encryption key bits. The larger the number of bits, the more difficult it would be to understand or determine the algorithm. The security of the message will depend on the encryption key bits used. More than keys by themselves, it's the algorithm and its complexity, which make the content more secured. Channels, which could be open or secure, are the mode for sending the message.

530. Which of the following should be included in an organization's IS security policy?

A. A list of key IT resources to be secured
B. The basis for access authorization
C. Identity of sensitive security features
D. Relevant software security features

Answer: B

The security policy provides the broad framework of security, as laid down and approved by the senior management. It includes a definition of those authorized to grant access and the basis for granting the access. Choices A, B and C are more detailed than that which should be included in a policy.

531. In the ISO/OSI model, which of the following protocols is the FIRST to establish security for the user application?

A. Session layer.
B. Transport layer
C. Network layer
D. Presentation layer

Answer: A

The session layer provides functions that allow two applications to communicate across the network. The functions include security, recognition of names, logons and so on. The session layer is the first layer where security is established for user applications. The transportation layer provides transparent transfer of data between end points. The network layer controls the packet routing and switching within the network, as well as to any other network. The presentation layer provides common communication services, such as encryption, text compression and reformatting.

532. Which of the following protocols would be involved in the implementation of a router and interconnectivity device monitoring system?

A. Simple network management
B. File transfer
C. Simple Mail Transfer Protocol
D. Telnet

Answer: A

The simple network management protocol provides a means to monitor and control network devices and to manage configurations and performance. The file transfer protocol (FTP), transfers files from a computer on the Internet to the user's computer and does not have any functionality related to monitoring network devices. Simple Mail Transfer Protocol (SMTP) is a protocol for sending and receiving e-mail messages and does not provide any monitoring or management for network devices. Telnet is a standard terminal emulation protocol used for remote terminal connections, enabling users to log into remote systems and use resources as if they were connected to a local system and does not provide any monitoring or management of network devices.

533. 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?

A. Appliances
B. Operating system based
C. Host based
D. Demilitarized

Answer: A

The software for appliances is embedded into chips. Firmware-based firewall products cannot be moved to higher capacity servers. Firewall software that sits on an operating system always can be scalable due to the ability to enhance the power of servers. Host-based firewalls operate on top of the server operating system and can be scalable. A demilitarized zone is a model of firewalls implementation and is not a firewall architecture.

534. Which of the following is a concern when data is transmitted through secure socket layer (SSL) encryption implemented on a trading partner's server?

A. Organization does not have control over encryption.
B. Messages are subjected to wire tapping.
C. Data might not reach the intended recipient.
D. The communication may not be secure.

Answer: A

The SSL security protocol provides data encryption, server authentication, message integrity and optional client authentication. Because SSL is built into all major browsers and web servers, simply installing a digital certificate turns on the SSL capabilities. SSL encrypts the data while it is being transmitted over the Internet. The encryption is done in the background, without any interaction from the user, consequently there's no password to remember either. The other choices are incorrect. Since the communication between client and server is encrypted, the confidentiality of information is not affected by wire tapping. Since SSL does the client authentication, only the intended recipient will receive the decrypted data. All data sent over an encrypted SSL connection is protected with a mechanism to detect tampering, that is, automatically determining whether data has been altered in transit.

535. The responsibility, authority and accountability of the IS audit function is documented appropriately in an audit charter and MUST be:

A. approved by the highest level of management.
B. approved by audit department management.
C. approved by user department management.
D. changed every year before commencement of IS audits.

Answer: A

"The standard on responsibility, authority and accountability states, &quot
The responsibility, authority and accountability of the information systems audit function are to be appropriately documented in an audit charter or engagement letter.&quot
Choice B and C are incorrect because the audit charter should be approved by the highest level of management, not merely by the information systems audit department, or the user department. The resulting planning methodologies should be reviewed and approved by senior management and by the audit committee. Choice D is incorrect because the audit charter, once established, is not routinely revised and should be changed only if change can be, and is, throughly justified."

536. In which of the following network configurations would problem resolution be the easiest?

A. Bus
B. Ring
C.Star
D. Mesh

Answer: C

The star configuration would be the easiest network for problem resolution. In a star configuration all lines are connected to the central hub. A problem can occur if the central hub fails. A bus configuration

can be difficult to troubleshoot since a cable break can be difficult to find. Ring configurations are also difficult to trouble shoot. Problems in a mesh configuration are also easy to diagnose, but not as easy as in a star configuration.

