CERTIFIED INTERNAL AUDITOR®
EXAM PRACTICE QUESTIONS

SPONSORED BY
N G SHANKAR, CIA
NEW DELHI, INDIA
CONTENTS

Foreword...........................................................................................................................................v
Topics Tested........................................................................................................................................1

PART 1
ESSENTIALS OF INTERNAL AUDITING

Exam Practice Questions..................................................................................................................9
Solutions for Part 1..........................................................................................................................37

PART 2
PRACTICE OF INTERNAL AUDITING

Exam Practice Questions..................................................................................................................67
Solutions for Part 2..........................................................................................................................91

PART 3
BUSINESS KNOWLEDGE FOR INTERNAL AUDITING

Exam Practice Questions..................................................................................................................113
Solutions for Part 3..........................................................................................................................133
FOREWORD

Certified Internal Auditor Exam Practice Questions is designed to familiarize interested parties with the content and format of the Certified Internal Auditor (CIA) exam. It is not meant to replace material supplied by providers of CIA exam review materials.

The questions in this publication, whether new or adapted from earlier CIA exams, are simply representative of the format, length, and content of questions that a CIA candidate can expect to see on future exams. A current or future CIA exam candidate’s success or failure in answering these questions should not be taken as any form of guarantee of that candidate’s results on an actual CIA exam.

The 2019 three-part CIA exam has been revised to:

- Bring it up to date with the current global practice of internal auditing.
- Clarify the knowledge and skills that exam candidates must possess in order to pass the exam.
- Refocus the content of Part 3 on the core knowledge and skills that internal auditors must have to do their job.

If there are any significant changes in the format or content of the CIA exam in the future, the Certifications Department will make those changes known through its website (www.theiia.org) and/or through mailings to current CIA candidates. For further information on the CIA program, please visit the Certifications & Qualifications heading on the website listed above, or contact Customer Relations for a brochure:

The Institute of Internal Auditors
Customer Relations
1035 Greenwood Blvd., Suite 401
Lake Mary, Florida 32746, USA
Phone: +1-401-937-1111
Fax: +1-407-937-1101
Email: CustomerRelations@theiia.org
TOPICS TESTED

PART 1

I. Foundations of Internal Auditing (15%)
   A. Interpret The IIA’s Mission of Internal Audit, Definition of Internal Auditing, and Core Principles for the Professional Practice of Internal Auditing, and the purpose, authority, and responsibility of the internal audit activity.
   B. Explain the requirements of an internal audit charter (required components, board approval, communication of the charter, etc.).
   C. Interpret the difference between assurance and consulting services provided by the internal audit activity.
   D. Demonstrate conformance with The IIA’s Code of Ethics.

II. Independence and Objectivity (15%)
   A. Interpret organizational independence of the internal audit activity (importance of independence, functional reporting, etc.).
   B. Identify whether the internal audit activity has any impairments to its independence.
   C. Assess and maintain an individual internal auditor's objectivity, including determining whether an individual internal auditor has any impairments to his/her objectivity.
   D. Analyze policies that promote objectivity.

III. Proficiency and Due Professional Care (18%)
   A. Recognize the knowledge, skills, and competencies required (whether developed or procured) to fulfill the responsibilities of the internal audit activity.
   B. Demonstrate the knowledge and competencies that an internal auditor needs to possess to perform his/her individual responsibilities, including technical skills and soft skills (communication skills, critical thinking, persuasion/negotiation and collaboration skills, etc.).
   C. Demonstrate due professional care.
   D. Demonstrate an individual internal auditor's competency through continuing professional development.
IV. Quality Assurance and Improvement Program (7%)
   A. Describe the required elements of the quality assurance and improvement program (internal assessments, external assessments, etc.).
   B. Describe the requirement of reporting the results of the quality assurance and improvement program to the board or other governing body.
   C. Identify appropriate disclosure of conformance vs. nonconformance with The IIA's *International Standards for the Professional Practice of Internal Auditing*.

