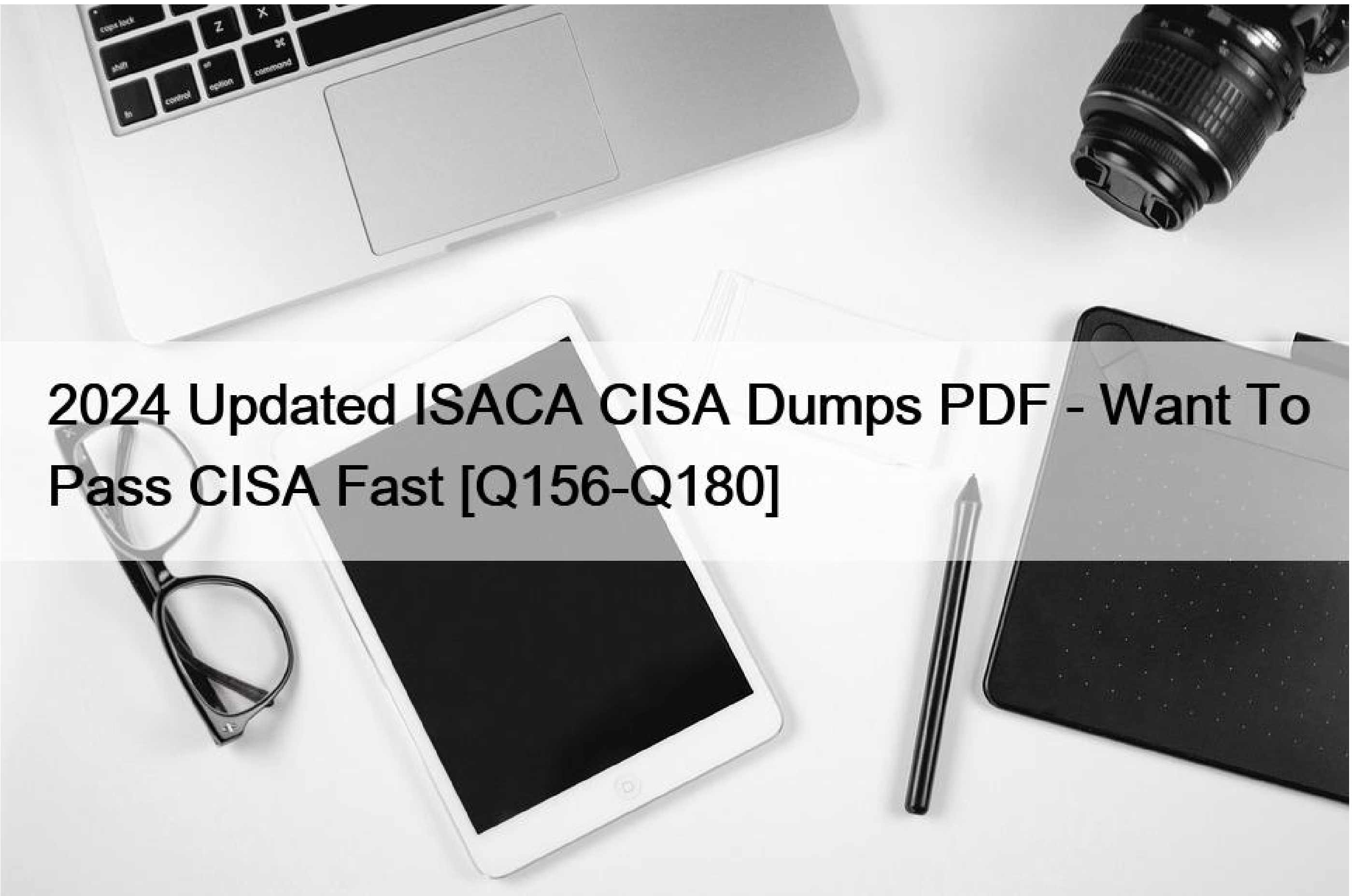
2024 Updated ISACA CISA Dumps PDF - Want To Pass CISA Fast [Q156-Q180



2024 Updated ISACA CISA Dumps PDF - Want To Pass CISA Fast CISA Practice Exam Dumps - 99% Marks In ISACA Exam

ISACA CISA certification is beneficial for individuals who want to work in the field of IT audit, risk management, and compliance. Certified Information Systems Auditor certification is also valuable for professionals who want to enhance their knowledge and skills in information security and control. The CISA certification is recognized by many organizations worldwide and can help professionals advance their careers and increase their earning potential.