537. Which of the following is the operating system mode in which all instructions can be executed?

A. Problem
B. Interrupt
C. Supervisor
D. Standard processing

Answer: C

The supervisor mode answers the request for all instructions and refers to most types of equipment. In the problem mode, privileged instructions cannot be executed. The other choices are not relevant to operating systems.

538. Which of the following BEST describes the role of a systems analyst?

A. Defines corporate databases
B. Designs systems based on the needs of the user
C. Schedules computer resources
D. Tests and evaluates programmer and optimization tools

Answer: B

The systems analyst designs systems based on the needs of the user. This individual interprets the needs and determines the programs and the programmers necessary to create the particular application. Choices A and D are roles of a database administrator, while choice C is a role of production control.

539. The PRIMARY reason for separating the test and development environments is to:

A. restrict access to systems under test.
B. segregate user and development staff.
C. control the stability of the test environment.
D. secure access to systems under development.

Answer: C

The test environment must be controlled and stable to ensure that development projects are tested in a realistic environment that, as far as possible, mirrors the live environment. Restricting access to test and development systems can be achieved easily by normal access control methods, and the mere separation of the environments will not provide adequate segregation of duties. The IS auditor must be aware of the benefits of separating these environments wherever possible.

540. Information for detecting unauthorized input from a terminal would be BEST provided by the:

A. console log printout.
B. transaction journal.
C. automated suspense file listing.
D. user error report.

Answer: B

The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error occurred, and the user error report would only list input that resulted in an edit error.

541. Congestion control is BEST handled by which OSI layer?

A. Data link
B. Session layer

C. Transport layer
D. Network layer

Answer: C

The transport layer is responsible for reliable data delivery. This layer implements a flow control mechanism that can detect congestion, reduce data transmission rates and increase transmission rates when the network appears to no longer be congested (e.g., TCP flow controls). The network layer is not correct because congestion control occurs based on router implementations of flow control at the subnet level (i.e., source quench messages sent out when router memory or the buffer reaches capacity), however, no message exists to cancel or discard messages, which actually may increase congestion problems. Session layer and data link do not have any functionality for network management.

542. A universal serial bus (USB) port:

A. connects the network without a network card.
B. connects the network with an Ethernet adapter.
C. replaces all existing connections.
D. connects the monitor.

Answer: B

The USB port connects the network without having to install a separate network interface card inside a computer by using a USB Ethernet adapter.

543. An IS auditor reviewing database controls discovered that changes to the database during normal working hours were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation, which of the following would be considered an adequate set of compensating controls?

A. Allow changes to be made only with the DBA user account.
B. Make changes to the database after granting access to a normal user account
C. Use the DBA user account to make changes, log the changes and review the change log the following day.
D. Use the normal user account to make changes, log the changes and review the change log the following day.

Answer: C

The use of a database administrator (DBA) user account normally is (should be) set up to log all changes made and is most appropriate for changes made outside of normal hours. The use of a log, which records the changes, allows changes to be reviewed. The use of the DBA user account without logging would permit uncontrolled changes to be made to databases once access to the account was obtained. The use of a normal user account with no restrictions would allow uncontrolled changes to any of the databases. Logging would only provide information on changes made, but would not limit changes to only those that were authorized. Hence, logging coupled with review form an appropriate set of compensating controls.

544. When assessing the portability of a database application, the IS auditor should verify that:

A. a structured query language (SQL) is used.
B. information import and export procedures with other systems exist.
C. indexes are used.
D. all entities have a significant name and identified primary and foreign keys.

Answer: A

The use of a structured query language (SQL) is a key element for database portability. Import and export of information with other systems is an objective of a database interfaces review. The use of an index is an objective of a database access review, and the fact that all entities have a significant name and identified primary and foreign keys is an objective of a database design review.

545. Utilizing audit software to compare the object code of two programs is an audit technique used to test program:

A. logic.
B. changes.
C. efficiency.
D. computations.

Answer: B

The use of audit software to compare programs is an audit technique used to test change control.

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

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

Answer: C

The use of continuous auditing techniques can actually improve system security when used in time-sharing environments that process a large number of transactions, but leave a scarce paper trail. Choice A is incorrect since the continuous audit approach often does require an IS auditor to collect evidence on system reliability while processing is taking place. Choice B is incorrect since an IS auditor normally would review and follow up only on material deficiencies or errors detected. Choice D is incorrect since the use of continuous audit techniques does depend on the complexity of an organization's computer systems.

