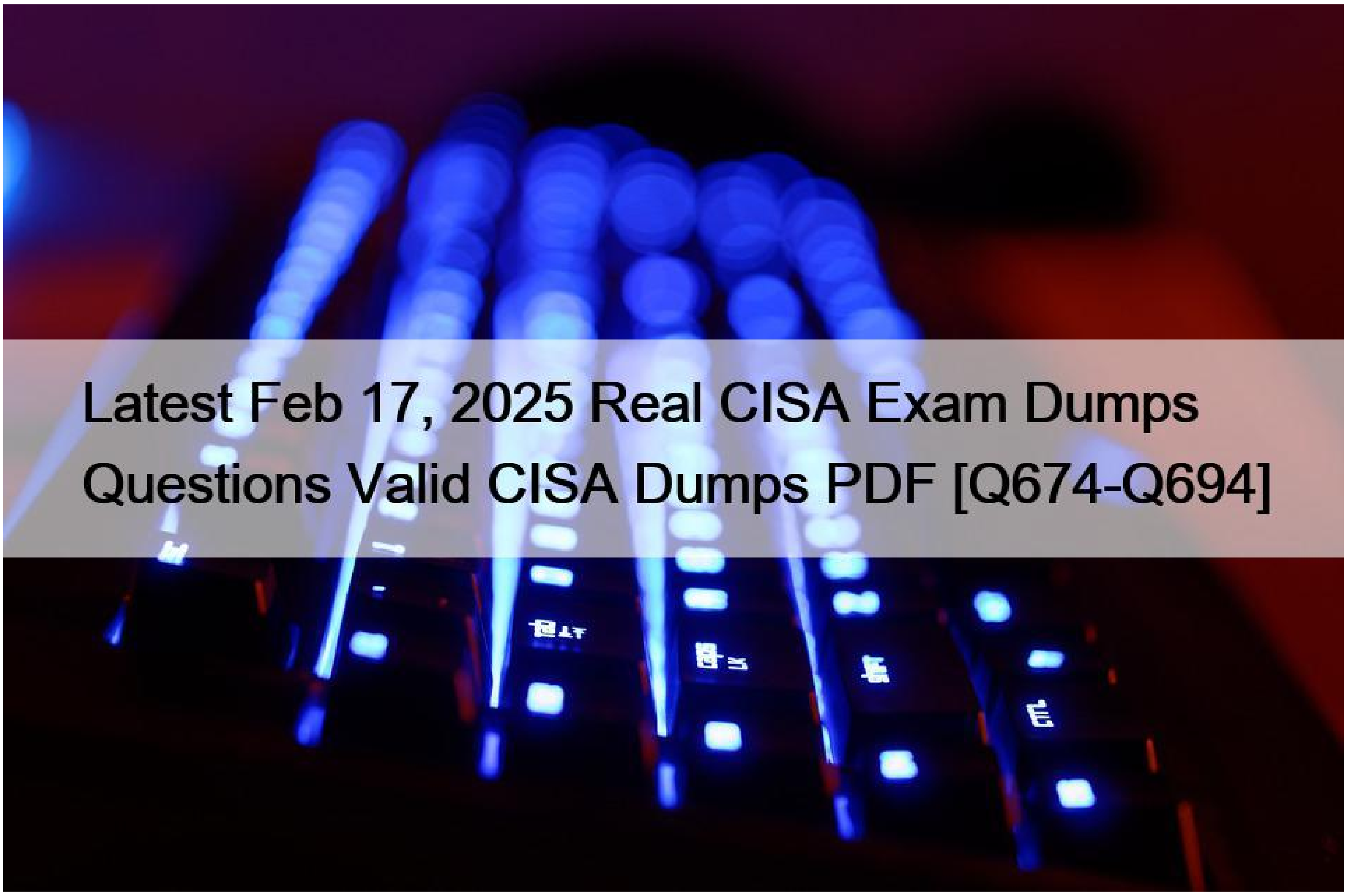
Latest Feb 17, 2025 Real CISA Exam Dumps Questions Valid CISA Dumps PDF [Q674-Q694



Latest Feb 17, 2025 Real CISA Exam Dumps Questions Valid CISA Dumps PDF
ISACA CISA Exam Dumps - PDF Questions and Testing Engine

The Certified Information Systems Auditor (CISA) certification is offered by ISACA (Information Systems Audit and Control Association) and is a globally recognized certification for professionals in the field of information systems (IS) auditing, control, and security. The CISA certification is designed to provide a comprehensive understanding of the auditing process, including risk management, governance, and IT compliance. Certified Information Systems Auditor certification is highly respected in the industry and is considered a benchmark for information systems audit, control, and security professionals.

As a renowned validation among tech specialists, the Isaca CISA exam can strategically help in plotting your career goals. This certification test is designed to fortify your command in information systems and management. It's one of the most practical validations for mid-career individuals eyeing to take the next step in their careers.