V. Governance, Risk Management, and Control (35%)
   A. Describe the concept of organizational governance.
   B. Recognize the impact of organizational culture on the overall control environment and individual engagement risks and controls.
   C. Recognize and interpret the organization's ethics and compliance-related issues, alleged violations, and dispositions.
   D. Describe corporate social responsibility.
   E. Interpret fundamental concepts of risk and the risk management process.
   F. Describe globally accepted risk management frameworks appropriate to the organization (COSO – ERM, ISO 31000, etc.).
   G. Examine the effectiveness of risk management within processes and functions.
   H. Recognize the appropriateness of the internal audit activity's role in the organization's risk management process.
   I. Interpret internal control concepts and types of controls.
   J. Apply globally accepted internal control frameworks appropriate to the organization (COSO, etc.).
   K. Examine the effectiveness and efficiency of internal controls.

VI. Fraud Risks (10%)
   A. Interpret fraud risks and types of frauds and determine whether fraud risks require special consideration when conducting an engagement.
   B. Evaluate the potential for occurrence of fraud (red flags, etc.) and how the organization detects and manages fraud risks.
   C. Recommend controls to prevent and detect fraud and education to improve the organization's fraud awareness.
   D. Recognize techniques and internal audit roles related to forensic auditing (interview, investigation, testing, etc.).
PART 2

I. Managing the Internal Audit Activity (20%)

1. Internal Audit Operations
   A. Describe policies and procedures for the planning, organizing, directing, and monitoring of internal audit operations.
   B. Interpret administrative activities (budgeting, resourcing, recruiting, staffing, etc.) of the internal audit activity.

2. Establishing a Risk-Based Internal Audit Plan
   A. Identify sources of potential engagements (audit universe, audit cycle requirements, management requests, regulatory mandates, relevant market and industry trends, emerging issues, etc.).
   B. Identify a risk management framework to assess risks and prioritize audit engagements based on the results of a risk assessment.
   C. Interpret the types of assurance engagements (risk and control assessments, audits of third parties and contract compliance, security and privacy, performance and quality audits, key performance indicators, operational audits, financial and regulatory compliance audits).
   D. Interpret the types of consulting engagements (training, system design, system development, due diligence, privacy, benchmarking, internal control assessment, process mapping, etc.) designed to provide advice and insight.
   E. Describe coordination of internal audit efforts with the external auditor, regulatory oversight bodies, and other internal assurance functions, and potential reliance on other assurance providers.

3. Communicating and Reporting to Senior Management and the Board
   A. Recognize that the chief audit executive communicates the annual audit plan to senior management and the board and seeks the board’s approval.
   B. Identify significant risk exposures and control and governance issues for the chief audit executive to report to the board.
   C. Recognize that the chief audit executive reports on the overall effectiveness of the organization’s internal control and risk management processes to senior management and the board.
   D. Recognize internal audit key performance indicators that the chief audit executive communicates to senior management and the board periodically.

II. Planning the Engagement (20%)

1. Engagement Planning
   A. Determine engagement objectives, evaluation criteria, and the scope of the engagement.
   B. Plan the engagement to assure identification of key risks and controls.
C. Complete a detailed risk assessment of each audit area, including evaluating and prioritizing risk and control factors.
D. Determine engagement procedures and prepare the engagement work program.
E. Determine the level of staff and resources needed for the engagement.

III. Performing the Engagement (40%)

1. Information Gathering
   A. Gather and examine relevant information (review previous audit reports and data, conduct walk-throughs and interviews, perform observations, etc.) as part of a preliminary survey of the engagement area.
   B. Develop checklists and risk-and-control questionnaires as part of a preliminary survey of the engagement area.
   C. Apply appropriate sampling (nonstatistical, judgmental, discovery, etc.) and statistical analysis techniques.