547. Which of the following techniques would provide the BEST assurance that the estimate of program development effort is reliable?

A. Function point analysis
B. Estimates by business area
C. A computer-based project schedule
D. An estimate by experienced programmer

Answer: A

The use of estimation techniques, such as function point analysis or lines of code estimation, provide a firm basis for estimation, particularly if supported by historic records of past activities. An estimate by an experienced programmer would be the next best option. However, it may be individualistic and unless there is a standard approach adopted by the programmer, the estimate can vary considerably from one programmer to another. Standard project scheduling tools assist in working out the overall project schedule, but are reliant on the quality of estimation of individual tasks. They do not give an estimate of actual development cost.

548. Which of the following would help to ensure the portability of an application connected to a database? The:

A. verification of database import and export procedures.
B. usage of a structured query language (SQL).
C. analysis of stored procedures/triggers.
D. synchronization of the entity-relation model with the database physical schema.

Answer: B

The use of structured query language (SQL) facilitates portability. Verification of import and export procedures with other systems ensures better interfacing with other systems, analyzing stored procedures/triggers ensures proper access/performance, and reviewing the design, entity-relation model will all be helpful but do not contribute to the portability of an application connecting to a database.

549. An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

A. Personally delete all copies of the unauthorized software.
B. Inform auditee of the unauthorized software, and follow up to confirm deletion.
C. Report the use of the unauthorized software to auditee management and the need to prevent recurrence.
D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.

Answer: C

The use of unauthorized or illegal software should be prohibited by an organization. Software piracy results in inherent exposure and can result in severe fines. The IS auditor must convince the user and user management of the risk and the need to eliminate the risk. An IS auditor should not assume the role of the enforcing officer and take on any personal involvement in removing or deleting the unauthorized software.

550. When logging on to an online system, which of the following processes would the system perform FIRST?

A. Initiation
B. Verification
C. Authorization
D. Authentication

Answer: D

The user's identity is confirmed before any of the other processes. Initiation is a distracter as the system must already have been initiated for the user to log on. Verification normally is performed after an event. Authorization normally will follow confirmation of the user's identity.

551. During the review of a biometrics system operation, the IS auditor should FIRST review the stage of:

A. enrollment.
B. identification.
C. verification.
D. storage.

Answer: A

The users of a biometrics device first must be enrolled in the device. The device captures a physical or behavioral image of the human, identifies the unique features and uses an algorithm to convert them into a string of numbers stored as a template to be used in the matching processes.

552. During an implementation review of a multiuser distributed application, the IS auditor finds minor weaknesses in three areas-the initial setting of parameters is improperly installed, weak passwords are being used and some vital reports are not being checked properly. While preparing the audit report, the IS auditor should:

A. record the observations separately with the impact of each of them marked against each respective finding.
B. advise the manager of probable risks without recording the observations, as the control weaknesses are minor ones.
C. record the observations and the risk arising from the collective weaknesses.
D. apprise the departmental heads concerned with each observation and properly document it in the report.

Answer: C

The weaknesses individually are minor, however together they have the potential to substantially weaken the overall control structure. Choices A and D reflect a failure on the part of the IS auditor to recognize the combined affect of the control weakness. Advising the local manager without reporting the facts and observations would conceal the findings from other stakeholders.

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

A. Wiring and schematic diagram
B. Users list and responsibilities
C. Applications list and their details
D. Backup and recovery procedures

Answer: A

The wiring and schematic diagram of the network is necessary to carry out a network audit. A network audit may not be feasible if a network wiring and schematic diagram is not available. All other documents are important but not necessary.

554. After implementation of a disaster recovery plan (DRP), pre-disaster and post-disaster operational cost for an organization will:

A. decrease.
B. not change (remain the same).
C. increase.
D. increase or decrease depending upon nature of the business.

Answer: C

There are costs associated with all activities and DRP is not an exception. Although there are costs associated with a DRP there are unknown costs that would be incurred if a DRP were not implemented.

555. When an employee is terminated from service, the MOST important action is to:

A. hand over all of the employee's files to another designated employee.
B. take a back up of the employee's work.
C. notify other employees of the termination.
D. disable the employee's logical access.

