Certified Information Systems Auditor (CISA)

Course Introduction — 4m

Course Introduction

Module 01 - The Process of Auditing Information Systems — 3h 44m

Lesson 1: Management of the Audit Function

Organization of the IS Audit Function
IS Audit Resource Management
Audit Planning
Effect of Laws and Regulations on IS Audit Planning

Lesson 2: ISACA IT Audit and Assurance Standards and Guidelines

ISACA IT Audit And Assurance Standards And Guidelines
ISACA IT Audit And Assurance Standards Framework
Auditing Standards
Audit Guidelines
Audit and Assurance Tools and Techniques
Relationship Among Standards, Guidelines, and Tools and Techniques
Information Technology Assurance Framework
Information Technology Assurance Framework Components
ITAF General Standards (Section 2200)
ITAF Performance Standards (Section 2400)
Reporting Standards (Section 2600)
IT Assurance Guidelines (Section 3000)

Lesson 3: Risk Analysis

Risk Analysis

Lesson 4: Internal Controls

Internal Control Objectives
IS Control Objectives
COBIT
General Controls
IS Controls

Lesson 5: Performing An IS Audit

Performing an IS Audit
Classification of Audits
Audit Programs
Audit Methodology
Fraud Detection
Risk-Based Auditing
Audit Risk and Materiality
Risk Assessment and Treatment
Risk Assessment Techniques
Audit Objectives
Compliance Versus Substantive Testing
Evidence
Interviewing and Observing Personnel in the Performance Of Their Duties
Sampling
Using The Services Of Other Auditors And Experts
Computer-Assisted Audit Techniques (CAAT)
Evaluation Of Audit Strengths And Weaknesses
Communicating Audit Results
Management Implementation Of Recommendations

Audit Documentation
Lesson 6: Control Self-Assessment
Objectives of CSA
Benefits of CSA
Disadvantages of CSA
Auditor Role in CSA
Technology Drivers for CSA
Traditional Versus CSA Approach
Lesson 7: The Evolving IS Audit Process
Automated Work Papers
Integrated Auditing
Continuous Auditing
Module 01 Review

Module 02 - Governance and Management of IT 3h 40m

Lesson 1: Corporate Governance
Corporate Governance
Lesson 2: IT Governance
IT Governance
Lesson 3: IT Monitoring and Assurance Practices for Board and Senior Management
IT Monitoring and Assurance Practices for Board and Senior Management
Best Practices for IT Governance
IT Governance Frameworks
Audit Role in IT Governance
IT Strategy Committee
IT Balanced Scorecard
Information Security Governance
Importance of Information Security Governance
Outcomes of Security Governance
Effective Information Security Governance
Roles and Responsibilities of Senior Management and Board of Directors
Enterprise Architecture
Lesson 4: Information Systems Strategy
Strategic Planning
Steering Committee
Lesson 5: Maturity and Process Improvement Models
Maturity and Process Improvement Models
Lesson 6: IT Investment and Allocation Practices
IT Investment and Allocation Practices
Implement IT Portfolio Management
IT Portfolio Management Versus Balanced Scorecard
Lesson 7: Policies and Procedures
Policies
Information Security Policy
Procedures
Lesson 8: Risk Management
Risk Management
Developing a Risk Management Program
Risk Management Process
Risk Analysis Methods
Lesson 9: IS Management Practices
Human Resource Management
Organizational Change Management
Financial Management Practices
Quality Management

Information Security Management
Performance Optimization
Lesson 10: IS Organizational Structure and Responsibilities
IS Roles and Responsibilities
Segregation of Duties
Segregation of Duties Controls
Compensating Controls for Lack of Segregation
Lesson 11: Auditing IT Governance Structure and Implementation
Reviewing Documentation
Reviewing Contractual Commitments
Lesson 12: Business Continuity Planning
IS Business Continuity Planning
Disasters and Other Disruptive Events
Business Continuity Planning Process
Business Continuity Policy
Business Impact Analysis
Classification of Operations and Criticality Analysis
Development of Business Continuity Plans
Other Issues and Plan Development
Components of a BCP
BCP Testing
BCP Maintenance
Summary of BCP
Module 02 Review

Module 03 - Information Systems Acquisition, Development and Implementation 3h 12m

