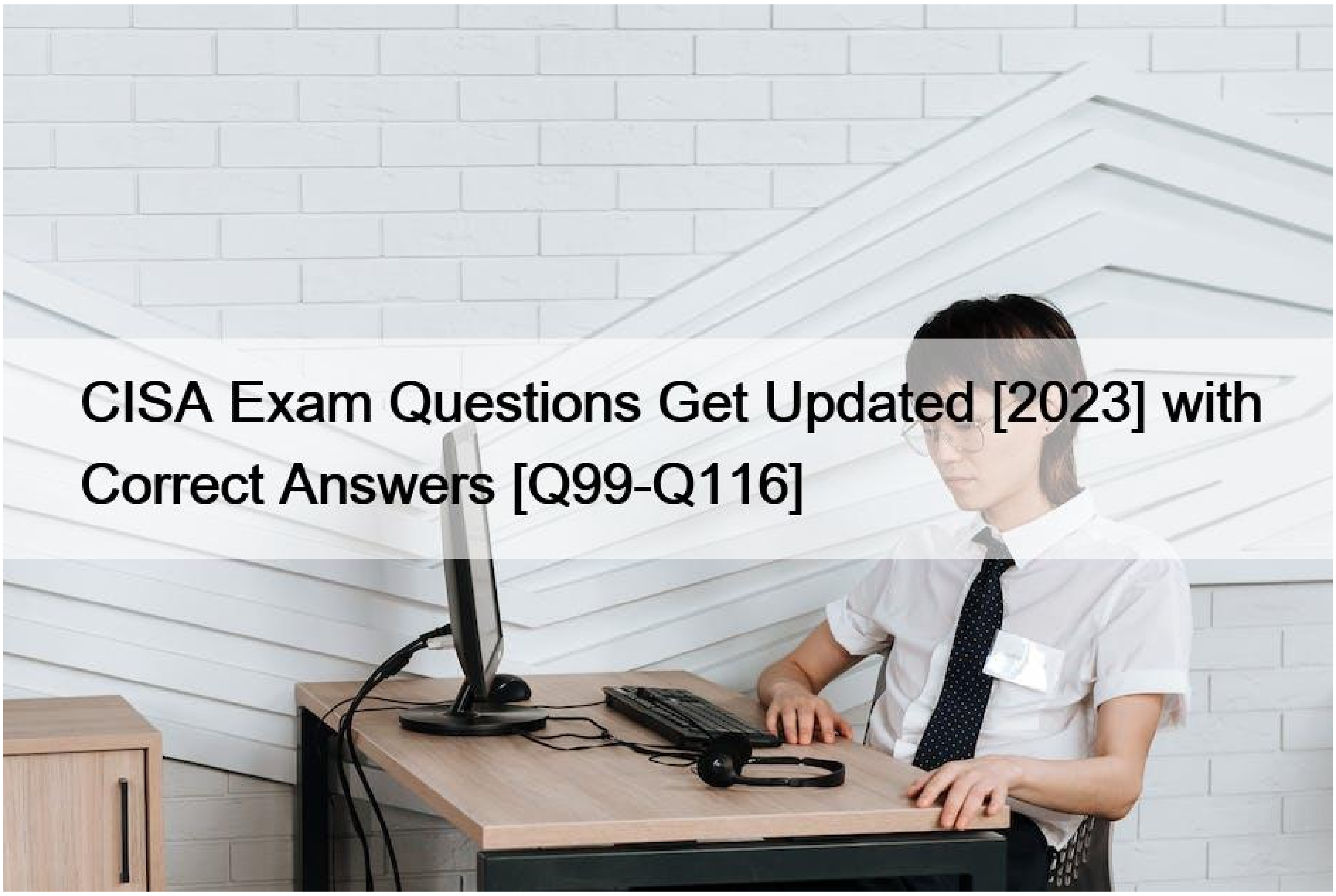
CISA Exam Questions Get Updated [2023 with Correct Answers [Q99-Q116



CISA Exam Questions Get Updated [2023] with Correct Answers
Practice CISA Questions With Certification guide Q&A from Training Expert DumpsMaterials

Q99. Which of the following falls within the scope of an information security governance committee?
* Selecting the organization&#8217;s external security auditors
* Approving access to critical financial systems
* Reviewing content for information security awareness programs
* Prioritizing information security technology initiatives

Q100. An IS auditor is planning to audit an organization&#8217;s infrastructure for access, patching, and change management. Which of the following is the BEST way to prioritize the systems?
* Complexity of the environment
* Criticality of the system
* System hierarchy within the infrastructure
* System retirement plan

Q101. An employee has accidentally posted confidential data to the company&#8217;s social media page. Which of the following is the BEST control to prevent this from recurring?