Answer: D

There is a probability that a terminated employee may misuse access rights, therefore, disabling the terminated employee's logical access is the most important action to take. All the work of the terminated employee needs to be handed over to a designated employee, however this should be performed after implementing choice D. All the work of the terminated employee needs to be backed up and the employees need to be notified of the termination of the employee but again this should not precede the action in choice D.

556. An enterprisewide network security architecture of public key infrastructure (PKI) would be comprised of:

A. A public key cryptosystem, private key cryptosystem and digital certificate
B. A public key cryptosystem, symmetric encryption and certificate authorities
C. A symmetric encryption, digital certificate and kerberos authentication
D. A public key cryptosystem, digital certificate and certificate authorities

Answer: D

These three elements make up a complete system. The other choices are combinations that do not make a complete system.

557. An IS auditor evaluating data integrity in a transaction driven system environment should review atomicity, to determine whether:

A. the database survives failures (hardware or software).
B. each transaction is separated from other transactions.
C. integrity conditions are maintained.
D. a transaction is completed or not, or a database is updated or not.

Answer: D

This concept is included in the atomicity, completeness, isolation and durability (ACID) principle. Durability means that the database survives failures (hardware or software). Isolation means that each transaction is separated from other transactions. Consistency means that integrity conditions are maintained.

558. The risk that an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when, in fact, they do, is an example of:

A. inherent risk.
B.control risk.
C. detection risk.
D. audit risk.

Answer: C

This is an example of detection risk.

559. Which of the following is a threat?

A. Lack of security
B. Loss of goodwill
C. Power outage
D. Information services

Answer: C

Threats, such as a power outage, are possible sources of danger to the assets of an organization. Lack of security is a vulnerability. Vulnerabilities are a set of circumstances susceptible to attack. Loss of goodwill is an impact. Information services are assets, vulnerable to threats and the resulting impacts.

560. For an online transaction processing system, transactions per second is a measure of:

A. throughput.
B. response time.
C. turnaround time.
D. uptime.

Answer: A

"Throughput measures how much work is done by a system over a period of time
it measures productivity of the system. In an online transaction processing system, transactions per second is a throughput index. Response time is defined as the length of time that elapsed between submission of an input and receipt of the first character of output in an online system. Turnaround time is the length of time that elapsed between submission of a job and receipt of a completed output. It is a measure of timeliness in a batch system. The percentage of time that the system is available for processing is called uptime or a reliability index
thus, this is not the correct answer."

561. When an information security policy has been designed, it is MOST important that the information security policy be:

A. stored offsite.
B. written by IS management.
C. circulated to users.
D. updated frequently.

Answer: C

To be effective, an information security policy should reach all members of the staff. Storing the security policy offsite or in a safe place may be desirable but of little value if its contents are not known to the organization's employees. The information security policy should be written by business unit managers

including IS, but not exclusively IS managers. Updating the information security policy is important but will not assure its dissemination.

562. Which of the following is a control over database administration activities?

A. A database checkpoint to restart processing after a system failure
B. Database compression to reduce unused space
C. Supervisory review of access logs
D. Backup and recovery procedures to ensure database availability

Answer: C

To ensure management approval of database administration activities and to exercise control over the use of database tools, there should be a supervisory review of access logs. Database administration activities include among others, database checkpoints, database compression techniques, and data backup and recovery procedures established and implemented to ensure database availability.

563. Which of the following is a control to compensate for a programmer having access to accounts payable production data?

A. Processing controls such as range checks and logic edits
B. Reviewing accounts payable output reports by data entry
C. Reviewing system-produced reports for checks (cheques) over a stated amount
D. Having the accounts payable supervisor match all checks (cheques) to approved invoices

Answer: D

To ensure that the programmer could not have a check (cheque) generated, it would be necessary for someone to confirm all of the checks (cheques) generated by the system. Range and logic checks could easily be bypassed by a programmer since they are privy to the controls that have been built into the system. The review of the accounts payable reports by data entry would only identify changes that might have been made to the data input. It would not identify information that might have been changed on the master files. Reviewing reports for checks (cheques) over a certain amount would not allow for the identification of any unauthorized low value checks (cheques) or catch alterations to the actual checks (cheques) themselves.

564. When reviewing the implementation of a LAN the IS auditor should FIRST review the:

A. node list.
B. acceptance test report.
C. network diagram.
D. user's list.

Answer: C

To properly review a LAN implementation, the IS auditor should first verify the network diagram and confirm the approval. Verification of nodes from the node list and the network diagram would be next followed by a review of the acceptance test report and then the user's list.

