



IIA-CIA-Part3 Practice Questions

Shared by Rios on 13-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

Which of the following techniques would best detect on inventory fraud scheme?

Options:

- A- Analyze invoice payments just under individual authorization limits.
- B- Analyze stratification of inventory adjustments by warehouse location.
- C- Analyze Inventory Invoice amounts and compare with approved contract amounts.
- D- Analyze differences discovered during duplicate payment testing.

Answer:

B

Explanation:

Understanding Inventory Fraud Detection:

Inventory fraud typically involves overstatement or understatement of inventory, fictitious inventory transactions, or misappropriation of stock.

A key way to detect fraud is analyzing inventory adjustments (e.g., write-offs, missing stock, excess inventory) to identify unusual patterns or discrepancies.

Why Stratifying Inventory Adjustments by Warehouse is the Best Approach:

Identifies high-risk locations: Certain warehouses may show significantly higher inventory losses or adjustments, indicating possible fraud.

Detects manipulation: Fraudsters may manipulate inventory records to cover theft or misstatements.

Supports data-driven audit procedures: Stratification allows internal auditors to prioritize high-risk areas for deeper investigation.

Why Other Options Are Incorrect:

A . Analyze invoice payments just under individual authorization limits -- Incorrect, as this technique detects fraudulent disbursements, not inventory fraud.

C . Analyze inventory invoice amounts and compare with approved contract amounts -- Incorrect, as this method detects pricing or procurement fraud, not inventory manipulation.

D . Analyze differences discovered during duplicate payment testing -- Incorrect, as this

technique is used to detect billing fraud, not inventory fraud.

IIA's Perspective on Fraud Detection and Internal Controls:

IIA Standard 2120 -- Risk Management requires internal auditors to assess fraud risk, including inventory manipulation.

IIA GTAG (Global Technology Audit Guide) on Fraud Detection recommends data analytics for inventory monitoring.

COSO Internal Control Framework highlights inventory control as a key component of financial accuracy and fraud prevention.

IIA Reference:

IIA Standard 2120 -- Risk Management & Fraud Detection

IIA GTAG -- Data Analytics for Fraud Detection in Inventory

COSO Internal Control Framework -- Inventory and Asset Management Controls

Thus, the correct and verified answer is B. Analyze stratification of inventory adjustments by warehouse location.

Question 2

Question Type: MultipleChoice

Which of the following is an example of a physical control?

Options:

- A- Providing fire detection and suppression equipment
- B- Establishing a physical security policy and promoting it throughout the organization
- C- Performing business continuity and disaster recovery planning
- D- Keeping an offsite backup of the organization's critical data

Answer:

A

Question 3

Question Type: MultipleChoice

Which of the following is a main driver behind the creation and prioritization of new strategic Initiatives established by an organization?

Options:

- A- Risk tolerance
- B- Performance
- C- Threats and opportunities
- D- Governance

Answer:

C

Explanation:

Strategic Initiatives and Their Drivers:

Organizations create and prioritize new strategic initiatives based on internal and external factors that affect their success.

Threats and opportunities, identified through strategic planning and risk assessment, are the primary drivers for launching new initiatives.

This aligns with the SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis framework, which helps organizations identify external risks and growth opportunities.

Why Threats and Opportunities Drive Strategic Initiatives:

Opportunities: Organizations may invest in new products, markets, or technologies to capitalize on emerging trends and gain a competitive edge.

Threats: External challenges such as regulatory changes, market competition, and economic downturns necessitate proactive strategies to mitigate potential risks.

Why Other Options Are Incorrect:

A . Risk tolerance:

While risk tolerance defines an organization's willingness to accept risk, it is not the primary driver for creating new initiatives.

B . Performance:

Performance evaluation helps measure the success of initiatives, but it does not directly drive new strategies.

D . Governance:

Governance ensures oversight and compliance but does not initiate strategic changes unless influenced by external threats and opportunities.

IIA's Perspective on Strategic Planning and Risk Management:

IIA Standard 2010 -- Planning states that internal auditors must assess how organizations identify and respond to threats and opportunities when developing strategic initiatives.

COSO Enterprise Risk Management (ERM) Framework highlights that strategic planning should integrate risk management, ensuring that organizations adapt to evolving external conditions.

IIA Reference:

IIA Standard 2010 -- Planning

COSO Enterprise Risk Management (ERM) Framework

SWOT Analysis in Strategic Decision-Making

Thus, the correct and verified answer is C. Threats and opportunities.

Question 4

Question Type: MultipleChoice

Which of the following statements is true regarding user developed applications (UDAs) and traditional IT applications?