* Require all updates to be made by the marketing director
* Implement a moderator approval process
* Perform periodic audits of social media updates
* Establish two-factor access control for social media accounts
Section: Protection of Information Assets

Explanation/Reference:

Q102. At the completion of a system development project, a postproject review should include which of the following?
* Assessing risks that may lead to downtime after the production release
* Identifying lessons learned that may be applicable to future projects
* Verifying the controls in the delivered system are working
* Ensuring that test data are deleted
Explanation/Reference:

Explanation:

A project team has something to learn from each and every project. As risk assessment is a key issue for project management, it is important for the organization to accumulate lessons learned and integrate them into future projects. An assessment of potential downtime should be made with the operations group and other specialists before implementing a system. Verifying that controls are working should be covered during the acceptance test phase and possibly, again, in the postimplementation review. Test data should be retained for future regression testing.

Q103. Sending a message and a message hash encrypted by the sender&#8217;s private key will ensure:
* authenticity and integrity.
* authenticity and privacy.
* integrity and privacy.
* privacy and nonrepudiation.
Explanation/Reference:

Explanation:

If the sender sends both a message and a message hash encrypted by its private key, then the receiver can apply the sender&#8217;s public key to the hash and get the message hash. The receiver can apply the hashing algorithm to the message received and generate a hash. By matching the generated hash with the one received, the receiver is ensured that the message has been sent by the specific sender, i.e., authenticity, and that the message has not been changed enroute. Authenticity and privacy will be ensured by first using the sender&#8217;s private key and then the receiver&#8217;s public key to encrypt the message. Privacy and integrity can be ensured by using the receiver&#8217;s public key to encrypt the message and sending a message hash/digest. Only nonrepudiation can be ensured by using the sender&#8217;s private key to encrypt the message. The sender&#8217;s public key, available to anyone, can decrypt a message; thus, it does not ensure privacy.

Q104. From a control perspective, the PRIMARY objective of classifying information assets is to:
* establish guidelines for the level of access controls that should be assigned.
* ensure access controls are assigned to all information assets.
* assist management and auditors in risk assessment.
* identify which assets need to be insured against losses.
Information has varying degrees of sensitivity and criticality in meeting business objectives. By assigning classes or levels of sensitivity and criticality to information resources, management can establish guidelines for the level of access controls that should be assigned. End user management and the security administrator will use these classifications in their risk assessment process to assign a given class to each asset.

Q105. An IT balanced scorecard is PRIMARILY used for:
* evaluating the IT project portfolio
* measuring IT strategic performance
* allocating IT budget and resources
* monitoring risk in lT-related processes

Q106. The PRIMARY purpose of a configuration management system is to:
* track software updates.
* define baselines for software.
* support the release procedure.
* standardize change approval.

Q107. Private Branch Exchange(PBX) environment involves many security risks, one of which is the people both internal and external to an organization. Which of the following risks are NOT associated with Private Branch Exchange?

1. Theft of service

2. Disclosure of information

3. Data Modifications

4. Denial of service

5. Traffic Analysis
* 3 and 4
* 4 and 5
* 1-4
* They are ALL risks associated with PBX
Explanation/Reference:

The NOT is a keyword used in the question. You need to find out the risks which are NOT associated with PBX. All the risk listed within the options are associated with PBX.

The threat of the PBX telephone system are many, depending on the goals of these attackers, and include:

Theft of service &#8211; Toll fraud, probably the most common of motives for attacker.

Disclosure of Information -Data disclosed without authorization, either by deliberate actionably accident.

Examples includes eavesdropping on conversation and unauthorized access to routing and address data.

Data Modification -Data altered in some meaningful way by recording, deleting or modifying it. For example, an intruder may change billing information or modify system table to gain additional services.

Unauthorized access &#8211; Actions that permit an unauthorized user to gain access to system resources or privileges.

Denial of service -Actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.

Traffic Analysis &#8211; A form of passive attack in which an intruder observes information about calls and make inferences, e.g. from the source and destination number or frequency and length of messages. For example, an intruder observes a high volume of calls between a company&#8217;s legal department and patent office, and conclude that a patent is being filed.

The following were incorrect answers:

All the risks presented in options are associated with PBX. So other options are not valid.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number356

Q108. A hub is a device that connects:
* two LANs using different protocols.
* a LAN with a WAN.
* a LAN with a metropolitan area network (MAN).
* two segments of a single LAN.
Explanation/Reference:

Explanation:

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.