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

A. Security awareness
B. Reading the security policy
C. Security committee
D. Logical access controls

Answer: D

To retain a competitive advantage and to meet basic business requirements, organizations must ensure the integrity of the information stored on their computer systems, preserve the confidentiality of sensitive data and ensure the continued availability of their information systems. To meet these goals logical access controls must be in place. Awareness (choice A) itself does not protect against unauthorized access or disclosure of information. Knowledge of an information systems security policy

(choice B), which should be known by the organization's employees, would help to protect information, but would not prevent the unauthorized access of information. A security committee (choice C) is key to the protection of information assets, but would address security issues within a broader perspective.

566. Which of the following would be considered an essential feature of a network management system?

A. A graphical interface to map the network topology
B. Capacity to interact with the Internet to solve the problems
C. Connectivity to a help desk for advice on difficult issues
D. An export facility for piping data to spreadsheets

Answer: A

To trace the topology of the network it would be essential that a graphical interface exist. It is not necessary that each network be on the Internet and a help desk, and the ability to export to a spreadsheet is not an essential element.

567. Which of the following testing methods is MOST effective during the initial phases of prototyping?

A. System
B. Parallel
C. Volume
D. Top-down

Answer: D

Top-down testing starts with the system's major functions and works downwards. The initial emphasis when using prototyping is to create screens and reports, thus shaping most of the proposed system's features in a short period. Volume and system testing is performed during final system testing phases. Parallel testing is not needed necessarily, especially if there's no old system to compare with.

568. Which of the following implementation modes would provide the GREATEST amount of security for outbound data connecting to the Internet?

A. Transport mode with authentication header plus encapsulating security payload (ESP)
B. Secure socket layer (SSL) mode
C. Tunnel mode with AH plus ESP
D. Triple-DES encryption mode

Answer: C

Tunnel mode provides protection to the entire IP package. To accomplish this, AH and ESP services can be nested. The transport mode provides primary protection for the higher layers of the protocols by extending protection to the data fields (payload) of an IP package. The SSL (secure socket layer) mode, provides security to the higher communication layers (transport layer). The triple-DES encryption mode is an algorithm that provides confidentiality.

569. 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?

A. Work is completed in tunnel mode with IP security using the nested services of authentication header (AH) and encapsulating security payload (ESP).
B. A digital signature with RSA has been implemented.
C. Digital certificates with RSA are being used.
D. Work is being completed in.TCP services.

Answer: A

Tunnel mode with IP security provides encryption and authentication of the complete IP package. To accomplish this, the AH (authentication header) and ESP (encapsulating security payload) services can be nested· Choices B and C provide authentication and integrity. TCP services do not provide encryption and authentication.

570. During a review of the controls over the process of defining IT service levels, an IS auditor would MOST likely interview the:

A. systems programmer.
B. legal staff.
C. business unit manager.
D. application programmer.

Answer: C

Understanding the business requirements is key in defining the service levels. While each of the other entities listed may provide some definition, the best choice here is the business unit manager, because of the knowledge this person has of the requirements of the organization.

571. Which of the following describes a difference between unit testing and system testing?

A. Unit testing is more comprehensive.
B. Programmers are not involved in system testing.
C. System testing relates to interfaces between programs.
D. System testing proves user requirements are complete.

Answer: C

Unit testing is different from system testing because system testing relates to interfaces between programs. System testing takes place before users are invited to test against their requirements. System testing normally will be carried out by the programming team. Unit testing is usually less comprehensive.

572. A request for a change to a report format in a module (subsystem) was made. After making the required changes, the programmer should carry out:

A. unit testing.
B. unit and module testing.
C. unit, module and regression testing.
D. module testing.

Answer: C

Unit, module and regression testing will ensure that the specific unit, module or subsystem and the complete system works as expected. Regression testing is required for any changes carried out at any level. The unit testing will ensure that the unit is working as expected. The unit and module testing will ensure that the unit and the module work as expected. Unit testing and module testing will ensure that the report or the unit and the module or the subsystem are working as expected, but will not ensure that there has not been an impact on the complete system. Regression testing is required for any changes carried out at any level.

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

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

Answer: C

Unless controlled, spooling for offline printing may enable additional copies to be printed. Print files are unlikely to be available for online reading by operators. Data on spool files are no easier to amend without authority than any other file. There is usually a lesser threat of unauthorized access to sensitive reports in the event of a system failure.