The CISA certification exam is designed for IT professionals who have experience in information systems auditing, control, and security. CISA exam covers various areas such as information systems auditing, risk management, IT governance, and information security management. CISA exam consists of 150 multiple-choice questions that are to be completed within four hours. CISA exam is graded on a scale of 200-800, with a passing score of 450.

QUESTION 674

An IS auditor is scheduled to conduct a follow-up and is told by operational management that new priorities prevented them from implementing the action plan. Management plans to address the audit issues after the next quarter. What should be the auditor&#8217;s NEXT course of action?
* Defer the follow-up engagement for later in the year.
* Report management&#8217;s lack of action to the audit committee.
* Assess the risk of the delayed implementation.
* Conduct the follow-up engagement as scheduled.

QUESTION 675

An IS auditor reviewing an information processing environment decides to conduct external penetration testing. Which of the following is MOST appropriate to include in the audit scope for the organization to distinguish between the auditor&#8217;s penetration attacks and actual attacks?
* Restricted host IP addresses of simulated attacks
* Testing techniques of simulated attacks
* Source IP addresses of simulated attacks
* Timing of simulated attacks

QUESTION 676

A development team has designed a new application and incorporated best practices for secure coding. Prior to launch, which of the following is the IS auditor&#8217;s BEST recommendation to mitigate the associated security risk?
* Integration testing
* Unit testing
* Penetration testing
* User acceptance testing

QUESTION 677

A finance department has a two-year project to upgrade the enterprise resource planning (ERP) system hosting the general ledger in year one the system version upgrade will be applied and in year two business processes will be updated to implement new system functionality. Which of the following should be the PRIMARY focus of an IS auditor reviewing the second year of the implementation&#8217;?
* Data migration
* Sociability testing
* User acceptance testing (UAT)
* Initial user access provisioning

During the second year of the ERP system upgrade project, the focus shifts to ensuring that the updated business processes integrate seamlessly with the new system functionality. User acceptance testing (UAT) validates that the system meets user requirements and business objectives.

* Data Migration (Option A): Data migration is more relevant in the first phase when upgrading the system version.

* Sociability Testing (Option B): This is less critical than confirming user functionality for process changes.

* Initial User Access Provisioning (Option D): This is part of security and access controls but not the primary focus of business process validation.

Reference: ISACA CISA Review Manual, Job Practice Area 3: Information Systems Operations and Business Resilience.

QUESTION 678

In a multinational organization, local security regulations should be implemented over global security policy because:

* global security policies include unnecessary controls for local businesses
* business objectives are defined by local business unit managers
* requirements of local regulations take precedence
* deploying awareness of local regulations is more practical than of global policy

Section: Governance and Management of IT

QUESTION 679

What would be an IS auditor&#8217;s BEST recommendation upon finding that a third-party IT service provider

hosts the organization&#8217;s human resources (HR) system in a foreign country?

* Conduct a privacy impact analysis.
* Implement change management review.
* Review third-party audit reports.
* Perform background verification checks.

Section: Information System Acquisition, Development and Implementation

QUESTION 680

Which of the following findings would be of GREATEST concern to an IS auditor performing an information

security audit of critical server log management activities?

* Log records can be overwritten before being reviewed.
* Logging procedures are insufficiently documented.
* Log records are dynamically into different servers.
* Logs are monitored using manual processes.

Section: Governance and Management of IT

QUESTION 681

Which of the following would be the BEST performance indicator for the effectiveness of an incident

management program?

* Incident alert meantime
* Average time between incidents
* Number of incidents reported
* Incident resolution meantime

Section: Protection of Information Assets

QUESTION 682

Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?
* Restricting evidence access to professionally certified forensic investigators
* Documenting evidence handling by personnel throughout the forensic investigation
* Performing investigative procedures on the original hard drives rather than images of the hard drives
* Engaging an independent third party to perform the forensic investigation
Explanation

The most important factor to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings is to document evidence handling by personnel throughout the forensic investigation. Documentation is essential to establish the chain of custody, prove the integrity and authenticity of the evidence, and demonstrate compliance with legal and ethical standards. Documentation should include information such as the date, time, location, source, destination, method, purpose, result, and authorization of each action performed on the evidence. Documentation should also include any observations, findings, assumptions, limitations, or exceptions encountered during the investigation. References:

CISA Review Manual (Digital Version)

CISA Questions, Answers & Explanations Database

QUESTION 683

During an IS audit of a data center, it was found that programmers are allowed to make emergency fixes to

operational programs. Which of the following should be the IS auditor&#8217;s PRIMARY recommendation?
* Bypass use ID procedures should be put in place to ensure that the changes are subject to after-the-

event approval and testing
* The ability to undertake emergency fixes should be restricted to selected key personnel
* Programmers should be allowed to implement emergency fixes only after obtaining verbal agreement

from the application owner
* Emergency program changes should be subject to program migration and testing procedures before

they are applied to operational systems
Section: Information System Operations, Maintenance and Support

QUESTION 684

Which of the following would an IS auditor consider to be the MOST important when evaluating an organization&#8217;s IS strategy? That it:
* has been approved by line management.
* does not vary from the IS department&#8217;s preliminary budget.
* complies with procurement procedures.
* supports the business objectives of the organization.
Explanation/Reference:

Explanation:

Strategic planning sets corporate or department objectives into motion. Both long-term and short-term strategic plans should be consistent with the organization&#8217;s broader plans and business objectives for attaining these goals. Choice A is incorrect since line management prepared the plans.

