

# 5-Day Training ToC – Internal Audit Function

**Duration: 5 Days (8 hours per day)**

---

## **Overview**

**This program is designed to prepare participants for the CIA Part 3 exam by providing an in-depth understanding of business acumen, information security, information technology, and financial management. It combines theory, practical applications, and mock tests to strengthen exam readiness.**

---

## **Prerequisites**

- Basic knowledge of auditing principles and internal control frameworks.
  - Familiarity with financial statements and accounting concepts.
  - Awareness of IT and cybersecurity fundamentals.
  - Recommended: Prior completion of CIA Part 1 & Part 2 domains (not mandatory).
- 

## **Day 1 – Business Acumen (Domain I - 35%)**

### **Session 1: Organizational Objectives, Behavior, and Performance**

- Strategic Planning Process (objectives, globalization, mission alignment)
- Performance Measures (financial vs. operational, efficiency, effectiveness)

- Organizational Behavior (group dynamics, motivation, politics, job design)
- Management Effectiveness (leadership, mentoring, commitment building)

## **Session 2: Organizational Structure and Business Processes**

- Centralized vs. decentralized structures and risks
- Risk implications in HR, procurement, marketing, logistics
- Project management basics: scope, time, cost, change
- Contracts: types, forms, key elements

## **Session 3: Data Analytics**

- Data types, governance, and role in auditing
  - Analytics process: defining questions, cleaning, analysis, reporting
  - Applications: diagnostic, predictive, anomaly detection
- 

## **Day 2 – Information Security (Domain II - 25%)**

### **Session 1: Core Information Security Concepts**

- Physical security (biometrics, cards, keys)
- Authentication & authorization (passwords, 2FA, digital signatures)
- Security controls (encryption, firewalls, antivirus)

### **Session 2: Emerging Security Threats & Practices**

- Data privacy laws and compliance impact
  - Risks: BYOD, IoT, phishing, ransomware, hacking
  - Cybersecurity policies and governance practices
- 

## **Day 3 – Information Technology (Domain III - 20%)**

### **Session 1: Application and System Software**

- Systems Development Lifecycle (SDLC)
- Databases and internet basics
- Software systems overview: CRM, ERP, GRC

### **Session 2: IT Infrastructure and Control Frameworks**

- LAN, WAN, VPN, servers, routers
- Key roles: network admin, DB admin, helpdesk
- IT control frameworks: COBIT, ITIL, ISO 27000

### **Session 3: Disaster Recovery**

- Hot, warm, cold sites
  - Backup processes and strategies
  - Recovery procedures & best practices
-

## **Day 4 – Financial Management (Domain IV - 20%)**

### **Session 1: Financial Accounting and Analysis**

- Types of financial statements and key terms
- Emerging concepts: consolidation, fair value, FX transactions
- Financial analysis: horizontal, vertical, ratios

### **Session 2: Managerial Accounting**

- CVP analysis, budgeting, expense allocation
  - Costing systems: absorption, activity-based, standard
  - Decision-making: relevant, incremental, fixed costs
- 

## **Day 5 – Consolidation & Exam Preparation**

### **Session 1: Mock Tests & Case Scenarios**

- Practice exam (100-question format)
- Case-based scenarios for practical application

### **Session 2: Discussion & Clarifications**

- Review of mock test answers
- Q&A on difficult topics

### **Session 3: Exam Strategy & Wrap-Up**

- Study tips and memory techniques
  - Time management strategies for the exam
  - Final guidance and preparation roadmap
- 

### **Deliverables**

- Comprehensive study materials (slides, guides)
- Mock tests for practice
- Participation certificate