## Domain 1: Information Systems Auditing Process

**Objective:** Understand audit planning, execution, reporting, and follow-up.
**Topics:**

- **1.1 Audit Standards & Guidelines**
    - ISACA's Code of Professional Ethics
    - IS Audit and Assurance Standards
- **1.2 Risk-Based Audit Planning**
    - Risk assessment techniques
    - Audit charter, scope, and objectives
- **1.3 Internal Controls**
    - Types of controls (preventive, detective, corrective)
    - Control assessment methods
- **1.4 Audit Evidence & Techniques**
    - Sampling, walkthroughs, testing
- **1.5 Communicating Audit Results**
    - Audit reporting, communication with stakeholders
- **1.6 Audit Follow-up & Corrective Actions**
    - Risk acceptance and residual risk

## Domain 2: Governance and Management of IT

**Objective:** Evaluate the IT governance structure and its ability to support business goals.
**Topics:**

- **2.1 IT Governance Frameworks**
    - COBIT, ISO/IEC 38500, ITIL
- **2.2 Strategic Planning & Steering Committees**

    - Alignment with business objectives

- **2.3 IT Policies, Standards, and Procedures**
- **2.4 IT Performance Monitoring** (1 hr)
    - KPIs, balanced scorecards
- **2.5 Organizational Structure & HR Management**
    - Segregation of duties, roles, and responsibilities
- **2.6 Risk Management Practices**
    - Risk identification, risk appetite, and mitigation strategies

## Domain 3: Information Systems Acquisition, Development and Implementation (6 hours)

**Objective:** Assess practices in system development, procurement, and change management.
**Topics:**

- **3.1 Business Case Development**
- **3.2 Project Management Practices**
    - Waterfall, Agile, DevOps
- **3.3 System Development Life Cycle (SDLC)**
    - Planning, analysis, design, testing, implementation
- **3.4 Acquisition/Procurement**
    - Vendor management, RFPs, third-party risk
- **3.5 Change & Release Management**
    - Change control, versioning, rollback
- **3.6 Data Conversion & Post-Implementation Review**

## Domain 4: Information Systems Operations and Business Resilience

**Objective:** Ensure effective and secure IT operations including resilience.
**Topics:**

- **4.1 IT Operations Management**
    - Scheduling, job controls, maintenance
- **4.2 Incident & Problem Management**
- **4.3 Disaster Recovery & Business Continuity Planning**
    - BIA, RTO/RPO, recovery sites
- **4.4 Backup & Restore Procedures**
- **4.5 IT Asset and Configuration Management**
- **4.6 Performance Monitoring & Capacity Planning**

## Domain 5: Protection of Information Assets

**Objective:** Evaluate information security policies, procedures, and controls.
**Topics:**

- **5.1 Logical Access Controls**
    - IAM, MFA, access provisioning
- **5.2 Physical & Environmental Security**
- **5.3 Network Security & Perimeter Defense**
    - Firewalls, IDS/IPS, segmentation
- **5.4 Encryption & Cryptography**
- **5.5 Data Classification & Protection**
- **5.6 Security Awareness & Training Programs**
- **5.7 Security Event Logging and SIEM**