CISA $^{Q\&As}$

Certified Information Systems Auditor

Pass Isaca CISA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

http://www.CertBus.com/CISA.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published
by Isaca Official Exam Center

Vendor: Isaca

Exam Code: CISA

Exam Name: Certified Information Systems Auditor

Q&As: Demo

QUESTION 1
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.

Correct Answer: A

QUESTION 2
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.

Correct Answer: B

QUESTION 3
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

Correct Answer: B

QUESTION 4
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.

Correct Answer: A

QUESTION 5
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

Correct Answer: B

QUESTION 6
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.

Correct Answer: A

QUESTION 7
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.

Correct Answer: D

QUESTION 8
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)

Correct Answer: D

QUESTION 9
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

Correct Answer: C

QUESTION 10
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

Correct Answer: B

QUESTION 11
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.

Correct Answer: B

QUESTION 12
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.

Correct Answer: C

QUESTION 13
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.

Correct Answer: D

QUESTION 14
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.

Correct Answer: A

QUESTION 15
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.

Correct Answer: C

QUESTION 16
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.

Correct Answer: B

QUESTION 17
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

Correct Answer: D

QUESTION 18
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.

Correct Answer: A

QUESTION 19
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

Correct Answer: A

QUESTION 20
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

Correct Answer: C

QUESTION 21
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.

Correct Answer: D

QUESTION 22
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.

Correct Answer: C

QUESTION 23
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

Correct Answer: B

QUESTION 24
When developing a risk-based audit strategy, an IS auditor should conduct a risk

assessment to ensure that:

A. controls needed to mitigate risks are in place.
B. vulnerabilities and threats are identified.
C. audit risks are considered.
D. a gap analysis is appropriate.

Correct Answer: B

QUESTION 25
To ensure that audit resources deliver the best value to the organization, the FIRST step

would be to:

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

Correct Answer: C

QUESTION 26
An organization's IS audit charter should specify the:

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

Correct Answer: D

QUESTION 27
An IS auditor is evaluating management's risk assessment of information systems. The IS

auditor should FIRST review:

A. the controls already in place.
B. the effectiveness of the controls in place.
C. the mechanism for monitoring the risks related to the assets.
D. the threats/vulnerabilities affecting the assets.

Correct Answer: D

QUESTION 28
In planning an audit, the MOST critical step is the identification of the:

A. areas of high risk.
B. skill sets of the audit staff.
C. test steps in the audit.
D. time allotted for the audit.

Correct Answer: A

QUESTION 29
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.

Correct Answer: D

QUESTION 30
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.

Correct Answer: A

QUESTION 31
An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling,

when:

A. the probability of error must be objectively quantified.
B. the auditor wishes to avoid sampling risk.
C. generalized audit software is unavailable.
D. the tolerable error rate cannot be determined.

Correct Answer: A

QUESTION 32
During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

A. address audit objectives.
B. collect sufficient evidence.
C. specify appropriate tests.
D. minimize audit resources.

Correct Answer: A

QUESTION 33
When selecting audit procedures, an IS auditor should use professional judgment to

ensure that:

A. sufficient evidence will be collected.
B. all significant deficiencies identified will be corrected within a reasonable period.
C. all material weaknesses will be identified.
D. audit costs will be kept at a minimum level.

Correct Answer: A

QUESTION 34
An IS auditor evaluating logical access controls should FIRST:

A. document the controls applied to the potential access paths to the system.
B. test controls over the access paths to determine if they are functional.
C. evaluate the security environment in relation to written policies and practices
D. obtain an understanding of the security risks to information processing.

Correct Answer: D

QUESTION 35
The PRIMARY purpose of an IT forensic audit is:

A. to participate in investigations related to corporate fraud.
B. the systematic collection of evidence after a system irregularity.
C. to assess the correctness of an organization's financial statements
D. to determine that there has been criminal activity.

Correct Answer: B

QUESTION 36
An IS auditor is performing an audit of a remotely managed server backup. The IS

auditor reviews the logs for one day and finds one case where logging on a server has

failed with the result that backup restarts cannot be confirmed. What should the auditor

do?

A. Issue an audit finding
B. Seek an explanation from IS management
C. Review the classifications of data held on the server
D. Expand the sample of logs reviewed

Correct Answer: D

QUESTION 37
In an IS audit of several critical servers, the IS auditor wants to analyze audit trails to

discover potential anomalies in user or system behavior. Which of the following tools are

MOST suitable for performing that task?