2. Analysis and Evaluation
   A. Use computerized audit tools and techniques (data mining and extraction, continuous monitoring, automated workpapers, embedded audit modules, etc.).
   B. Evaluate the relevance, sufficiency, and reliability of potential sources of evidence.
   C. Apply appropriate analytical approaches and process mapping techniques (process identification, workflow analysis, process map generation and analysis, spaghetti maps, RACI diagrams, etc.).
   D. Determine and apply analytical review techniques (ratio estimation, variance analysis, budget vs. actual, trend analysis, other reasonableness tests, benchmarking, etc.).
   E. Prepare workpapers and documentation of relevant information to support conclusions and engagement results.
   F. Summarize and develop engagement conclusions, including assessment of risks and controls.

3. Engagement Supervision
   A. Identify key activities in supervising engagements (coordinate work assignments, review workpapers, evaluate auditors’ performance, etc.).

IV. Communicating Engagement Results and Monitoring Progress (20%)

1. Communicating Engagement Results and the Acceptance of Risk
   A. Arrange preliminary communication with engagement clients.
   B. Demonstrate communication quality (accurate, objective, clear, concise, constructive, complete, and timely) and elements (objectives, scope, conclusions, recommendations, and action plan).
   C. Prepare interim reporting on the engagement progress.
   D. Formulate recommendations to enhance and protect organizational value.
E. Describe the audit engagement communication and reporting process, including holding the exit conference, developing the audit report (draft, review, approve, and distribute), and obtaining management’s response.

F. Describe the chief audit executive’s responsibility for assessing residual risk.

G. Describe the process for communicating risk acceptance (when management has accepted a level of risk that may be unacceptable to the organization).

2. Monitoring Progress

A. Assess engagement outcomes, including the management action plan.

B. Manage monitoring and follow-up of the disposition of audit engagement results communicated to management and the board.

PART 3

I. Business Acumen (35%)

1. Organizational Objectives, Behavior, and Performance

A. Describe the strategic planning process and key activities (objective setting, globalization and competitive considerations, alignment to the organization’s mission and values, etc.).

B. Examine common performance measures (financial, operational, qualitative vs. quantitative, productivity, quality, efficiency, effectiveness, etc.).

C. Explain organizational behavior (individuals in organizations, groups, and how organizations behave, etc.) and different performance management techniques (traits, organizational politics, motivation, job design, rewards, work schedules, etc.).

D. Describe management’s effectiveness to lead, mentor, guide people, build organizational commitment, and demonstrate entrepreneurial ability.

2. Organizational Structure and Business Processes

A. Appraise the risk and control implications of different organizational configuration structures (centralized vs. decentralized, flat structure vs. traditional, etc.).

B. Examine the risk and control implications of common business processes (human resources, procurement, product development, sales, marketing, logistics, management of outsourced processes, etc.).

C. Identify project management techniques (project plan and scope, time/team/resources/cost management, change management, etc.).

D. Recognize the various forms and elements of contracts (formality, consideration, unilateral, bilateral, etc.).

3. Data Analytics

A. Describe data analytics, data types, data governance, and the value of using data analytics in internal auditing.
B. Explain the data analytics process (define questions, obtain relevant data, clean/normalize data, analyze data, communicate results).

C. Recognize the application of data analytics methods in internal auditing (anomaly detection, diagnostic analysis, predictive analysis, network analysis, text analysis, etc.).

II. Information Security (25%)

1. Information Security

A. Differentiate types of common physical security controls (cards, keys, biometrics, etc.).

B. Differentiate the various forms of user authentication and authorization controls (password, two-level authentication, biometrics, digital signatures, etc.) and identify potential risks.

C. Explain the purpose and use of various information security controls (encryption, firewalls, antivirus, etc.).

D. Recognize data privacy laws and their potential impact on data security policies and practices.

E. Recognize emerging technology practices and their impact on security (bring your own device [BYOD], smart devices, internet of things [IoT], etc.).

F. Recognize existing and emerging cybersecurity risks (hacking, piracy, tampering, ransomware attacks, phishing attacks, etc.).