QUESTION 685

Which of the following typically focuses on making alternative processes and resources available for transaction processing?
* Cold-site facilities
* Disaster recovery for networks
* Diverse processing
* Disaster recovery for systems
Explanation/Reference:

Explanation:

Disaster recovery for systems typically focuses on making alternative processes and resources available for transaction processing.

QUESTION 686

During a follow-up audit, an IS auditor finds that some critical recommendations have not been addressed as management has decided to accept the risk. Which of the following is the IS auditor&#8217;s BEST course of action?
* Adjust the annual risk assessment accordingly.
* Update the audit program based on management&#8217;s acceptance of risk.
* Evaluate senior managements acceptance of the risk.
* Require the auditee to address the recommendations in full.

QUESTION 687

While conducting an audit of a service provider, an IS auditor observes that the service provider has

outsourced a part of the work to another provider. Since the work involves confidential information, the IS

auditor&#8217;s PRIMARY concern should be that the:
* requirement for protecting confidentiality of information could be compromised.
* contract may be terminated because prior permission from the outsourcer was not obtained.
* other service provider to whom work has been outsourced is not subject to audit.
* outsourcer will approach the other service provider directly for further work.
Section: Protection of Information Assets

Explanation:

Many countries have enacted regulations to protect the confidentiality of information maintained in their

countries and/or exchanged with other countries. Where a service provider outsources part of its services

to another service provider, there is a potential risk that the confidentiality of the information will be

compromised. Choices B and C could be concerns but are no related to ensuring the confidentiality of

information. There is no reason why an IS auditor should be concerned with choice D.

QUESTION 688

In a botnet, malbot logs into a particular type of system for making coordinated attack attempts. What type of system is this?
* Chat system
* SMS system
* Email system
* Log system
* Kernel system
* None of the choices.
In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as botnets . In a botnet , the malware or malbot logs in to an Internet Relay Chat channel or other chat system. The attacker can then give instructions to all the infected systems simultaneously.

QUESTION 689

The MAJOR advantage of a component-based development approach is the:
* ability to manage an unrestricted variety of data types.
* provision for modeling complex relationships.
* capacity to meet the demands of a changing environment.
* support of multiple development environments.
Components written in one language can interact with components written in other languages or running on other machines, which can increase the speed of development. Software developers can then focus on business logic. The other choices are not themost significant advantages of a component-based development approach.

QUESTION 690

An IS auditor concludes that a local area network&#8217;s (LAN&#8217;s) access security is satisfactory. In reviewing the work, the audit manager should:
* re-perform some steps of the audit to verify the quality of the work.
* verify that the elements of an agreed-upon audit plan have been addressed.
* verify user management&#8217;s agreement with the findings.
* assess whether the auditor had the appropriate skills to perform the work.
Section: The process of Auditing Information System

QUESTION 691

Documentation of workaround processes to keep a business function operational during recovery of IT systems is a core part of a:
* business continuity plan.
* business impact analysis.
* threat and risk assessment
* disaster recovery plan

QUESTION 692

Which of the following is MOST important to determine when conducting an audit Of an organization&#8217;s data privacy practices?
* Whether a disciplinary process is established for data privacy violations
* Whether strong encryption algorithms are deployed for personal data protection
* Whether privacy technologies are implemented for personal data protection
* Whether the systems inventory containing personal data is maintained
The systems inventory containing personal data is a crucial element for auditing an organization&#8217;s data privacy practices.

The systems inventory is a list of all the systems, applications, databases, and devices that collect, store, process, or transmit personal data within the organization12. The systems inventory helps the auditor to identify the scope, location, ownership, and classification of personal data, as well as the risks and controls associated with them12. The systems inventory also helps the auditor to verify compliance with data privacy laws, regulations, and internal policies that apply to different types of personal data

QUESTION 693

When auditing the security architecture of an online application, an IS auditor should FIRST review the:
* firewall standards.
* configuration of the firewall
* firmware version of the firewall
* location of the firewall within the network

Explanation

The security architecture of an online application is a design that describes how various security components and controls are integrated and configured to protect the application from internal and external threats. When auditing the security architecture of an online application, an IS auditor should first review the location of the firewall within the network, as this determines how effectively the firewall can filter and monitor the traffic between different network segments and zones. The firewall standards, configuration, and firmware version are also important aspects to review, but they are secondary to the location of the firewall.

QUESTION 694

An organization decides to establish a formal incident response capability with clear roles and responsibilities facilitating centralized reporting of security incidents. Which type of control is being implemented?
* Corrective control
* Compensating control
* Preventive control
* Detective control

Reliable Certified Information Systems Auditor CISA Dumps PDF Feb 17, 2025 Recently Updated Questions: https://www.dumpsmaterials.com/CISA-real-torrent.html]