NEW QUESTION 156

During a security audit, which of the following is MOST important to review to ensure data confidentiality is managed?
* Access log monitoring
* Network configuration
* Access controls
* Data flows

NEW QUESTION 157

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

* Cyclic integrity
* Domain integrity
* Relational integrity
* Referential integrity

Explanation/Reference:

Explanation:

Referential integrity ensures that a foreign key in one table will equal null or the value of a primary in the other table. For every tuple in a table having a referenced/foreign key, there should be a corresponding tuple in another table, i.e., for existence of all foreign keys in the original tables, if this condition is not satisfied, then it results in a dangling tuple. Cyclical checking is the control technique for the regular checking of accumulated data on a file against authorized source documentation. There is no cyclical integrity testing. Domain integrity testing ensures that a data item has a legitimate value in the correct range or set. Relational integrity is performed at the record level and is ensured by calculating and verifying specific fields.

NEW QUESTION 158

An IS auditor finds that conference rooms have active network ports. Which of the

following is MOST important to ensure?

* The corporate network is using an intrusion prevention system (IPS)
* This part of the network is isolated from the corporate network
* A single sign-on has been implemented in the corporate network
* Antivirus software is in place to protect the corporate network

If the conference rooms have access to the corporate network, unauthorized users may be able to connect to the corporate network; therefore, both networks should be isolated either via a firewall or being physically separated. An I PS would detect possible attacks, but only after they have occurred. A single sign-on would ease authentication management. Antivirus software would reduce the impact of possible viruses; however, unauthorized users would still be able to access the corporate network, which is the biggest risk.

NEW QUESTION 159

Which of the following provides the MOST protection against emerging threats?

* Demilitarized zone (DMZ)
* Heuristic intrusion detection system (IDS)
* Real-time updating of antivirus software
* Signature-based intrusion detection system (IDS)

Explanation

A heuristic intrusion detection system (IDS) provides the most protection against emerging threats, as it uses behavioral analysis and anomaly detection to identify unknown or zero-day attacks. A heuristic IDS can adapt to changing patterns and learn from previous incidents, making it more effective than a signature-based IDS, which relies on predefined rules and signatures to detect known attacks. A demilitarized zone (DMZ) is a network segment that separates the internal network from the external network, and it can provide some protection against external threats, but not against internal or emerging threats. Real-time updating of antivirus software is important to protect against malware, but it may not be sufficient to prevent new or sophisticated attacks that exploit unknown vulnerabilities. References: CISA Review Manual (Digital Version) 1, page

452-453.

NEW QUESTION 160

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.

NEW QUESTION 161

What is a risk associated with attempting to control physical access to sensitive areas such as computer rooms using card keys or locks?
* Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.
* The contingency plan for the organization cannot effectively test controlled access practices.
* Access cards, keys and pads can be easily duplicated allowing easy compromise of the control.
* Removing access for those who are no longer authorized is complex.
Explanation/Reference:

Explanation:

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, while technology is constantly changing, card keys have existed for some time and appear to be a viable option for the foreseeable future.

NEW QUESTION 162

Which of the following are BEST suited for continuous auditing?
* Manual transactions
* Irregular transactions
* Low-value transactions
* Real-time transactions

NEW QUESTION 163

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

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

Section: Protection of Information Assets

Explanation:

Although the primary business objective of BCP and DRP is to mitigate the risk and impact of a business

interruption, the dominating objective remains the protection of human life.

NEW QUESTION 164

Which of the following would BEST manage the risk of changes in requirements after the analysis phase of a business application development project?

* Expected deliverables meeting project deadlines
* Sign-off from the IT team
* Ongoing participation by relevant stakeholders
* Quality assurance (OA) review

NEW QUESTION 165

An organization recently implemented a cloud document storage solution and removed the ability for end users to save data to their local workstation hard drives. Which of the following findings should be the IS auditor&#8217;s GREATEST concern?

* Users are not required to sign updated acceptable use agreements.
* Users have not been trained on the new system.
* The business continuity plan (BCP) was not updated.
* Mobile devices are not encrypted.

Explanation

This should be the IS auditor&#8217;s greatest concern, because it means that the organization has not considered the potential impact of the cloud document storage solution on its ability to continue its operations in the event of a disruption or disaster. A BCP is a document that outlines the procedures and actions to be taken in order to maintain or resume critical business functions during and after a crisis. A BCP should be updated whenever there is a significant change in the organization&#8217;s IT infrastructure, systems, processes, or dependencies, such as implementing a cloud document storage solution. The IS auditor should verify that the BCP reflects the current state of the organization&#8217;s IT environment, and that it addresses the risks, challenges, and opportunities associated with the cloud document storage solution.