Lesson 1: Business Realization
Portfolio/Program Management
Business Case Development and Approval
Benefits Realization Techniques
Lesson 2: Project Management Structure
Project Context and Environment
Project Organizational Forms
Project Communication and Culture
Project Objectives
Roles and Responsibilities of Groups and Individuals
Lesson 3: Project Management Practices
Initiation of a Project
Project Planning
Example of Project Management for New Software
Software Size Estimation
Lines of Source Code
Function Point Analysis (FPA)
Function Points
Cost Budgets
Software Cost Estimation
Scheduling and Establishing the Timeframe
Critical Path Methodology
Gantt Charts
Program Evaluation Review Technique (PERT)
Time Box Management
General Project Management
Project Controlling
Management of Resource Usage
Management of Risk
Closing a Project

Lesson 4: Business Application Development
Traditional SDLC Approach
SDLC Phases
SDLC
Integrated Resource Management Systems
Description of SDLC Phases
Risks Associated with Software Development
Lesson 5: Business Application Systems
Electronic Commerce
E-Commerce Models
E-Commerce Architectures
E-Commerce Risks
E-Commerce Requirements
E-Commerce Audit and Control Issues or Best Practices
Components of PKI
Electronic Data Interchange
General Requirements of EDI
Traditional EDI
Web Based EDI
EDI Risks and Controls
Controls in EDI Environment
E-Mail
E-Mail Security Issues
Standards for E-Mail Security
Point-Of-Sale Systems (POS)
Electronic Banking
Risk Management Challenges in E-Banking
Risk Management Controls for E-Banking
Electronic Finance
Payment Systems
Electronic Money Model
Electronic Checks Model
Electronic Transfer Model
Electronic Funds Transfer
Controls in an EFT Environment
Automated Teller Machines
Image Processing
Business Intelligence
Decision Support System (DSS)
DSS Frameworks
Customer Relation Management (CRM)
Supply Chain Management (SCM)
Lesson 6: Alternative Forms of Software Project Organization
Agile Development
Prototyping
Rapid Application Development (RAD)
Lesson 7: Alternative Development Methods
Data Oriented System Development
Object Oriented System Development
Component-Based Development
Web-Based Application Development
Software Reengineering
Reverse Engineering
Lesson 8: Infrastructure Development/Acquisition Practices
Project Phases of Physical Architecture Analysis
Planning Implementation of Infrastructure

Critical Success Factors
Hardware Acquisition
Acquisition Steps
System Software Acquisition
System Software Implementation
System Software Change Control Procedures
Lesson 9: Information Systems Maintenance Practices
Change Management Process Overview
Deploying Changes
Documentation
Testing Changed Programs
Auditing Program Changes
Emergency Changes
Change Exposures (Unauthorized Changes)
Configuration Management
Lesson 10: System Development Tools And Productivity Aids
Code Generators
Computer Aided Software Engineering
Fourth-Generation Languages (4GL)
Lesson 11: Business Process Reengineering And Process Change Projects
Business Process Reengineering And Process Change Projects Continued
Benchmarking Process
The Benchmarking Process
ISO 9126
Software Capability Maturity Model
ISO 15504
Lesson 12: Application Controls
Inputs Controls
Processing Procedures And Controls
Processing Controls
Data File Control Procedures
Output Controls
Business Process Control Assurance
Lesson 13: Auditing Application Controls
Risk Assessment Model To Analyze Application Controls
Observing And Testing User Performing Procedures
Data Integrity Testing
Example Of Referential And Relational Integrity
Data Integrity In Online Transaction Processing Systems
Test Application Systems
Continuous Online Auditing
Online Auditing Techniques
Lesson 14: Auditing Systems Development, Acquisition And Maintenance
Project Management
Feasibility Study
Requirements Definition
Software Acquisition Process
Detailed Design And Development
Testing
Implementation Phase
Post Implementation Review
System Change Procedures And The Program Migration Process
Module 03 Review

Module 04 - Information Systems Operations, Maintenance and Support 2h 47m

Lesson 1: Information Systems Operations
Management of IS Operations
Service Management
Service Level
Infrastructure Operations
Scheduling
Monitoring Use of Resources
Process of Incident Handling
Problem Management
Detection, Documentation, Control, Resolution and Reporting of Abnormal Conditions
Support/Helpdesk
Change Management Process
Release Management
Information Security Management
Media Sanitization

Lesson 2: Information Systems Hardware

Computer Hardware Components and Architecture
Common Enterprise Backend Devices
Specialized Devices
Risks
Security Control
Radiofrequency Identification
RFID Applications
RFID Risks
RFID Security Control
Hardware Maintenance Program
Hardware Monitoring Procedures
Capacity Management

