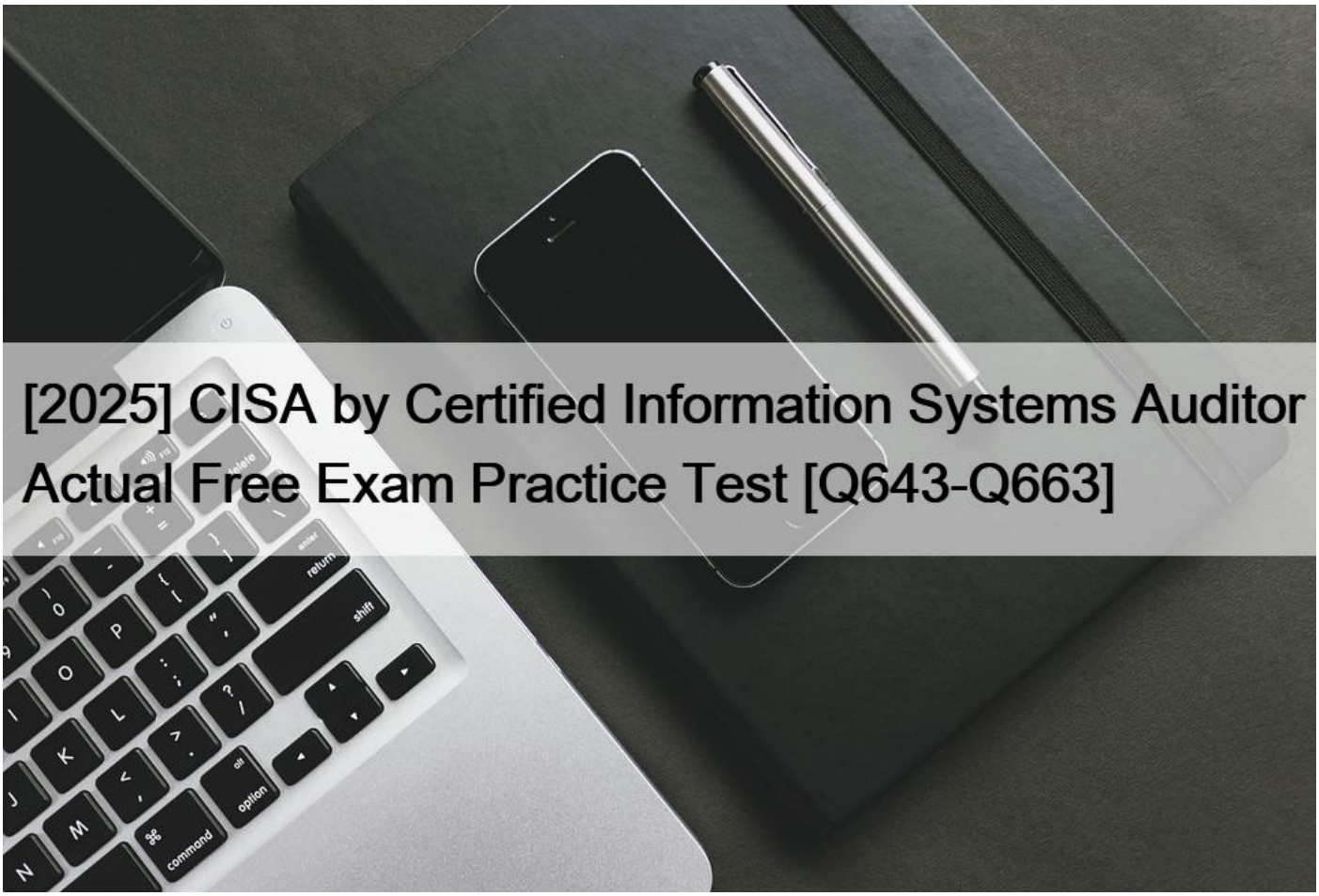
[2025 CISA by Certified Information Systems Auditor Actual Free Exam Practice Test [Q643-Q663



[2025] CISA by Certified Information Systems Auditor Actual Free Exam Practice Test
Free Certified Information Systems Auditor CISA Exam Question

The CISA Exam consists of four domains: Information Systems Auditing Process, Governance and Management of IT, Information Systems Acquisition, Development and Implementation, and Information Systems Operations, Maintenance and Support. Each domain covers a different set of topics related to information systems auditing, such as risk management, control frameworks, IT governance, and security controls. CISA exam is four hours long and consists of 150 multiple-choice questions.