574. An IS auditor's primary concern when application developers wish to use a copy of yesterday's production transaction file for volume tests is that:

A. users may prefer to use contrived data for testing.

B. unauthorized access to sensitive data may result.
C. error handling and credibility checks may not be fully proven.
D. full functionality of the new process is not necessarily tested.

Answer: B

Unless the data is sanitized there is the risk of disclosing sensitive date.

575. A retail company recently installed data warehousing client software at geographically diverse sites. Due to time zone differences between the sites, updates to the warehouse are not synchronized. Which of the following will be affected the MOST?

A. Data availability
B. Data completeness
C. Data redundancy
D. Data inaccuracy

Answer: B

Unsynchronized updates will generally cause data completeness to be affected, for example sales data from one site do not match costs incurred in another site.

576. Which of the following is the BEST form of transaction validation?

A. Use of key field verification techniques in data entry
B. Use of programs to check the transaction against criteria set by management
C. Authorization of the transaction by supervisory personnel in an adjacent department
D. Authorization of the transaction by a department supervisor prior to the batch process

Answer: B

Use of programs to check the transaction against criteria set by management is the best answer because validation involves comparison of the transaction against predefined criteria.

577. Which of the following is MOST effective in controlling application maintenance?

A. Informing users of the status of changes
B. Establishing priorities on program changes
C. Obtaining user approval of program changes
D. Requiring documented user specifications for changes

Answer: C

User approvals of program changes will ensure that changes are correct as specified by the user and that they are authorized. Therefore, erroneous or unauthorized changes are less likely to occur, minimizing system downtime and errors.

578. Following the development of an application system, it is determined that several design objectives have not been achieved. This is MOST likely to have been caused by:

A. insufficient user involvement.
B. early dismissal of the project manager.
C. inadequate quality assurance (QA) tools.
D. noncompliance with defined approval points.

Answer: A

User involvement is the most common reason for the failure of an application system development.

579. Which of the following groups should assume ownership of a systems development project and the resulting system?

A. User management
B. Senior management

C. Project steering committee
D. Systems development management

Answer: A

User management assumes ownership of the project and resulting system. They should review and approve deliverables as they are defined and accomplished. Senior management approves the project and the resources needed to complete it. The project steering committee provides overall direction and is responsible for monitoring costs and timetables. Systems development management provides technical support.

580. Which of the following access control functions is LEAST likely to be performed by a database management system (DBMS) software package?

A. User access to field data
B. User sign-on at the network level
C. User authentication at the program level
D. User authentication at the transaction level

Answer: B

User sign-on is carried out by the access control software, not by DBMS software. The other choices are all primary tasks of DBMS software.

581. In a LAN environment, which of the following minimizes the risk of data corruption during transmission?

A. Using end-to-end encryption for data communication
B. Using separate conduits for electrical and data cables
C. Using check sums for checking the corruption of data
D. Connecting the terminals using a star topology

Answer: B

Using separate conduits for data cables and electrical cables, minimizes the risk of data corruption due to an induced magnetic field created by electrical current. Data encryption minimizes the risk of data leakage in case of wire tapping, however it can not prevent corruption. A check sum will help detect the data corruption during communication, but will not prevent it. Using a star topology, will increase the speed of communication, but will not detect the corruption.

582. Utility programs that assemble software modules needed to execute a machine instruction application program version are:

A. text editors.
B. program library managers.
C. linkage editors and loaders.
D. debuggers and development aids.

Answer: C

Utility programs that assemble software modules needed to execute a machine instruction application program version are linkage editors and loaders.

583. The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

A. Utilization of an intrusion detection system to report incidents.
B. Mandating the use of passwords to access all software.
C. Installing an efficient user log system to track the actions of each user
D. Provide training on a regular basis to all current and new employees.

Answer: D

Utilizing an intrusion detection system to report on incidents that occur is an implementation of a security program and is not effective in establishing a security awareness program. Choices B and C do not address awareness. Training is the only choice that is directed at security awareness.

584. 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?

A. Verifying production to customer orders
B. Logging all customer orders in the ERP system
C. Using hash totals in the order transmitting process
D. Approving (production supervisor) orders prior to production

Answer: A

Verification will ensure that production orders match customer orders. Logging can be used to detect inaccuracies, but does not in itself guarantee accurate processing. Hash totals will ensure accurate order transmission, but not accurate processing centrally. Production supervisory approval is a time consuming manual process that does not guarantee proper control.