A. CASE tools
B. Embedded data collection tools
C. Heuristic scanning tools
D. Trend/variance detection tools

Correct Answer: D

QUESTION 38
An IS auditor is evaluating a corporate network for a possible penetration by employees.

Which of the following findings should give the IS auditor the GREATEST concern?

A. There are a number of external modems connected to the network.
B. Users can install software on their desktops.
C. Network monitoring is very limited.
D. Many user IDs have identical passwords.

Correct Answer: D

QUESTION 39
Which of the following is the PRIMARY advantage of using computer forensic software

for investigations?

A. The preservation of the chain of custody for electronic evidence
B. Time and cost savings
C. Efficiency and effectiveness
D. Ability to search for violations of intellectual property rights

Correct Answer: A

QUESTION 40
An IS auditor has imported data from the client's database. The next step-confirming

whether the imported data are complete-is performed by:

A. matching control totals of the imported data to control totals of the original data.
B. sorting the data to confirm whether the data are in the same order as the original data.
C. reviewing the printout of the first 100 records of original data with the first 100 records of imported data.
D. filtering data for different categories and matching them to the original data.

Correct Answer: A

QUESTION 41

The vice president of human resources has requested an audit to identify payroll

overpayments for the previous year. Which would be the BEST audit technique to use in

this situation?

A. Test data
B. Generalized audit software
C. Integrated test facility
D. Embedded audit module

Correct Answer: B

QUESTION 42
During a security audit of IT processes, an IS auditor found that there were no

documented security procedures. The IS auditor should:

A. create the procedures document.
B. terminate the audit.
C. conduct compliance testing.
D. identify and evaluate existing practices.

Correct Answer: D

QUESTION 43
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

Correct Answer: C

QUESTION 44
An organization is implementing a new system to replace a legacy system. Which of the

following conversion practices creates the GREATEST risk?

A. Pilot
B. Parallel
C. Direct cutover
D. Phased

Correct Answer: C

QUESTION 45
Which of the following system and data conversion strategies provides the GREATEST

redundancy?

A. Direct cutover
B. Pilot study
C. Phased approach
D. Parallel run

Correct Answer: D

QUESTION 46
Which of the following would impair the independence of a quality assurance team?

A. Ensuring compliance with development methods
B. Checking the testing assumptions
C. Correcting coding errors during the testing process
D. Checking the code to ensure proper documentation

Correct Answer: C

QUESTION 47
From a risk management point of view, the BEST approach when implementing a large

and complex IT infrastructure is:

A. a big bang deployment after proof of concept.
B. prototyping and a one-phase deployment.
C. a deployment plan based on sequenced phases.
D. to simulate the new infrastructure before deployment.

Correct Answer: C

QUESTION 48
An organization is migrating from a legacy system to an enterprise resource planning

(ERP) system. While reviewing the data migration activity, the MOST important concern

for the IS auditor is to determine that there is a:

A. correlation of semantic characteristics of the data migrated between the two systems.
B. correlation of arithmetic characteristics of the data migrated between the two systems.
C. correlation of functional characteristics of the processes between the two systems.
D. relative efficiency of the processes between the two systems.

Correct Answer: A

QUESTION 49
The reason a certification and accreditation process is performed on critical systems is to

ensure that:

A. security compliance has been technically evaluated.
B. data have been encrypted and are ready to be stored.
C. the systems have been tested to run on different platforms.
D. the systems have followed the phases of a waterfall model.

Correct Answer: A

QUESTION 50
During a postimplementation 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.

Correct Answer: A

QUESTION 51
During an application audit, an IS auditor finds several problems related to corrupted data

in the database. Which of the following is a corrective control that the IS auditor should

recommend?

A. implement data backup and recovery procedures.

B. Define standards and closely monitor for compliance.

C. Ensure that only authorized personnel can update the database.

D. Establish controls to handle concurrent access problems.

Correct Answer: A

QUESTION 52
An IS auditor finds out-of-range data in some tables of a database. Which of the

following controls should the IS auditor recommend to avoid this situation?