Options:

- A- UDAs and traditional IT applications typically follow a similar development life cycle
- B- A UDA usually includes system documentation to illustrate its functions, and IT-developed applications typically do not require such documentation.
- C- Unlike traditional IT applications. UDAs typically are developed with little consideration of controls.
- D- IT testing personnel usually review both types of applications thoroughly to ensure they were developed properly.

Answer:

C

Explanation:

User-Developed Applications (UDAs) are software tools, typically spreadsheets or small databases, created by business users rather than IT professionals. These applications often lack formal security, documentation, and control measures, increasing the risk of data errors, unauthorized access, and compliance failures.

Why Option C is Correct?

UDAs are often created quickly to meet immediate business needs, without following IT governance, security controls, or development standards.

Unlike traditional IT applications, UDAs lack structured testing, change management, and formal documentation.

The IIA's GTAG 14 -- Auditing User-Developed Applications states that UDAs present higher risks because they are not subject to the same controls as IT-managed applications.

Explanation of the Other Options:

A . UDAs and traditional IT applications typically follow a similar development life cycle. Incorrect. Traditional IT applications follow a formal Software Development Life Cycle (SDLC), whereas UDAs are developed informally by end-users.

B . A UDA usually includes system documentation to illustrate its functions, and IT-developed applications typically do not require such documentation. Incorrect. IT applications require extensive documentation, whereas UDAs often lack documentation entirely.

D . IT testing personnel usually review both types of applications thoroughly to ensure they were developed properly. Incorrect. IT applications undergo rigorous testing and quality assurance, while UDAs often bypass IT reviews altogether.

IIA Reference & Best Practices:

IIA GTAG 14 -- Auditing User-Developed Applications highlights the risks of UDAs and emphasizes the need for internal controls.

COBIT Framework (Control Objectives for Information and Related Technologies) recommends IT governance measures for all business-critical applications.

ISO 27001 (Information Security Management System) warns against uncontrolled user-developed applications due to security risks.

Thus, the correct answer is C. Unlike traditional IT applications, UDAs typically are developed with little consideration of controls.

Question 5

Question Type: MultipleChoice

The project manager responsible for overseeing a controversial project decides to accept the risks associated with the project launch. These risks might have a significant impact on the organization meeting its environmental sustainability goals. Which of the following is the best next step for the chief audit executive to take in response to the decision?

Options:

- A- Educate employees working on the project launch about the risks
- B- Notify the board about the significant risks the organization might face
- C- Communicate the risks to senior management
- D- Instruct the project manager to stop the controversial project development

Answer:

C

Explanation:

The CAE's first step when a project manager accepts a risk that appears significant is to discuss and communicate the risk with senior management. If management agrees with the project manager, and the CAE still considers the risk unacceptable, then it must be escalated to the board.

Option A (employee education) is outside audit's role. Option B is premature---escalation to the board happens only if management does not resolve the issue. Option D is not within internal audit's authority.

IIA Standards -- Standard 2600: Communicating the Acceptance of Risks.

Question 6

Question Type: MultipleChoice

Which of the following IT-related activities is most commonly performed by the second line of defense?

Options:

- A- Block unauthorized traffic.
- B- Encrypt data.

- C- Review disaster recovery test results.
- D- Provide independent assessment of IT security.

Answer:

C

Explanation:

Understanding the Three Lines of Defense Model:

First Line of Defense (Operational Management): Performs daily IT security tasks, such as blocking unauthorized traffic and encrypting data.

Second Line of Defense (Risk Management & Compliance): Monitors and reviews security controls, including disaster recovery testing and risk management activities.

Third Line of Defense (Internal Audit): Provides an independent assessment of IT security controls.

Why Option C (Review Disaster Recovery Test Results) Is Correct?

The second line of defense is responsible for monitoring and evaluating IT risk management processes, including disaster recovery and business continuity planning.

Reviewing disaster recovery test results ensures that the organization is prepared for IT disruptions and meets compliance requirements.

IIA Standard 2110 -- Governance requires auditors to evaluate whether IT risk management activities (such as disaster recovery) are being effectively monitored.

Why Other Options Are Incorrect?

Option A (Block unauthorized traffic):

This is a first-line defense task, typically handled by IT security teams (e.g., firewall and intrusion detection system monitoring).

Option B (Encrypt data):

Encryption is part of daily IT security operations and is handled by the first line of defense.

Option D (Provide an independent assessment of IT security):

Independent assessments are the responsibility of internal audit (third line of defense), not the second line.

Final Justification:

The second line of defense focuses on monitoring IT risk, making disaster recovery test review a key responsibility.

IIA Standard 2110 and the Three Lines of Defense Model confirm this role.