Career Prospects for Successful Exam-Passers

Any successful candidate who manages to pass the ISACA CISA certification exam can take the role of information systems auditor in international companies. According to Payscale.com, a mid-level auditor with a minimum of 5-9 years of experience can get an annual salary of $75k.

QUESTION 643

An IS auditor has found that an organization is unable to add new servers on demand in a cost-efficient manner Which of the following is the auditor s BEST recommendation?
* Upgrade hardware to newer technology.
* Increase the capacity of existing systems.
* Build a virtual environment
* Hire temporary contract workers for the IT function.

QUESTION 644

Which of the following audit is mainly designed to evaluate the internal control structure in a given process or area?
* Compliance Audit
* Financial Audit
* Operational Audit
* Forensic audit

Section: The process of Auditing Information System

Explanation:

Operational audit is mainly designed to evaluate the internal control structure in a given process or area.

Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives. Operational audit is a more comprehensive form of an Internal audit.

For your exam you should know below information about different types of audit:

What is an audit?

An audit in general terms is a process of evaluating an individual or organization’s accounts. This is usually done by an independent auditing body. Thus, audit involves a competent and independent person obtaining evidence and evaluating it objectively with regard to a given entity, which in this case is the subject of audit, in order to establish conformance to a given set of standards. Audit can be on a person, organization, system, enterprise, project or product.

Compliance Audit

A compliance audit is a comprehensive review of an organization’s adherence to regulatory guidelines.

Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

What, precisely, is examined in a compliance audit will vary depending upon whether an organization is a public or private company, what kind of data it handles and if it transmits or stores sensitive financial data.

For instance, SOX requirements mean that any electronic communication must be backed up and secured with reasonable disaster recovery infrastructure. Health care providers that store or transmit e-health records, like personal health information, are subject to HIPAA requirements. Financial services companies that transmit credit card data are subject to PCI DSS requirements. In each case, the organization must be able to demonstrate compliance by producing an audit trail, often generated by data from event log

management software.

Financial Audit

A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework.

The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

Operational Audit

Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives. Operational audit is a more comprehensive form of an Internal audit.

The Institute of Internal Auditor (IIA) defines Operational Audit as a systematic process of evaluating an organization’s effectiveness, efficiency and economy of operations under management’s control and reporting to appropriate persons the results of the evaluation along with recommendations for improvement.

Objectives

To appraise the effectiveness and efficiency of a division, activity, or operation of the entity in meeting organizational goals.

To understand the responsibilities and risks faced by an organization.

To identify, with management participation, opportunities for improving control.

To provide senior management of the organization with a detailed understanding of the Operations.

Integrated Audits

An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess overall objectives within an organization, related to financial information and asset, safeguarding, efficiency and or internal auditors and would include compliance test of internal controls and substantive audit step.

IS Audit

An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization’s goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

The primary functions of an IT audit are to evaluate the systems that are in place to guard an organization’s information. Specifically, information technology audits are used to evaluate the organization’s ability to protect its information assets and to properly dispense information to authorized parties. The IT audit aims to evaluate the following:

Will the organization’s computer systems be available for the business at all times when required? (known as availability) Will the information in the systems be disclosed only to authorized users? (known as security and confidentiality) Will the information provided by the system always be accurate, reliable, and timely? (measures the integrity) In this way, the audit hopes to assess the risk to the company’s valuable asset (its information) and establish methods of minimizing those risks.

Forensic Audit

Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence – in a predefined context – in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

The purpose of a forensic audit is to use accounting procedures to collect evidence for the prosecution or investigation of financial crimes such as theft or fraud. Forensic audits may be conducted to determine if wrongdoing occurred, or to gather materials for the case against an alleged criminal.