A. Log all table update transactions.

B. implement before-and-after image reporting.

C. Use tracing and tagging.

D. implement integrity constraints in the database.

Correct Answer: D

QUESTION 53
Responsibility and reporting lines cannot always be established when auditing automated

systems since:

A. diversified control makes ownership irrelevant.

B. staff traditionally changes jobs with greater frequency.

C. ownership is difficult to establish where resources are shared.

D. duties change frequently in the rapid development of technology.

Correct Answer: C

QUESTION 54
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.

Correct Answer: C

QUESTION 55
Which of the following would help to ensure the portability of an application connected

to a database?

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

Correct Answer: B

QUESTION 56
Business units are concerned about the performance of a newly implemented system.

Which of the following should an IS auditor recommend?

A. Develop a baseline and monitor system usage.
B. Define alternate processing procedures.
C. Prepare the maintenance manual.
D. implement the changes users have suggested.

Correct Answer: A

QUESTION 57
A company undertakes a business process reengineering (BPR) project in support of a

new and direct marketing approach to its customers. Which of the following would be an

IS auditor's main concern about the new process?

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

Correct Answer: A

QUESTION 58
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

Correct Answer: A

QUESTION 59
When two or more systems are integrated, input/output controls must be reviewed by an

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.

Correct Answer: C

QUESTION 60
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.

Correct Answer: C

QUESTION 61
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 that the type of transaction is valid for the 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.

Correct Answer: B

QUESTION 62
A company has recently upgraded its purchase system to incorporate EDI transmissions.

Which of the following controls should be implemented in the EDI interface to provide

for efficient data mapping?

A. Key verification

B. One-for-one checking

C. Manual recalculations

D. Functional acknowledgements

Correct Answer: D

QUESTION 63
Once an organization has finished the business process reengineering (BPR) of all its

critical operations, an IS auditor would MOST likely focus on a review of:

A. pre-BPR process flowcharts.

B. post-BPR process flowcharts.

C. BPR project plans.

D. continuous improvement and monitoring plans.

Correct Answer: B

QUESTION 64
An IS auditor has completed a network audit. Which of the following is the MOST

significant logical security finding?

A. Network workstations are not disabled automatically after a period of inactivity.
B. Wiring closets are left unlocked
C. Network operating manuals and documentation are not properly secured.
D. Network components are not equipped with an uninterruptible power supply.

Correct Answer: A

QUESTION 65
Which of the following would MOST effectively enhance the security of a challenge-

response based authentication system?

A. Selecting a more robust algorithm to generate challenge strings
B. implementing measures to prevent session hijacking attacks
C. increasing the frequency of associated password changes
D. increasing the length of authentication strings

Correct Answer: B

QUESTION 66
Which of the following should an IS auditor recommend for the protection of specific

sensitive information stored in the data warehouse?

A. implement column- and row-level permissions
B. Enhance user authentication via strong passwords
C. Organize the data warehouse into subject matter-specific databases
D. Log user access to the data warehouse

Correct Answer: A

QUESTION 67
The responsibility for authorizing access to a business application system belongs to the:

A. data owner.
B. security administrator.
C. IT security manager.
D. requestor's immediate supervisor.

Correct Answer: A

QUESTION 68
An organization has created a policy that defines the types of web sites that users are

forbidden to access. What is the MOST effective technology to enforce this policy?

A. Stateful inspection firewall
B. Web content filter
C. Web cache server
D. Proxy server

Correct Answer: B

QUESTION 69
What would be the MOST effective control for enforcing accountability among database

users accessing sensitive information?

A. implement a log management process
B. implement a two-factor authentication
C. Use table views to access sensitive data
D. Separate database and application servers

Correct Answer: A

QUESTION 70
Which of the following intrusion detection systems (IDSs) monitors the general patterns

of activity and traffic on a network and creates a database?

A. Signature-based
B. Neural networks-based
C. Statistical-based
D. Host-based

Correct Answer: B

QUESTION 71
The MOST important difference between hashing and encryption is that hashing:

A. is irreversible.
B. output is the same length as the original message.
C. is concerned with integrity and security.
D. is the same at the sending and receiving end.

Correct Answer: A

QUESTION 72
Which of the following cryptography options would increase overhead/cost?

A. The encryption is symmetric rather than asymmetric.
B. A long asymmetric encryption key is used.
C. The hash is encrypted rather than the message.
D. A secret key is used.