The other options are not as concerning as the BCP not being updated:

Users are not required to sign updated acceptable use agreements. This is a minor concern, but it does not pose a major threat to the organization&#8217;s business continuity. Acceptable use agreements are documents that define the rules and guidelines for using IT resources, such as the cloud document storage solution. Users should sign updated acceptable use agreements to acknowledge their responsibilities and obligations, and to comply with the organization&#8217;s policies and standards. However, this does not affect the organization&#8217;s ability to continue its operations in a crisis.

Users have not been trained on the new system. This is a moderate concern, but it does not jeopardize the organization&#8217;s business continuity. Training users on the new system is important to ensure that they can use it effectively and efficiently, and to avoid errors or misuse that could compromise the security or performance of the system. However, this does not prevent the organization from accessing or restoring its data in a crisis.

Mobile devices are not encrypted. This is a serious concern, but it does not directly impact the organization&#8217;s business continuity. Encrypting mobile devices is a security measure that protects the data stored on them from unauthorized access or disclosure in case of loss or theft. However, this does not affect the availability or integrity of the data stored in the cloud document storage solution, which should have its own encryption mechanisms.

NEW QUESTION 166

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:
* critical.
* vital.
* sensitive.
* noncritical.
Explanation/Reference:

Explanation:

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.

NEW QUESTION 167

Digital signatures are an effective control method for information exchange over an insecure network because they:
* enable nonrepudiation.
* are under the sole custody of the receiver.
* are constant over time.
* authenticate the user biometrically.
Section: Protection of Information Assets

NEW QUESTION 168

An IS auditor is reviewing a bank&#8217;s service level agreement (SLA) with a third-party provider that hosts the bank&#8217;s secondary data center, which of the following findings should be of GREATEST concern to the auditor?
* The recovery time objective (RTO) has a longer duration than documented in the disaster recovery plan (ORP).
* The SLA has not been reviewed in more than a year.
* Backup data is hosted online only.
* The recovery point objective (RPO) has a shorter duration than documented in the disaster recovery plan (DRP).
Explanation

The recovery time objective (RTO) has a longer duration than documented in the disaster recovery plan (DRP) should be of greatest concern to the auditor when reviewing a bank&#8217;s SLA with a third-party provider that hosts the bank&#8217;s secondary data center. This is because the RTO is the maximum acceptable time for restoring a system or an application after a disaster or a disruption. A longer RTO than the DRP means that the bank may not be able to resume its critical business operations within the expected time frame, which may result in significant financial losses, reputational damage, customer dissatisfaction, or regulatory non-compliance12.

The SLA has not been reviewed in more than a year is not the greatest concern, although it is a good practice to review and update the SLA periodically to ensure that it reflects the current business needs and expectations, as well as any changes in the service provider&#8217;s capabilities or performance. However, a lack of review does not necessarily imply a lack of compliance or quality of service, as long as the SLA is still valid and enforceable34.

Backup data is hosted online only is not the greatest concern, although it may pose some security risks if the backup data is not encrypted or protected by adequate access controls. Online backup data means that the backup data is stored on a remote server that can be accessed via the Internet, which may offer some advantages such as faster recovery, lower cost, and higher availability than offline backup data that is stored on physical media such as tapes or disks. However, online backup data also requires reliable network connectivity and bandwidth, as well as proper security measures to prevent unauthorized access or tampering56.

The recovery point objective (RPO) has a shorter duration than documented in the DRP is not the greatest concern, although it may indicate some inconsistency or misalignment between the SLA and the DRP. The RPO is the maximum acceptable amount of data loss measured in time from a disaster or a disruption. A shorter RPO than the DRP means that the bank may lose less data than expected, which may be beneficial for its business continuity and recovery. However, a shorter RPO may also imply more frequent backups, which may increase the cost and complexity of the backup process

NEW QUESTION 169

Which of the following reports should an IS auditor use to check compliance with a service level agreement&#8217;s (SLA) requirement for uptime?
* Utilization reports
* Hardware error reports
* System logs
* Availability reports
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 corrective action. System logs are a recording of the system&#8217;s activities.

NEW QUESTION 170

What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off? Choose the BEST answer.
* Employee security awareness training
* Administrator alerts
* Screensaver passwords
* Close supervision
Explanation/Reference:

Screensaver passwords are an effective control to implement as a countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off.

NEW QUESTION 171

An IS auditor finds that periodic reviews of read-only users for a reporting system are not being performed.

Which of the following should be the IS auditor&#8217;s NEXT course of action?

- Review the list of end users and evaluate for authorization.
- Report this control process weakness to senior management.
- Verify managements approval for this exemption
- Obtain a verbal confirmation from IT for this exemption.