IIA Reference:

IPPF Standard 2110 -- Governance (IT Risk Management)

IIA Three Lines of Defense Model

COBIT Framework -- IT Governance & Risk Management

Question 7

Question Type: MultipleChoice

Which of the following measures the operating success of a company for a given period of time?

Options:

- A- Liquidity ratios.
- B- Profitability ratios.
- C- Solvency ratios.
- D- Current ratios.

Answer:

B

Explanation:

Profitability ratios measure a company's ability to generate profit over a specific period, making them the best indicators of operating success. These ratios assess financial performance by comparing income to various financial metrics such as revenue, assets, and equity.

Step-by-Step

Correct Answer (B - Profitability Ratios)

Profitability ratios reflect how effectively a company generates income from its operations over a given period.

Key profitability ratios include:

Gross Profit Margin: Measures how efficiently a company produces goods and services.

Operating Profit Margin: Shows profitability from core operations.

Net Profit Margin: Indicates the percentage of revenue converted into profit.

Return on Assets (ROA): Measures how efficiently assets generate earnings.

Return on Equity (ROE): Assesses how well equity investments generate returns.

The IIA Practice Guide: Auditing Financial Performance emphasizes profitability ratios in evaluating operational success.

Why Other Options Are Incorrect:

Option A (Liquidity Ratios):

Liquidity ratios measure a company's ability to meet short-term obligations rather than its operating success.

Examples: Current Ratio, Quick Ratio.

IIA GTAG 13: Business Performance emphasizes that liquidity ratios relate to short-term financial health, not operating success.

Option C (Solvency Ratios):

Solvency ratios evaluate a company's ability to meet long-term financial obligations, not operating performance.

Examples: Debt-to-Equity Ratio, Interest Coverage Ratio.

Option D (Current Ratio):

The current ratio is a liquidity ratio, measuring whether a company can meet its short-term liabilities with current assets.

It does not directly assess profitability or operational success.

IIA Reference for Validation:

IIA Practice Guide: Auditing Financial Performance -- Covers the role of profitability ratios in evaluating a company's success.

IIA GTAG 13: Business Performance -- Discusses financial analysis, including profitability, liquidity, and solvency metrics.

Thus, profitability ratios (B) are the best measures of a company's operating success over a period.

Question 8

Question Type: MultipleChoice

An analytical model determined that on Friday and Saturday nights the luxury brands stores should be open for extended hours and with a doubled number of employees

present; while on Mondays and Tuesdays costs can be minimized by reducing the number of employees to a minimum and opening only for evening hours Which of the

following best categorizes the analytical model applied?

Options:

- A- Descriptive.
- B- Diagnostic.
- C- Prescriptive.
- D- Prolific.

Answer:

C

Explanation:

Types of Analytical Models in Business Intelligence:

Descriptive Analytics -- Answers 'What happened?' by summarizing past data.

Diagnostic Analytics -- Answers 'Why did it happen?' by identifying causes of trends or issues.

Prescriptive Analytics -- Answers 'What should we do?' by providing data-driven recommendations and optimal solutions for decision-making.

Prolific Analytics -- This is not a recognized category in standard analytics models.

Why Prescriptive Analytics is the Best Choice?

The model makes specific recommendations for store operations (extended hours, staffing adjustments).

It optimizes resource allocation based on demand patterns.

It goes beyond identifying past trends (descriptive) or diagnosing causes (diagnostic) and provides actionable solutions.

Why Not the Other Options?

A . Descriptive -- Would only summarize sales data but not suggest changes.

B . Diagnostic -- Would explain why luxury stores see higher traffic on weekends but would not recommend actions.

D . Prolific -- Not a standard analytics category.

IIA Reference:

IIA's GTAG on Data Analytics -- Describes prescriptive analytics as the highest level of business intelligence, driving decision-making.

COSO's Enterprise Risk Management (ERM) Framework -- Encourages data-driven decision-making using prescriptive models.

COBIT 2019 on IT Governance -- Recommends leveraging prescriptive analytics for operational efficiency.

Final Answer: C. Prescriptive.



Question 9

Question Type: MultipleChoice

An internal auditor found the following information while reviewing the monthly financial statements for a wholesaler of safety glasses: Opening inventory: 1,000 units at \$2 per unit; Purchased: 5,000 units at \$3 per unit; Sold: 3,000 units at \$7 per unit. The cost of goods sold was reported at \$8,500. Which of the following inventory methods was used to derive this value?

Options:

- A- Average cost method
- B- First-in, first-out (FIFO) method
- C- Specific identification method
- D- Activity-based costing method



Answer:

B

Question 10

Question Type: MultipleChoice

For employees, the primary value of implementing job enrichment is Which option best?

