CISA Q&As

Certified Information Systems Auditor

Pass Isaca CISA Exam with 100% Guarantee

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

https://www.passapply.com/cisa.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

The PRIMARY focus of a post-implementation review is to verify that:

A. enterprise architecture (EA) has been complied with.

B. user requirements have been met.

C. acceptance testing has been properly executed.

D. user access controls have been adequately designed.

Correct Answer: B

QUESTION 2

An IS audit report highlighting inadequate network internal controls is challenged because no serious incident has ever occurred. Which of the following actions performed during the audit would have BEST supported the findings?

A. Compliance testing

B. Threat risk assessment

C. Penetration testing

D. Vulnerability assessment

Correct Answer: C

QUESTION 3

An internal audit has found that critical patches were not implemented within the timeline established by policy without a valid reason. Which of the following is the BEST course of action to address the audit findings?

A. Monitor and notify IT staff of critical patches.

B. Evaluate patch management training.

C. Perform regular audits on the implementation of critical patches.

D. Assess the patch management process.

Correct Answer: B

QUESTION 4

Which of the following is found in an audit charter?

A. Audit objectives and scope

B. Required training for audit staff

C. The process of developing the annual audit plan

D. The authority given to the audit function

Correct Answer: A

QUESTION 5

Which of the following audit is mainly designed to evaluate the internal control structure in a given process or area?

A. Compliance Audit

B. Financial Audit

C. Operational Audit

D. Forensic audit

Correct Answer: C

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 6

Which of the following step of PDCA implement the plan, execute the process and make product?

A. Plan

B. Do

C. Check

D. Act

Correct Answer: B

QUESTION 7

An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

A. Obtain error codes indicating failed data feeds.

B. Purchase data cleansing tools from a reputable vendor.

C. Appoint data quality champions across the organization.

D. Implement business rules to reject invalid data.

Correct Answer: D

QUESTION 8

An IS auditor learns a server administration team regularly applies workarounds to address repeated failures of critical data processing services Which of the following would BEST enable the organization to resolve this issue?

A. Problem management

B. Incident management

C. Service level management

D. Change management

Correct Answer: B

QUESTION 9

Which of the following is the GREATEST benefit of adopting an international IT governance framework rather than establishing a new framework based on the actual situation of a specific organization1?

A. Readily available resources such as domains and risk and control methodologies

B. Comprehensive coverage of fundamental and critical risk and control areas for IT governance

C. Fewer resources expended on trial-and-error attempts to fine-tune implementation methodologies

D. Wide acceptance by different business and support units with IT governance objectives

Correct Answer: D

QUESTION 10

Which of the following layer of an enterprise data flow architecture is concerned with the assembly and preparation of data for loading into data marts?

A. Data preparation layer

B. Desktop Access Layer

C. Data Mart layer

D. Data access layer

Correct Answer: A

Data preparation layer ?This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

For CISA exam you should know below information about business intelligence: Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA) A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer ?This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas

and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer ?Enterprise information derives from number of sources:

Operational data ?Data captured and maintained by an organization\\'s existing systems, and usually held in system-specific database or flat files. External Data ?Data provided to an organization by external sources. This could include data

such as customer demographic and market share information.

Nonoperational data ?Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse ?This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support

three basic form of an inquiry.

Drilling up and drilling down ?Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across ?Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company. Historical

Analysis ?The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start

of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer ?Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical

processing (OLAP) data structure.

Data Staging and quality layer ?This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems

periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer ?This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology

now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer ?This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer ?Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be

comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer ?The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer ?This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control

messages.

Internet/Intranet layer ?This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram ?De-construct business processes.

Entity relationship diagram ?Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is

involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as

Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Mart layer ?Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical

processing (OLAP) data structure.

Data access layer ?his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology

now permits SQL access to data even if it is not stored in a relational database.

Reference:

CISA review manual 2014 Page number 188

QUESTION 11

An IS auditor is reviewing a network diagram. Which of the following would be the BEST location for placement of a firewall?

A. Between virtual local area networks (VLANs)

B. At borders of network segments with different security levels

C. Between each host and the local network switch/hub

D. Inside the demilitarized zone (DMZ)

Correct Answer: D

QUESTION 12

When verifying the accuracy and completeness of migrated data for a new application system replacing a legacy system. It is MOST effective for an IS auditor to review;

A. data analytics findings.

B. audit trails

C. acceptance lasting results

D. rollback plans

Correct Answer: B

QUESTION 13

During an audit of identity and access management, an IS auditor finds that the engagement audit plan does not include the testing of controls that regulate access by third parties. Which of the following would be the auditor\\'s BEST course of action?

A. Plan to test these controls in another audit.

B. Escalate the deficiency to audit management.

C. Add testing of third-party access controls to the scope of the audit.

D. Determine whether the risk has been identified in the planning documents.

Correct Answer: D

QUESTION 14

Which of the following BEST demonstrates that IT strategy Is aligned with organizational goals and objectives?

A. IT strategies are communicated to all Business stakeholders

B. Organizational strategies are communicated to the chief information officer (CIO).

C. Business stakeholders are Involved In approving the IT strategy.

D. The chief information officer (CIO) is involved In approving the organizational strategies

Correct Answer: C

QUESTION 15

Which of the following BEST indicates a need to review an organization\\'s information security policy?

A. Completion of annual IT risk assessment

B. Increasing complexity of business transactions

C. Increasing exceptions approved by management

D. High number of low-risk findings in the audit report

Correct Answer: B