585. A key element in a risk analysis is/are:

A. audit planning.
B. controls.
C. vulnerabilities.
D. liabilities.

Answer: C

Vulnerabilities are a key element in the conduct of a risk analysis. Audit planning consists of short and long-term processes that may detect threats to the information assets. Controls mitigate risks associated with specific threats. Liabilities are part of business and are not inherently a risk.

586. With reference to the risk management process, which of the following statements is correct?

A. Vulnerabilities can be exploited by a threat.
B. Vulnerabilities are events with the potential to cause harm to IS resources.
C. Vulnerability exists because of threats associated with use of information resources.
D. Lack of user knowledge is an example of a threat.

Answer: A

Vulnerabilities are characteristics of IS resources that can be exploited with some harm resulting. Threats not vulnerabilities are events with the potential to cause harm. A threat occurs because of a vulnerability associated with the use of information resources. Lack of user knowledge is an example of a vulnerability.

587. Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?

A. Halon gas
B. Wet-pipe sprinklers
C. Dry-pipe sprinklers
D. Carbon dioxide gas

Answer: C

Water sprinklers, with an automatic power shut-off system, are accepted as efficient because they can be set to automatic release without threat to life and water is environmentally friendly. Sprinklers must be dry pipe to prevent the risk of leakage. Halon is efficient and effective as it does not threaten human life, and therefore can be set to automatic release, but it is environmentally damaging and very expensive. Water is an acceptable medium but the pipes should be empty to avoid leakage, so a full system is not a viable option. Carbon dioxide is accepted as an environmentally acceptable gas, but it is less efficient as it cannot be set to automatic release in a staffed site because it threatens life.

588. 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:

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

Answer: C

When an auditor observes such conditions, it is best to fully apprise the auditee and suggest that further problem resolutions be attempted. Recording it as a minor error and leaving it to auditee's discretion would be inappropriate, and neglecting the error would indicate that the auditor has not taken steps to further probe the issue to its logical end.

589. When reviewing an organization's logical access security, which of the following would be of the MOST concern to an IS auditor?

A. Passwords are not shared.
B. Password files are encrypted.
C. Redundant logon IDs are deleted.
D. The allocation of logon IDs is controlled.

Answer: B

When evaluating the technical aspects of logical security, unencrypted files represent the greatest risk. The sharing of passwords, checking for the redundancy of logon ids, and proper logon ID procedures are essential, but they are less important than ensuring that the password files are encrypted.

590. An IS auditor performing an audit of the company's IS strategy would be LEAST likely to:

A. assess IS security procedures.
B. review both short- and long-term IS strategies.
C. interview appropriate corporate management personnel.
D. ensure that the external environment has been considered.

Answer: A

When performing an audit of IS strategic planning it is unlikely that the IS auditor would assess specific security procedures. During an IS strategy review overall goals and business plans would be reviewed to determine that the organization's plans are consistent with its goals.

591. 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. a backup server be available to run ETCS operations with up-to-date data.
B. a backup server be loaded with all the relevant software and data.
C. the systems staff of the organization be trained to handle any event.
D. source code of the ETCS application be placed in escrow.

Answer: D

Whenever proprietary application software is purchased, the contract should provide for a source code agreement. This will ensure that the purchasing company will have the opportunity to modify the software should the vendor cease to be in business. Having a backup server with current data and staff training is critical but not as critical as ensuring the availability of the source code.

592. In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

A. Automated logging of changes to development libraries

B. Additional staff to provide separation of duties
C. Procedures that verify that only approved program changes are implemented
D. Access controls to prevent the operator from making program modifications

Answer: C

While it would be preferred that strict separation of duties be adhered to and that additional staff is recruited, as suggested in choice B, this practice is not always possible in small organizations. The IS auditor must look at recommended alternative processes. Of the choices, C is the only practical one that has an impact. The IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed by a third party on a regular basis. This would be a compensating control process. Choice A, involving logging of changes to development libraries, would not detect changes to production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

593. Which of the following would an IS auditor consider to be the MOST important to review when conducting a business continuity audit?

A. A hot site is contracted for and available as needed.
B. A business continuity manual is available and current.
C. Insurance coverage is adequate and premiums are current.
D. Media backups are performed on a timely basis and stored offsite.