Options:

- A- Validation of the achievement of their goals and objectives
- B- Increased knowledge through the performance of additional tasks
- C- Support for personal growth and a meaningful work experience
- D- An increased opportunity to manage better the work done by their subordinates

Answer:

C

Question 11

Question Type: MultipleChoice

While conducting' audit procedures at the organization's data center an internal auditor noticed the following:

- Backup media was located on data center shelves.
- Backup media was organized by date.
- Backup schedule was one week in duration.

The system administrator was able to present restore logs.

Which option best is reasonable for the internal auditor to conclude?

Options:

- A- Backup media is not properly stored, as the storage facility should be off-site.
- B- Backup procedures are adequate and appropriate according to best practices.
- C- Backup media is not properly indexed, as backup media should be indexed by system, not date.
- D- Backup schedule is not sufficient, as full backup should be conducted daily.

Answer:

A

Explanation:

The auditor's observation indicates that backup media is stored on-site in the data center, which is a major risk in disaster recovery and business continuity planning (BCP). Best practices recommend storing backup media off-site to prevent data loss due to fires, floods, cyberattacks,

or other disasters affecting the primary site.

Step-by-Step Justification:

Off-Site Storage Reduces Disaster Risks:

Keeping backups only at the primary data center means that any physical disaster (fire, flood, theft, or power surge) can destroy both primary and backup data.

Best practices require off-site or cloud-based backup storage to ensure data recovery in case of emergencies.

Regulatory and Compliance Considerations:

IIA Standard 2110 (Governance): Emphasizes disaster recovery policies to protect critical IT assets.

ISO/IEC 27001 (Information Security Management System): Recommends storing backups in a geographically separate location.

NIST SP 800-34 (Contingency Planning Guide for Federal Information Systems): Requires off-site storage to ensure effective disaster recovery.

Why the Other Options Are Incorrect:

B . Backup procedures are adequate and appropriate according to best practices:

Incorrect, as on-site-only storage violates best practices for disaster recovery.

C . Backup media is not properly indexed, as backup media should be indexed by system, not date:

While indexing is important, the main issue here is improper storage, not indexing methods.

D . Backup schedule is not sufficient, as full backup should be conducted daily:

Backup frequency depends on business needs; a weekly backup is common for many organizations.

However, the biggest concern here is lack of off-site storage, not frequency.

IIA Reference:

IIA GTAG (Global Technology Audit Guide) on Business Continuity and Disaster Recovery: Recommends off-site storage for backups.

ISO/IEC 27001 -- Information Security Controls (A.12.3.1): Requires backup data to be securely stored off-site.

COBIT 5 Framework -- DSS04 (Manage Continuity): Supports off-site backups for IT continuity.

Thus, the correct answer is A. Backup media is not properly stored, as the storage facility should be off-site.

Question 12

Question Type: MultipleChoice

Which of the following activities best illustrates a user's authentication control?

Options:

- A- Identity requests are approved in two steps.
- B- Logs are checked for misaligned identities and access rights.
- C- Users have to validate their identity with a smart card.
- D- Functions can be performed based on access rights

Answer:

C

Explanation:

Authentication control is a security measure used to verify the identity of users before granting access to systems or data. Authentication methods ensure that only authorized individuals can access resources.

Why Option C (Users have to validate their identity with a smart card) is Correct:

Authentication is the process of verifying a user's identity before granting access.

Smart card authentication is a strong authentication method because it requires a physical device (smart card) and a PIN or biometric verification.

This falls under multi-factor authentication (MFA), enhancing security by combining something the user has (smart card) with something they know (PIN).

Why Other Options Are Incorrect:

Option A (Identity requests are approved in two steps):

Incorrect because this refers to identity approval (authorization), not authentication.

Option B (Logs are checked for misaligned identities and access rights):

Incorrect because log monitoring is a detective control, not an authentication control.

Option D (Functions can be performed based on access rights):

Incorrect because this describes authorization (determining what a user can do after authentication).

IIA Reference:

IIA GTAG -- 'Auditing Identity and Access Management': Covers authentication methods like smart cards and multi-factor authentication.

COBIT 2019 -- DSS05 (Manage Security Services): Recommends strong authentication controls, including smart card validation.

NIST Cybersecurity Framework -- 'Access Control Guidelines': Highlights authentication best practices, including smart card use.



To Get Premium Files for IIA-CIA-Part3 Visit

<https://www.p2pexams.com/products/iaa-cia-part3>

For More Free Questions Visit

<https://www.p2pexams.com/iaa/pdf/iaa-cia-part3>

20%
DISCOUNT

P2P
exams