Correct Answer: B

QUESTION 73
The MOST important success factor in planning a penetration test is:

A. the documentation of the planned testing procedure.
B. scheduling and deciding on the timed length of the test.
C. the involvement of the management of the client organization.
D. the qualifications and experience of staff involved in the test.

Correct Answer: C

QUESTION 74
Which of the following virus prevention techniques can be implemented through

hardware?

A. Remote booting
B. Heuristic scanners

C. Behavior blockers

D. Immunizers

Correct Answer: A

QUESTION 75
Which of the following append themselves to files as a protection against viruses?

A. Behavior blockers

B. Cyclical redundancy checkers (CRCs)

C. Immunizers

D. Active monitors

Correct Answer: C

QUESTION 76
Which of the following acts as a decoy to detect active internet attacks?

A. Honeypots

B. Firewalls

C. Trapdoors

D. Traffic analysis

Correct Answer: A

QUESTION 77
A certificate authority (CA) can delegate the processes of:

A. revocation and suspension of a subscriber's certificate.

B. generation and distribution of the CA public key.

C. establishing a link between the requesting entity and its public key.

D. issuing and distributing subscriber certificates.,

Correct Answer: C

QUESTION 78
Which of the following results in a denial-of-service attack?

A. Brute force attack

B. Ping of death

C. Leapfrog attack

D. Negative acknowledgement (NAK) attack

Correct Answer: B

QUESTION 79
Which of the following is the GREATEST advantage of elliptic curve encryption over

RSA encryption?

A. Computation speed

B. Ability to support digital signatures

C. Simpler key distribution

D. Greater strength for a given key length

Correct Answer: A

QUESTION 80

Which of the following would be the BEST overall control for an Internet business

looking for confidentiality, reliability and integrity of data?

A. Secure Sockets Layer (SSL)
B. Intrusion detection system (IDS)
C. Public key infrastructure (PKI)
D. Virtual private network (VPN)

Correct Answer: C

QUESTION 81

To ensure message integrity, confidentiality and non repudiation between two parties, the

MOST effective method would be to create a message digest by applying a cryptographic

hashing algorithm against:

A. the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key by using the receiver's public key.
B. any part of the message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key using the receiver's public key.
C. the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering both the encrypted message and digest using the receiver's public key.
D. the entire message, enciphering the message digest using the sender's private key and enciphering the message using the receiver's public key.

Correct Answer: A

QUESTION 82

Which of the following antivirus software implementation strategies would be the MOST

effective in an interconnected corporate network?

A. Server antivirus software
B. Virus walls
C. Workstation antivirus software
D. Virus signature updating

Correct Answer: B

QUESTION 83

Which of the following would be of MOST concern to an IS auditor reviewing a virtual

private network (VPN) implementation? Computers on the network that are located:

A. on the enterprise's internal network.
B. at the backup site.
C. in employees' homes.
D. at the enterprise's remote offices.

Correct Answer: C

QUESTION 84

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

A. confidentiality.

B. integrity.
C. availability.
D. timeliness.

Correct Answer: B

QUESTION 85
Which of the following should be the MOST important criterion in evaluating a backup

solution for sensitive data that must be retained for a long period of time due to

regulatory requirements?

A. Full backup window
B. Media costs
C. Restore window
D. Media reliability

Correct Answer: D

QUESTION 86
In the event of a data center disaster, which of the following would be the MOST

appropriate strategy to enable a complete recovery of a critical database?

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

Correct Answer: B

QUESTION 87
Which of the following backup techniques is the MOST appropriate when an

organization requires extremely granular data restore points, as defined in the recovery

point objective (RPO)?

A. Virtual tape libraries
B. Disk-based snapshots
C. Continuous data backup
D. Disk-to-tape backup

Correct Answer: C

QUESTION 88
What is the BEST backup strategy for a large database with data supporting online sales?

A. Weekly full backup with daily incremental backup
B. Daily full backup
C. Clustered servers
D. Mirrored hard disks

Correct Answer: A

QUESTION 89
During an audit, an IS auditor notes that an organization's business continuity plan (BCP)

does not adequately address information confidentiality during a recovery process. The IS

auditor should recommend that the plan be modified to include:

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

Correct Answer: A

QUESTION 90
Which of the following is the GREATEST risk when storage growth in a critical file

server is not managed properly?