G. Describe cybersecurity and information security-related policies.

III. Information Technology (20%)

1. Application and System Software

A. Recognize core activities in the systems development lifecycle and delivery (requirements definition, design, developing, testing, debugging, deployment, maintenance, etc.) and the importance of change controls throughout the process.

B. Explain basic database terms (data, database, record, object, field, schema, etc.) and internet terms (HTML, HTTP, URL, domain name, browser, click-through, electronic data interchange [EDI], cookies, etc.).

C. Identify key characteristics of software systems (customer relationship management [CRM] systems; enterprise resource planning [ERP] systems; and governance, risk, and compliance [GRC] systems; etc.).

2. IT Infrastructure and IT Control Frameworks

A. Explain basic IT infrastructure and network concepts (server, mainframe, client-server configuration, gateways, routers, LAN, WAN, VPN, etc.) and identify potential risks.

B. Define the operational roles of a network administrator, database administrator, and help desk.

C. Recognize the purpose and applications of IT control frameworks (COBIT, ISO 27000, ITIL, etc.) and basic IT controls.

3. Disaster Recovery
A. Explain disaster recovery planning site concepts (hot, warm, cold, etc.).
B. Explain the purpose of systems and data backup.
C. Explain the purpose of systems and data recovery procedures.

IV. Financial Management (20%)

1. Financial Accounting and Finance

A. Identify concepts and underlying principles of financial accounting (types of financial statements and terminologies such as bonds, leases, pensions, intangible assets, research and development, etc.).
B. Recognize advanced and emerging financial accounting concepts (consolidation, investments, fair-value partnerships, foreign currency transactions, etc.).
C. Interpret financial analysis (horizontal and vertical analysis and ratios related to activity, profitability, liquidity, leverage, etc.).
D. Describe revenue cycle, current asset management activities and accounting, and supply chain management (including inventory valuation and accounts payable).
E. Describe capital budgeting, capital structure, basic taxation, and transfer pricing.

2. Managerial Accounting

A. Explain general concepts of managerial accounting (cost-volume-profit analysis, budgeting, expense allocation, cost-benefit analysis, etc.).
B. Differentiate costing systems (absorption, variable, fixed, activity-based, standard, etc.).
C. Distinguish various costs (relevant and irrelevant costs, incremental costs, etc.) and their use in decision making.
PART 1

ESSENTIALS OF INTERNAL AUDITING

EXAM PRACTICE QUESTIONS: 125

All references to the International Professional Practices Framework refer to The IIA’s International Professional Practices Framework (IPPF), which includes the Core Principles, Definition of Internal Auditing, Code of Ethics, Standards, Glossary, Implementation Guidance, and Supplemental Guidance. All references to Standards refer to the International Standards for the Professional Practice of Internal Auditing outlined in The IIA’s IPPF. All references to CAE refer to chief audit executive.

1. A specific objective of an audit of an organization’s expenditure cycle is to determine if all goods paid for have been received and charged to the correct account. This objective would address which of the following primary objectives identified in the Standards?
   I. Reliability and integrity of financial and operational information.
   II. Compliance with laws, regulations, and contracts.
   III. Effectiveness and efficiency of operations.
   IV. Safeguarding of assets.
   a. I and II only.
   b. I and IV only.
   c. I, II, and IV only.
   d. II, III, and IV only.
2. Which of the following is “mandatory guidance” in The IIA’s IPPF?  
   I. Implementation Guidance.  
   II. Code of Ethics.  
   III. The Core Principles for the Professional Practice of Internal Auditing.  
   IV. Standards.  
   a. I, II, and IV only.  
   b. II and IV only.  
   c. II, III, and IV only.  
   d. I, II, III, and IV.  

3. Which of the following is a Core Principle for the Professional Practice of Internal Auditing?  
   a. Maintain confidentiality.  
   b. Promote an ethical culture in the internal audit profession.  
   c. Develop consistency in internal audit practices.  
   d. Is appropriately positioned and adequately resourced.  

