Certified Information Systems Auditor (CISA)
Course Outline

Class #	Contents	Duration
Domain 1: Information Systems Auditing Process		
Part A: Planning		
01	• IS Audit Standards, Guidelines, and Codes of Ethics • Business Processes • Types of Controls	2 Hours
02	• Risk-based Audit Planning • Types of Audits and Assessments	2 Hours
Part B: Execution		
03	• Audit Project Management • Sampling Methodology • Audit Evidence Collection Techniques	2 Hours
04	• Data Analytics • Reporting and Communication Techniques • Quality Assurance and Improvement of the Audit Process	2 Hours
Domain 2: Governance and Management of IT		
Part A: IT Governance		
05	• IT Governance and IT Strategy • IT-related Frameworks • IT Standards, Policies and Procedures	2 Hours
06	• Organizational Structure • Enterprise Architecture • Enterprise Risk Management • Maturity Models • Laws, Regulations and Industry Standards Affecting the Organization	2 Hours
Part B: IT Management		
07	• IT Resource Management • IT Service Provider Acquisition and Management	2 Hours
08	• IT Performance Monitoring and Reporting • Quality Assurance and Quality Management of IT	2 Hours

Class #	Contents	Duration
Domain 3: Information Systems Acquisition, Development, and Implementation		
Part A: Information Systems Acquisition and Development		
09	• Project Governance and Management • Business Case and Feasibility Analysis	2 Hours
10	• System Development Methodologies • Control Identification and Design	2 Hours
Part B: Information Systems Implementation		
11	• Testing Methodologies • Configuration and Release Management	2 Hours
12	• System Migration, Infrastructure Deployment and Data Conversion • Post-implementation Review	2 Hours
Domain 4: Information Systems Operations and Business Resilience		
Part A: Information Systems Operations		
13	• Common Technology Components • IT Asset Management • Job Scheduling and Production Process Automation • System Interfaces • End-user Computing • Data Governance	2 Hours
14	• Systems Performance Management • Problem and Incident Management • Change, Configuration, Release and Patch Management • IT Service Level Management • Database Management	2 Hours
Part B: Business Resilience		
15	• Business Impact Analysis • System Resiliency • Data Backup, Storage and Restoration	2 Hours
16	• Business Continuity Plan • Disaster Recovery Plans	2 Hours
Chapter 5: Protection of Information Assets		
Part A: Information Asset Security and Control		
17	• Information Asset Security Frameworks, Standards and Guidelines • Privacy Principles • Physical Access and Environmental Controls	2 Hours

Class #	Contents	Duration
	• Identity and Access Management • Network and End-point Security	
18	• Data Classification • Data Encryption and Encryption-related Techniques • Public Key Infrastructure • Web-based Communication Technologies • Virtualized Environments • Mobile, Wireless and Internet-of-things Devices	2 Hours
Part B: Security Event Management		
19	• Security Awareness Training and Programs • Information System Attack Methods and Techniques • Security Testing Tools and Techniques	2 Hours
20	• Security Monitoring Tools and Techniques • Incident Response Management • Evidence Collection and Forensics	2 Hours
Sample Test		
	Mock Test – 01	2 Hours
	Mock Test – 02	2 Hours
	Total Course Length:	**44 Hours**