Incorrect answers:

A. 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.

B. A gateway, which is a level 7 device, is used to connect a LAN to a WAN.

C. A LAN is connected with a MAN using a router, which operates in the network layer.

Q109. Which of the following roles is ULTIMATELY accountable for the protection of an organization&#8217;s information?
* The board of directors
* The chief information security officer (CISO)
* The data owner
* The chief information officer (CIO)
Section: Protection of Information Assets

Q110. Which of the following is MOST important to include in forensic data collection and preservation procedures?
* Assuring the physical security of devices
* Maintaining chain of custody
* Determining tools to be used
* Preserving data integrity

Q111. Which of the following is MOST likely to result from compliance testing?
* Comparison of data with physical counts
* Confirmation of data with outside sources
* Identification of errors due to processing mistakes

* Discovery of controls that have not been applied

Q112. An organization wants to reuse company-provided smartphones collected from staff leaving the organization. Which of the following would be the BEST recommendation?
* The memory cards of the smartphones should be replaced.
* Data should be securely deleted from the smartphones.
* The SIM card and telephone number should be changed.
* Smartphones should not be reused, but physically destroyed.

Q113. What is the BEST control to address SQL injection vulnerabilities?
* Input validation
* Unicode translation
* Secure Sockets Layer (SSL) encryption
* Digital signatures

Q114. Which of the following is MOST important to include in an organization&#8217;s incident response plan to help prevent similar incidents from happening in the future?
* Containment and neutralization actions
* Documentation of incident details
* Incident closure procedures
* Post-incident review

Q115. Assessing IT risks is BEST achieved by:
* evaluating threats associated with existing IT assets and IT projects.
* using the firm&#8217;s past actual loss experience to determine current exposure.
* reviewing published loss statistics from comparable organizations.
* reviewing IT control weaknesses identified in audit reports.
Section: Protection of Information Assets

Explanation:

To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk

assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process,

but by themselves are not sufficient. Basing an assessment on past losses will not adequately reflect

inevitable changes to the firm&#8217;s IT assets, projects, controls and strategic environment. There are also

likely to be problems with the scope and quality of the loss data available to be assessed. Comparable

organizations will have differences in their IT assets, control environment and strategic circumstances.

Therefore, their loss experience cannot be used to directly assess organizational IT risk. Control

weaknesses identified during audits will be relevant in assessing threat exposure and further analysis may

be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not

all of the critical IT assets and projects will have recently been audited, and there may not be a sufficient assessment of strategic IT risks.

Q116. Which of the following PBX feature allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available?
* Automatic Call distribution
* Call forwarding
* Tenanting
* Voice mail
Explanation/Reference:

Automatic Call distribution allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

For your exam you should know below mentioned PBX features and Risks:

System Features

Description

Risk

Automatic Call distribution

Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Tapping and control of traffic

Call forwarding

Allow specifying an alternate number to which calls will be forwarded based on certain condition User tracking

Account codes

Used to:

Track calls made by certain people or for certain projects for appropriate billing Dial-In system access (user dials from outside and gain access to normal feature of the PBX) Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Fraud, user tracking, non authorized features

Access Codes

Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features

Silent Monitoring

Silently monitors other calls

Eavesdropping

Conferencing

Allows for conversation among several users

Eavesdropping, by adding unwanted/unknown parties to a conference

override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message Eavesdropping

Auto-answer

Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off

Gaining information not normally available, for various purpose

Tenanting

Limits system user access to only those users who belong to the same tenant group &#8211; useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc Illegal usage, fraud, eavesdropping

Voice mail

Stores messages centrally and &#8211; by using a password &#8211; allows for retrieval from inside or outside lines.

Disclosure or destruction of all messages of a user when that user&#8217;s password in known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Privacy release

Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Eavesdropping

No busy extension

Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Eavesdropping a conference in progress

Diagnostics

Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device.

It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics

Fraud and illegal usage

Camp-on or call waiting

When activated, sends a visual audible warning to an off-hook instrument that is receiving another call.

Another option of this feature is to conference with the camped-on or call waiting Making the called individual a party to a conference without knowing it.

Dedicated connections

Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility

Eavesdropping on a line

The following were incorrect answers:

Call forwarding &#8211; Allow specifying an alternate number to which calls will be forwarded based on certain condition

Tenanting &#8211; Limits system user access to only those users who belong to the same tenant group useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Voice Mail &#8211; Stores messages centrally and &#8211; by using a password &#8211; allows for retrieval from inside or outside lines.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 358