Lesson 3: IS Architecture and Software

Operating Systems
Software Integrity Issues
Activity Logging and Reporting Options
Data Communication Software
Data Management
File Organization
Database Management Systems
Example of Data in DBMS
DBMS Architecture
DBMS Metadata Architecture
Database Structure
Relational Database
Database Models
Relational Database Model
Database Controls
Tape and Disk Management Systems
Utility Programs
Software Licensing Issues
Digital Rights Management

Lesson 4: Network Infrastructure

Enterprise Network Architecture
Types of Networks
Network Services
Network Standards and Protocols
OSI Architecture
OSI Layers

Application of the OSI Model in Network Architectures
Local Area Network
Network Physical Media Specifications
Implementation of WANs
LAN Media Access Technologies
LAN Components
OSI Layer Diagram
LAN Technology Selection Criteria
Wide Area Networks
WAN Message Transmission Techniques
WAN Devices
WAN Technologies
Wireless Networks
Wireless Wide Area Networks
Wireless Local Area Networks
Wireless Security
Wireless Application Protocol
Risks of Wireless Communications
World Wide Web Services
General Internet Terminology
Network Administration and Control
Network Performance Metrics
Network Management Issues
Network Management Tools
Client/Server Technology

Lesson 5: Disaster Recovery Planning

Recovery Point Objective and Recovery Time Objective
Recovery Strategies
Application Disaster Recovery Methods
Data Storage Disaster Recovery Methods
Telecommunication Networks Disaster Recovery Methods
Methods for Network Protection
Development of Disaster Recovery Plans
Organization and Assignment Of Responsibilities
Backup and Restoration
Off-Site Library Controls
Types of Backup Devices and Media
Periodic Backup Procedures
Frequency of Rotation
Backup Schemes
Module 04 Review

Module 05 - Protection of Information Assets 2h 30m

Lesson 1: Importance Of Information Security
Key Elements of Information Security Management
Information Security Management Roles and Responsibilities
Inventory and Classification of Information Assets
System Access Permission
Mandatory and Discretionary Access Controls
Privacy Management Issue and the Role of IS Auditors
Critical Success Factors to Information Security Management
Information Security and External Parties
Identification of Risks Related to External Parties
Addressing Security When Dealing with Customers
Addressing Security and Third-Party Agreements
Human Resources Security and Third Parties

Computer Crime Issues and Exposures
Types of Computer Crimes
Peer to Peer, Instant Messaging, Data Leakage and Web-Based Technologies
Security Incident Handling and Response

Lesson 2: Logical Access

Logical Access Exposures
Familiarization with the Enterprise IT Environment
Paths of Logical Access
General Points of Entry
Logical Access Control Software
Identification and Authentication
Features of Passwords
Identification and Authentication Best Practices
Token Devices, One-Time Passwords
Management of Biometrics
Single Sign-On
Authorization Issues
Access Control Lists
Logical Access Security Administration
Remote Access Security
Common Connectivity Methods
Remote Access Using PDAs
Access Issues with Mobile Technology
Access Rights to System Logs
Tools for Audit Trail Analysis
Use of Intrusion Detection
Storing, Retrieving, Transporting and Disposing of Confidential Information

Lesson 3: Network Infrastructure Security

LAN Security
Virtualization
Client/Server Security
Wireless Security Threats and Risks Mitigation
Internet Threats and Security
Network Security Threats
Internet Security Control Audits
Firewall Security Systems
Common Attacks Against a Firewall
Examples of Firewall Implementation
Intrusion Detection
Describing IDS and IPS Deployment
Encryption
Uses of Encryption
Viruses
Technical Controls Against Viruses
AV Software
Voice Over IP
Private Branch Exchange

Lesson 4: Auditing Information Security Management Framework

Auditing Logical Access
Techniques for Testing Security

Lesson 5: Auditing Network Infrastructure Security

Auditing Remote Access
Network Penetration Test
Types of Penetration Tests
Full Network Assessment Reviews
Development and Authorization of Network Changes

Unauthorized Changes
Computer Forensics
Chain of Evidence
Lesson 6: Environmental Exposures and Controls
Lesson 7: Physical Access Exposures and Controls
Physical Access Exposures
Physical Access Controls
Auditing Physical Access
Lesson 8: Mobile Computing
Module 05 Review
Course Closure

Total Duration: 15hrs 56m