4. Which of the following types of IPPF guidance require(s) public exposure?  
   I. A new Implementation Guide.  
   II. A new standard.  
   IV. A new definition in the IPPF Glossary.  
   a. III only.  
   b. II and IV only.  
   c. II, III, and IV only.  
   d. I, II, III, and IV.  

5. Which of the following is a part of the Mission of Internal Audit?  
   a. Promoting an ethical culture in the profession of internal auditing.  
   b. Protecting organizational value.  
   c. Reducing the occurrence of fraud.  
   d. Respecting the value and ownership of information received and not disclosing information without appropriate authority.  

6. Which of the following is not a role of the internal audit activity in best practice governance activities?  
   a. Support the board in enterprisewide risk assessment.  
   b. Ensure the timely implementation of audit recommendations.  
   c. Monitor compliance with the corporate code of conduct.  
   d. Discuss areas of significant risks.
1. **Solution: b (I and IV only)**

   I. Correct. According to Standard 2130.A1: “The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization’s governance, operations, and information systems regarding the:

   - Achievement of the organization’s strategic objectives;
   - Reliability and integrity of financial and operational information;
   - Effectiveness and efficiency of operations and programs;
   - Safeguarding of assets; and
   - Compliance with laws, regulations, policies, procedures, and contracts.”

   The specific engagement objective of determining if goods are charged to the appropriate account would address the objective regarding the reliability and integrity of information.

   II. Incorrect. The specific engagement objective described does not address compliance.

   III. Incorrect. The specific engagement objective described may address effectiveness of operations but does not address efficiency.

   IV. Correct. The specific engagement objective of determining if all goods paid for have been received would address the objective regarding safeguarding of assets.

2. **Solution: c (II, III, and IV only)**

   I. Incorrect. Implementation Guides are only recommended guidance; they are not mandatory guidance.

   II, III, and IV. Correct. The IIA’s Code of Ethics, Core Principles for the Professional Practice of Internal Auditing, and the Standards are mandatory guidance.
3. **Solution: d**
   a. Incorrect. This is a principle of The IIA’s Code of Ethics but not one of the Core Principles.
   b. Incorrect. This is the purpose of The IIA’s Code of Ethics.
   c. Incorrect. This is not a Core Principle, nor is it something even desirable across the internal audit profession, as practice will vary depending on organizational environment, culture, and level of maturity of the audit function.
   d. Correct. This is one of the 10 Core Principles.

4. **Solution: b (II and IV only)**
   I. Incorrect. The Implementation Guides do not require public exposure prior to issuance; they only require internal IIA committee approval.
   II. Correct. A new standard requires public exposure of 90 days.
   III. Incorrect. Supplemental Guides do not require public exposure; they only require internal IIA committee approval.
   IV. Correct. The Glossary is a part of the Standards. Thus, new definitions or changes to the definitions require 90-day public exposure.

5. **Solution: b**
   a. Incorrect. This is the purpose of the Code of Ethics.
   b. Correct. The Mission of Internal Audit is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.
   c. Incorrect. This is management’s responsibility. Internal audit evaluates the potential of fraud (Standard 2120.A2). Further, this is only one part of protecting organizational value.
   d. Incorrect. This is the confidentiality principle from the Code of Ethics.

6. **Solution: b**
   a. Incorrect. The internal audit activity performs this role. The board and management are responsible for the identification of an appropriate risk model and methodology.
   b. Correct. It is the role of management to ensure the timely implementation of the audit recommendations.
   The internal audit activity is responsible for the development of a timely procedure to monitor the disposition of the audit recommendations. The internal audit activity works with senior management and the audit committee to ensure that audit recommendations receive appropriate attention.
   c. Incorrect. The internal audit activity should monitor compliance with the corporate code of conduct set by the board and management.
   d. Incorrect. The internal audit activity is responsible for discussing significant financial, technical, and operational risks and exposures and the plans to minimize such risks.