

Sample Materials IIA-CIA-Part3 All-in-One Exam Guide

Download valid IIA-CIA-Part3 exam dumps to pass your exam easily

Exam : IIA-CIA-Part3

**Title : CIA Exam Part Three:
Business Knowledge for
Internal Auditing**

<https://www.passcert.com/IIA-CIA-Part3.html>

1 / 4

What's more, part of that ITPassLeader IIA-CIA-Part3 dumps now are free: <https://drive.google.com/open?id=1k4XZVxNDsxYpj9TLP8D2XbtMNJePUOZP>

ITPassLeader's web-based IIA IIA-CIA-Part3 practice test also contains mock exams just like the desktop practice exam software with some extra features. As this is a web-based software, this is accessible through any browser like Opera, Safari, Chrome, Firefox and MS Edge with a good internet connection. Business Knowledge for Internal Auditing (IIA-CIA-Part3) practice test is also customizable so that you can easily set the timings and change the number of questions according to your ease.

What are the special features of the IIA CIA Part 3 Exam

We are sure that the IIA CIA Part 3 Exam candidates can pass the exam successfully. After you purchase our products, we will provide free update in time for one year. The latest information of these tests can be found in our ITPassLeader. We are committed to your ongoing success. **IIA CIA Part 3 exam dumps** will help you to learn about the field and get a clear idea about the required knowledge and skills that you will need to learn.

Our IIA CIA Part 3 Exam is written to the highest standards of technical accuracy which can make you succeed in the exam.

IIA-CIA-Part3 exam is a comprehensive examination designed to measure the candidate's knowledge in business principles and concepts that are essential for internal auditing professionals. It is a challenging exam that requires the candidate to have a deep understanding of various business domains. Hence, individuals interested in pursuing a career in internal auditing should consider taking the IIA-CIA-Part3 Exam to enhance their professional recognition and career prospects.

IIA-CIA-Part3 certification exam is recognized by employers around the world as a sign of excellence in the field of internal auditing. Business Knowledge for Internal Auditing certification can help internal auditors advance their careers and increase their earning

potential. It also provides employers with a way to ensure that their internal auditors have the knowledge and skills necessary to perform their job duties effectively.

>> Real IIA-CIA-Part3 Dumps Free <<

Business Knowledge for Internal Auditing Practice Torrent - IIA-CIA-Part3 Actual Test & IIA-CIA-Part3 Free Demo

Your personal information on our IIA-CIA-Part3 exam braindumps such as your names, email address will be strictly protected by our system. Our workers will never randomly spread your information to other merchants for making money. In short, your purchasing of our IIA-CIA-Part3 Preparation quiz is totally safe and sound. Also, our website has strong back protection program to resist attacking from hackers. We will live up to your trust and keep advancing on our IIA-CIA-Part3 study materials.

IIA Business Knowledge for Internal Auditing Sample Questions (Q251-Q256):

NEW QUESTION # 251

An internal auditor is investigating a potential fraudulent activity. What is the first test the auditor should perform on the transaction data under scrutiny?

- A. Detailed review of the data contents to strategize the best analytical techniques.
- B. Digital analysis for statistically unlikely occurrences that may indicate system tampering.
- C. Verification of the completeness and integrity of the obtained data.
- D. Calculation of statistical parameters to identify outliers requiring further scrutiny.

Answer: C

NEW QUESTION # 252

Monitoring is an important component of internal control. Which of the following is not an example of monitoring?

- A. Management has asked internal auditing to perform regular audits of the controls over cash processing.
- B. Data processing management regularly generates exception reports for unusual transactions or volumes of transactions and follows up with investigation as to causes.
- C. Management regularly compares divisional performance with budgets for the division.
- D. Data processing management regularly reconciles batch control totals for items processed with batch controls for items submitted.

Answer: D

Explanation:

Monitoring assesses the quality of internal control over time. Management considers whether internal control is properly designed and operating as intended and modifies it to reflect changing conditions. Monitoring may be in the form of separate, periodic evaluations or of ongoing monitoring. Ongoing monitoring occurs as part of routine operations. It includes management and supervisory review, comparisons, reconciliations, and other actions by personnel as part of their regular activities. However, reconciling batch control totals is a processing control. This information is relevant to a theory of constraints (TOC) analysis. A manufacturer that can sell all of its output produces its sole product using three operations. Each unit sells for US \$120, and direct materials costing US \$48 per unit are added at the start of the first operation. Other variable costs are immaterial. The following annual cost and capacity information is available concerning those operations:

NEW QUESTION # 253

Which of the following best describes a man-in-the-middle cyber-attack?