Explanation

The IS auditor&#8217;s next course of action should be to report this control process weakness to senior management, as it may indicate a lack of oversight and accountability for the reporting system. Read-only users may have access to sensitive or confidential information that should be restricted or monitored. Periodic reviews of read-only users are a good practice to ensure that the access rights are still valid and appropriate for the users&#8217; roles and responsibilities. Reporting this weakness to senior management will also allow them to take corrective actions or implement compensating controls if needed.

Option A is incorrect because reviewing the list of end users and evaluating for authorization is not the IS auditor&#8217;s responsibility, but rather the system owner&#8217;s or administrator&#8217;s. The IS auditor should only verify that such reviews are performed and documented by the responsible parties.

Option C is incorrect because verifying management&#8217;s approval for this exemption is not sufficient to address the control process weakness. Even if there is a valid reason for not performing periodic reviews of read-only users, the IS auditor should still report this as a potential risk and recommend mitigating controls.

Option D is incorrect because obtaining a verbal confirmation from IT for this exemption is not adequate evidence or documentation. The IS auditor should obtain written approval from management and verify that it is aligned with the organization&#8217;s policies and standards.

References:

CISA Review Manual (Digital Version)1, Chapter 1: The Process of Auditing Information Systems, Section 1.4: Audit Evidence, p. 31-32.

CISA Review Manual (Print Version), Chapter 1: The Process of Auditing Information Systems, Section

1.4: Audit Evidence, p. 31-32.

CISA Online Review Course2, Module 1: The Process of Auditing Information Systems, Lesson 4:

Audit Evidence, slide 9-10.

CISA Questions, Answers & Explanations Database3, Question ID: QAE_CISA_710.

NEW QUESTION 172

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

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

NEW QUESTION 173

Which of following is MOST important to determine when conducting a post-implementation review?
* Whether the solution architecture compiles with IT standards
* Whether success criteria have been achieved
* Whether the project has been delivered within the approved budget
* Whether lessons teamed have been documented
Explanation

The most important thing to determine when conducting a post-implementation review is whether success criteria have been achieved. A post-implementation review is a process of evaluating the results and outcomes of a project or initiative after it has been completed and implemented. The success criteria are the measurable indicators that define what constitutes a successful project or initiative in terms of its objectives, benefits, quality, performance, and stakeholder satisfaction. The IS auditor should verify whether the success criteria have been achieved by comparing the actual results and outcomes with the expected or planned ones, and by assessing whether they meet or exceed the expectations and requirements of the stakeholders. The IS auditor should also identify any gaps, issues, or risks that may affect the sustainability or scalability of the project or initiative, and provide recommendations for improvement or remediation. The other options are not as important as determining whether success criteria have been achieved when conducting a post-implementation review, because they either focus on specific aspects or components of the project or initiative rather than the overall value proposition, or they are part of the pre-implementation or implementation phases rather than the post-implementation phase. References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.3

NEW QUESTION 174

Which of the following activities should an IS auditor perform FIRST during an external network security assessment?
* Enumeration
* Reconnaissance
* Exploitation
* Vulnerability scanning

NEW QUESTION 175

Which of the following controls should be implemented to BEST minimize system downtime for maintenance?
* Nightly full backups
* Virtualization
* Warm site
* Clustering
Section: Information System Acquisition, Development and Implementation

NEW QUESTION 176

Which of the following is the PRIMARY advantage of using virtualization technology for corporate applications?
* Increased application performance
* Improved disaster recovery
* Stronger data security
* Better utilization of resources

NEW QUESTION 177

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

* format string vulnerabilities
* integer misappropriation
* code injection
* None of the choices.

A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data.

NEW QUESTION 178

Following a security breach m which a hacker exploited a well-known vulnerability in the domain controller, an IS auditor has been asked to conduct a control assessment. The auditor&#8217;s BEST course of action would be to determine if:

* the network traffic was being monitored.
* the patches were updated.
* the domain controller was classified for high availability.
* the logs were monitored.

NEW QUESTION 179

.What is the primary security concern for EDI environments? Choose the BEST answer.

* Transaction authentication
* Transaction completeness
* Transaction accuracy
* Transaction authorization

Transaction authorization is the primary security concern for EDI environments.

NEW QUESTION 180

A retirement system verifies that the field for employee status has either a value of A (for active) or R (for retired). This is an example of which type of check?

* Validity
* Existence
* Limit
* Completeness

Section: Protection of Information Assets

Updated Verified CISA Q&As - Pass Guarantee: https://www.validbraindumps.com/CISA-exam-prep.html]