The following answers are incorrect:

Compliance Audit – A compliance audit is a comprehensive review of an organization’s adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

Financial Audit- A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

Forensic Audit – Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence – in a predefined context – in the area of legal/ financial disputes and or irregularities (including fraud) and giving preventative advice.

Reference:

CISA Review Manual 2014 Page number 44

http://searchcompliance.techtarget.com/definition/compliance-audit

http://en.wikipedia.org/wiki/Financial_audit

http://en.wikipedia.org/wiki/Operational_auditing

http://en.wikipedia.org/wiki/Information_technology_audit

http://www.investorwords.com/16445/forensic_audit.html

QUESTION 645

During the implementation of an enterprise resource planning (ERP) system, an IS auditor is reviewing the results of user acceptance testing (UAT). The auditor’s PRIMARY focus should be to determine if:
* the business process owner has signed off on the results.
* system integration testing was performed.
* all errors found in the testing process have been corrected.
* application interfaces have been satisfactorily tested.

QUESTION 646

After delivering an audit report, the audit manager discovers that evidence was overlooked during the audit This evidence indicates that a procedural control may have failed and could contradict a conclusion of the audit Which of the following risks is MOST affected by this oversight?
* Inherent
* Operational
* Audit
* Financial

QUESTION 647

Fourth-Generation Languages (4GLs) are most appropriate for designing the application’s graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures. True or false?
* True
* False

Explanation/Reference:

Fourth-generation languages(4GLs) are most appropriate for designing the application’s graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures.

QUESTION 648

Which of the following is a distinctive feature of the Secure Electronic Transactions (SET) protocol when used for electronic credit card payments?
* The buyer is assured that neither the merchant nor any other party can misuse their credit card data.
* All personal SET certificates are stored securely in the buyer’s computer.
* The buyer is liable for any transaction involving his/her personal SET certificates.
* The payment process is simplified, as the buyer is not required to enter a credit card number and an expiration date.

The usual agreement between the credit card issuer and the cardholder stipulates that the cardholder assumes responsibility for any use of their personal SET certificates for e-commerce transactions. Depending upon the agreement between the merchant and the buyer’s credit card issuer, the merchant will have access to the credit card number and expiration date. Secure data storage in the buyer’s computer (local computer security) is not part of the SET standard. Although the buyer is not required to enter their credit card data, they will have to handle the wallet software.

QUESTION 649

Which of the following is an example of personally identifiable information (PII)?
* Office address
* Marital status
* Passport number

* Date of birth

QUESTION 650

An organization is in the process of deciding whether to allow a bring your own device (BYOD) program. If approved, which of the following should be the FIRST control required before implementation?
* Device baseline configurations
* Device registration
* An acceptable use policy
* An awareness program

Section: Information System Acquisition, Development and Implementation

QUESTION 651

Which of the following is the BEST detective control for a job scheduling process involving data transmission?
* Jobs are scheduled to be completed daily end data is transmitted using a secure Fife Transfer Protocol (FTP)
* Job failure alerts are automatically generated and routed to support personnel
* Metrics denoting the volume of monthly job failures are reported and reviewed by senior management
* Jobs are scheduled and a log of this activity n retained for subsequent review

QUESTION 652

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.

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.

QUESTION 653

Of the following, who is accountable for ensuring the representation of major stakeholders involved in a project?
* Change control board
* Steering committee
* Project management office (PMO)
* Project manager

QUESTION 654

The record-locking option of a database management system (DBMS) serves to.
* eliminate the risk of concurrent updates to a record
* allow database administrators (DBAs) to record the activities of users.
* restrict users from changing certain values within records.
* allow users to lock others out of their files.

The record-locking option of a database management system (DBMS) serves to eliminate the risk of concurrent updates to a record by different users or transactions. Record locking is a technique of preventing simultaneous access to data in a database, to prevent inconsistent results1. For example, if two bank clerks try to update the same bank account for two different transactions, record locking can ensure that only one clerk can modify the record at a time, while the other has to wait until the lock is released. This way, the record will reflect both transactions correctly and avoid data corruption.