Answer: D

Without data to process, all other components of the recovery effort are in vain. Even in the absence of a plan, recovery efforts of any type would not be practical without data to process.

594. Losses can be minimized MOST effectively by using outside storage facilities to do which of the following?

A. Provide current, critical information in backup files
B. Ensure that current documentation is maintained at the backup facility
C. Test backup hardware
D. Train personnel in backup procedures

Answer: A

Without having current, critical information in offsite backup files recovery is generally impossible. Having current backup documentation offsite, tested backup hardware and personnel trained in backup procedures facilitates the recovery process, but they are not as important as having the current, critical information available in offsite backup files.

595. Which of the following can consume valuable network bandwidth?

A. Trojan horses
B. Trap doors
C. Worms
D. Vaccines

Answer: C

Worms are destructive programs that may destroy data or utilize tremendous computer and communication resources. Trojan horses can capture and transmit private information to the attacker's computer. Trap doors are exits out of an authorized program. Vaccines are programs designed to detect computer viruses.

596. Programs that can run independently and travel from machine to machine across network connections, with the ability to destroy data or utilize tremendous computer and communication resources, are referred to as:

A. trojan horses.
B. viruses.
C. worms.

D. logic bombs.

Answer: C

Worms are nonreplicating programs that can run independently and travel from machine to machine. A trojan horse resembles a commonly used authorized program that does something unrelated to its stated or intended purpose causing a malicious or fraudulent action or event to occur. Viruses are malicious program code inserted into other executable code that can self-replicate and spread from computer to computer. Logic bombs are programmed threats that lie dormant in commonly used software for an extended period of time until they are triggered.

597. An organization acquiring other businesses continues using its legacy EDI systems, and uses three separate value added network (VAN) providers. No written VAN agreements exist. The IS auditor should recommend that management:

A. obtain independent assurance of the third party service providers.
B. set up a process for monitoring the service delivery of the third party.
C. ensure that formal contracts are in place.
D. consider agreements with third party service providers in the development of continuity plans.

Answer: C

Written agreements would assist management in ensuring compliance with external requirements. While management should obtain independent assurance of compliance, this can not be achieved until there is a contract in place. One aspect of managing third party services is to provide monitoring, however, this can not be achieved until there is a contract. Ensuring that VAN agreements are available for review may assist in the development of continuity plans if they are deemed critical IT resources, however, this can not be achieved until there is a contract in place.

598. The role of IT auditor in complying with the Management Assessment of Internal Controls (Section 404 of the Sarbanes-Oxley Act) is:

A. planning internal controls
B. documenting internal controls
C. designing internal controls
D. implementing internal controls

Answer: B

Choice (B) is the correct answer. The role of the IT auditor is to document, understand, and test the internal controls in computer systems. Planning, designing, and implementing internal controls is part of operating management's responsibility. This responsibility does not change whether complying with Sarbanes-Oxley Act or not. Compliance efforts are ongoing and include documenting internal controls on a quarterly basis. Organizations need to identify and document all electronic and manual processes related to the financial reporting process.

599. A primary function of risk management is the identification of cost-effective controls. In selecting appropriate controls, which of the following methods is best to study the effectiveness of adding various safeguards in reducing vulnerabilities?

A. "What if" analysis
B. Traditional cost/benefit analysis
C. Screening analysis
D. A "back-of-the-envelope" analysis

Answer: A

Choice (A) is the correct answer. With the "what if" analysis method, the effect of adding various safeguards (and therefore reducing vulnerabilities) is tested to see what difference each makes. Trade-offs can then be made based on the cost of the safeguard and its benefit in terms of reduced risk. Choice (B) is incorrect. In traditional cost/benefit analysis, the cost is based on the purchase and operating costs of safeguards. The benefit is calculated based on an expected decrease in future losses. Choice (C) is incorrect. Screening analysis can be used to concentrate on the highest-risk areas. One method is to examine risks with very severe consequences, such as a high dollar loss or loss of life. Choice (D) is

incorrect. With "back-of-the envelope" analysis, a high-medium-low ranking can often provide all the information needed. However, especially for the selection of expensive safeguards or the analysis of systems with unknown consequences, more in-depth analysis may be warranted.

600. According to the Committee of Sponsoring Organizations (COSO), the internal control framework consists of which of the following?

A. Processes, people, objectives.
B. Profits, products, processes.
C. Costs, revenues, margins.
D. Return on investment, earnings per share, market share.

Answer: A