A. Backup time would steadily increase
B. Backup operational cost would significantly increase
C. Storage operational cost would significantly increase
D. Server recovery work may not meet the recovery time objective (RTO)

Correct Answer: D

QUESTION 91
Which of the following is the MOST important consideration when defining recovery

point objectives (RPOs)?

A. Minimum operating requirements
B. Acceptable data loss
C. Mean time between failures
D. Acceptable time for recovery

Correct Answer: B

QUESTION 92
A structured walk-through test of a disaster recovery plan involves:

A. representatives from each of the functional areas coming together to go over the plan.
B. all employees who participate in the day-to-day operations coming together to practice executing the plan.
C. moving the systems to the alternate processing site and performing processing operations.
D. distributing copies of the plan to the various functional areas for review.

Correct Answer: B

QUESTION 93
In a contract with a hot, warm or cold site, contractual provisions should cover which of

the following considerations?

A. Physical security measures
B. Total number of subscribers
C. Number of subscribers permitted to use a site at one time
D. References by other users

Correct Answer: C

QUESTION 94
Which of the following is the GREATEST concern when an organization's backup

facility is at a warm site?

A. Timely availability of hardware
B. Availability of heat, humidity and air conditioning equipment
C. Adequacy of electrical power connections
D. Effectiveness of the telecommunications network

Correct Answer: A

QUESTION 95
Which of the following recovery strategies is MOST appropriate for a business having

multiple offices within a region and a limited recovery budget?

A. A hot site maintained by the business
B. A commercial cold site
C. A reciprocal arrangement between its offices
D. A third-party hot site

Correct Answer: C

QUESTION 96
The PRIMARY purpose of a business impact analysis (BIA) is to:

A. provide a plan for resuming operations after a disaster.
B. identify the events that could impact the continuity of an organization's operations.
C. publicize the commitment of the organization to physical and logical security.
D. provide the framework for an effective disaster recovery plan.

Correct Answer: B

QUESTION 97
After implementation of a disaster recovery plan, pre-disaster and post-disaster

operational costs for an organization will:

A. decrease.
B. not change (remain the same).
C. increase.
D. increase or decrease depending upon the nature of the business.

Correct Answer: C

QUESTION 98
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

Correct Answer: D

QUESTION 99
An organization having a number of offices across a wide geographical area has

developed a disaster recovery plan. Using actual resources, which of the following is the

MOST cost-effective test of the disaster recovery plan?

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

Correct Answer: B

QUESTION 100
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.

Correct Answer: D

QUESTION 101
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.

Correct Answer: C

QUESTION 102
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.

Correct Answer: C

QUESTION 103
Disaster recovery planning (DRP) 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.

Correct Answer: A

QUESTION 104
An IS auditor conducting a review of disaster recovery planning (DRP) at a financial

processing organization has discovered the following:
?The existing disaster recovery plan was compiled two years earlier by a systems

analyst in the organization's IT department using transaction flow projections from the

operations department.

?The plan was presented to the deputy CEO for approval and formal issue, but it is still

awaiting their attention.

?The plan has never been updated, tested or circulated to key management and staff,

though interviews show that each would know what action to take for its area in the event of a disruptive
incident.

The IS auditor's report should recommend that:

A. the deputy CEO be censured for their failure to approve the plan.
B. a board of senior managers is set up to review the existing plan.
C. the existing plan is approved and circulated to all key management and staff.
D. a manager coordinates the creation of a new or revised plan within a defined time limit.

Correct Answer: D

QUESTION 105
An IS auditor conducting a review of disaster recovery planning (DRP) at a financial

processing organization has discovered the following:
?The existing disaster recovery plan was compiled two years earlier by a systems

analyst in the organization's IT department using transaction flow projections from the

operations department.

?The plan was presented to the deputy CEO for approval and formal issue, but it is still

awaiting his/her attention.

?The plan has never been updated, tested or circulated to key management and staff,

though interviews show that each would know what action to take for its area in the event

of a disruptive incident.

The basis of an organization's disaster recovery plan is to reestablish live processing at an

alternative site where a similar, but not identical, hardware configuration is already

established. An IS auditor should:

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 is 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.

Correct Answer: C

To Read the **Whole Q&As**, please purchase the **Complete Version** from **Our website**.

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

One Year Free Update
Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee
To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy
We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Guarantee & Policy | Privacy & Policy | Terms & Conditions