Record locking does not serve to allow database administrators (DBAs) to record the activities of users. This is a function of auditing or logging, which can track the actions performed by users on the database2. Record locking does not affect the ability of DBAs to monitor or audit user activities.

Record locking does not serve to restrict users from changing certain values within records. This is a function of access control or authorization, which can enforce rules or policies on what data users can view or modify2.

Record locking does not affect the permissions or privileges of users on the database.

Record locking does not serve to allow users to lock others out of their files. This is a function of encryption or password protection, which can secure files from unauthorized access or modification3. Record locking does not affect the security or confidentiality of files on the database.

References:

* Record locking – Wikipedia1

* Database security – Wikipedia2

* File system permissions – Wikipedia3

QUESTION 655

What is the MOST critical finding when reviewing an organization’s information security management?
* No periodic assessments to identify threats and vulnerabilities
* No dedicated security officer
* No employee awareness training and education program
* No official charter for the information security management system

QUESTION 656

Which of the following is the PRIMARY reason that asset classification is vital to an information security program?
* To ensure risk mitigation efforts are adequate
* To ensure asset protection efforts are in line with industry standards
* To ensure sufficient resources are allocated for information security
* To ensure the appropriate level of protection to assets

QUESTION 657

An IS auditor reviewing the implementation of an intrusion detection system (IDS) should be MOST concerned if:
* IDS sensors are placed outside of the firewall.
* a behavior-based IDS is causing many false alarms.
* a signature-based IDS is weak against new types of attacks.
* the IDS is used to detect encrypted traffic.

Explanation/Reference:

Explanation:

An intrusion detection system (IDS) cannot detect attacks within encrypted traffic, and it would be a concern if someone was

misinformed and thought that the IDS could detect attacks in encrypted traffic. An organization can place sensors outside of the firewall to detect attacks.

These sensors are placed in highly sensitive areas and on extranets. Causing many false alarms is normal for a behavior-based IDS, and should not be a matter of concern. Being weak against new types of attacks is also expected from a signature- based IDS, because it can only recognize attacks that have been previously identified.

QUESTION 658

Which of the following is MOST important to have in place before developing a disaster recovery plan (DRP)?
* System restoration procedures
* Appropriate insurance coverage
* A duplicate processing facility
* Defined acceptable downtime

QUESTION 659

Default permit is only a good approach in an environment where:
* security threats are non-existent or negligible.
* security threats are non-negligible.
* security threats are serious and severe.
* users are trained.
* None of the choices.

Explanation/Reference:

Explanation:

Everything not explicitly permitted is forbidden (default deny) improves security at a cost in functionality.

This is a good approach if you have lots of security threats. On the other hand., “”Everything not explicitly forbidden is permitted”” (default permit) allows greater functionality by sacrificing security. This is only a good approach in an environment where security threats are non- existent or negligible.

QUESTION 660

An organization using instant messaging to communicate with customers prevent legitimate customers from being impersonated by:
* Authentication users before conversation are initiated.
* Using firewall to limit network traffic to authorized ports.
* Logging conversation.
* Using call monitoring.

QUESTION 661

A new system is being developed by a vendor for a consumer service organization. The vendor will provide its proprietary software once system development is completed. Which of the following is the MOST important requirement to include in the vendor contract to ensure continuity?
* The vendor must train the organization’s staff to manage the new software.
* Source code for the software must be placed in escrow.
* The vendor must have a documented disaster recovery plan (DRP) in place.
* Continuous 24/7 support must be available.

QUESTION 662

Which of the following should be an IS auditor’s GREATEST concern when evaluating an organization’s ability to recover from system failures?
* Data backups being stored onsite
* Inadequate backup job monitoring
* Lack of documentation for data backup procedures
* Lack of periodic data backup restoration testing

QUESTION 663

Which of the following outsourced services has the GREATEST need for security monitoring?
* Web site hosting
* Application development
* Virtual private network (VPN) services
* Enterprise infrastructure

Section: Information System Operations, Maintenance and Support