- A. The perpetrator is able to delete data on the network without physical access to the device.
- B. The perpetrator is able to exploit network activities for unapproved purposes.
- C. The perpetrator is able to disable default security controls and introduce additional vulnerabilities.
- D. The perpetrator is able to take over control of data communication in transit and replace traffic.

Answer: D

Explanation:

* Understanding a Man-in-the-Middle (MITM) Attack:

* A Man-in-the-Middle (MITM) attack occurs when a cybercriminal intercepts, alters, or steals data while it is being transmitted between two parties.

* The attacker can modify messages, inject malicious content, or eavesdrop on sensitive communications without the knowledge of the sender or receiver.

* How MITM Attacks Work:

* Attackers position themselves between two communicating parties (e.g., a user and a banking website) and intercept the data exchange.

* This allows them to steal login credentials, financial information, or confidential communications.

* Common MITM attack methods include:

* Wi-Fi eavesdropping (public network interception).

* Session hijacking (stealing active user sessions).

* HTTPS spoofing (tricking users into thinking they are on a secure website).

* Why Other Options Are Incorrect:

* A. The perpetrator is able to delete data on the network without physical access to the device

- Incorrect.

* This describes a remote cyberattack, such as malware or ransomware, rather than MITM, which focuses on data interception.

* B. The perpetrator is able to exploit network activities for unapproved purposes - Incorrect.

* This is too broad and could refer to insider threats, malware, or privilege escalation attacks, rather than specifically MITM.

* D. The perpetrator is able to disable default security controls and introduce additional vulnerabilities - Incorrect.

* This describes a system exploitation attack, such as a rootkit or backdoor installation, not an MITM attack.

* IIA's Perspective on Cybersecurity and IT Risk Management:

* IIA Standard 2110 - Governance requires organizations to implement cybersecurity controls to mitigate risks like MITM attacks.

* IIA GTAG (Global Technology Audit Guide) on Cybersecurity Risks advises organizations to use encryption (e.g., TLS, VPNs) to protect data in transit.

* NIST Cybersecurity Framework recommends multi-factor authentication (MFA) and secure protocols to prevent MITM attacks.

IIA References:

* IIA Standard 2110 - IT Security and Cyber Risk Governance

* IIA GTAG - Cybersecurity Controls and Threat Mitigation

* NIST Cybersecurity Framework - Secure Data Transmission

Thus, the correct and verified answer is C. The perpetrator is able to take over control of data communication in transit and replace traffic.

NEW QUESTION # 254

Which of the following is a risk that is higher when an electronic funds transfer EFT system is used?

- A. Improper change control procedures.
- B. Inadequate back-ups and disaster recovery procedures.
- C. Insufficient online edit checks.
- **D. Unauthorized access and activity.**

Answer: D

Explanation:

Unauthorized access to money transfer activities or data is an inherent and unique risk of EFT systems. An unauthorized person may attempt to read, alter, or delete information in data files or to enter authorized fund transfers. Hence, in the financial services industry, protection of confidential customer transactions is especially important. Moreover, unauthorized transfers subject a financial institution to a direct risk of serious loss.

NEW QUESTION # 255

If a supervisor fails to give an employee a negative evaluation because of fear of damaging a good working relationship, this is known as the:

- A. Halo effect.
- **B. Leniency error.**
- C. Regency effect.

- Answer: B**

A leniency error is a manager's failure to give a negative evaluation because of fear of damaging a good working relationship with an employee.

• • • • •

IIA-CIA-Part3 Test Answers: <https://www.itpassleader.com/IIA/IIA-CIA-Part3-dumps-pass-exam.html>

- 2026 Latest ITPassLeader IIA-CIA-Part3 PDF Dumps and IIA-CIA-Part3 Exam Engine Free Share:
<https://drive.google.com/open?id=1k4XZVxNDsxYpjl9TLP8D2XbtMNJePUOZP>