Certified Information Systems Security Auditor

Course Title: C)ISSA

Duration: 4 days

Language: English

Class Format Options:

Instructor-led classroom
Live Online Training

Prerequisites:

- A minimum of 1 year of Information Systems

Student Materials:

- Student Workbook

Certification Exams:

- Mile2 C)ISSA – Certified Information Systems Security Auditor
- Covers ISACA® CISA exam objectives

CPEs: 32 Hours

WHO SHOULD ATTEND?

- IS Security Officers
- IS Managers
- Risk Managers
- Auditors
- Information Systems Owners
- IS Control Assessors
- System Managers
- Government

COURSE OVERVIEW

Many organizations require an Information System Auditor's expert knowledge when it comes to identifying critical issues and providing effective auditing solutions. The knowledge and course content provided in the vendor neutral **Certified Information Systems Security Auditor -** C)ISSA will not only cover ISACA®'s exam but will provide a measurable certification that demonstrates proficiency in the IS Auditing Field.

The Certified Information Systems Security Auditor covers the skills and knowledge to assess vulnerabilities, report on compliance and implement controls for private and public enterprises.

The Certified Information Systems Security Auditors will receive in-depth knowledge in topics that pertain to the following:

IS audit, control, assurance, and security professionals, including IT consultants, auditors, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers.

Auditing Career

C)SS™ CERTIFIED SECURITY SENTINEL

C)ISSO™ Certified Information Systems Security Officer

C)ISMS-LA

C)ISMS-LI™

C)ISSA™ *

All CombosInclude:

- Online Video
- Electronic Book (Workbook/Lab guide*)
  *in all technical classes
- Exam Prep Questions
- Exam

ias™ INFORMATION ASSURANCE SERVICES · pt™ PENETRATION TESTING · dr™ DISASTER RECOVERY · gs™ GENERAL SECURITY · SC™ SECURE CODING · vbp™ VIRTUALIZATION BEST PRACTICES · ws™ WIRELESS SECURITY · cf™ COMPUTER FORENSICS

ACCREDITATIONS

UPON COMPLETION

Upon completion, **Certified Information Systems Security Auditor** students will be able to establish industry acceptable auditing standards with current best practices and policies. Students will also be prepared to competently take the CISSA exam.

EXAM INFORMATION

The **Certified Information Systems Security Auditor**exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions. The cost is $400 USD and must be purchased from Mile2.com.

COURSE CONTENT

I. The Process of Auditing Information Systems
II. Risk Based Auditing
III. Audit Planning and Performance
IV. Reporting on Audit
V. IT Governance and Management
VI. Strategic Planning and Models
VII. Resource Management
VIII. Business Continuity Planning
IX. Systems Acquisition, Development and Implementation
X. Systems Development Models
XI. Types of Specialized Business Applications
XII. Application Controls
XIII. Information Systems Operations, Maintenance and Support
XIV. System and Communications
XV. Hardware

DETAILED MODULEDESCRIPTION

Chapter One Section A – The Process of Auditing Information Systems

Exam Relevance
Agenda
Chapter 1 Learning Objectives
Learning Objectives (continued)
Audit Charter
Definition of Auditing
Definition of Information Systems Auditing
Audit Objectives
Audit Planning
Audit Planning cont.
IS Audit Resource Management
Types of Audits
Elements of an Audit
Creating the Plan for an Audit
Planning the Audit
Audit Methodology
Phases of an Audit
Audit Workpapers
Audit Procedures
Types of Tests for IS Controls
Forensic Audits
Fraud Detection

Chapter One Section B – Risk Based Auditing

Risk – Based Auditing
Definition of Risk
Purpose of Risk Management
Risk Management
Purpose of Risk Analysis
Why Use Risk Based Auditing
Risk Assessment and Treatment
Risk Assessment and Treatment cont.
General Controls
Internal Controls
Areas of Internal Control
IS Controls Versus Manual Controls
IS Controls
IS Controls cont.
Internal Control Objectives
Assessing and Implementing Countermeasures
Performing an Audit Risk Assessment
A Risk Based Audit Approach
Risk – based Auditing
Risk – based Auditing

Chapter One Section C – Audit Planning and Performance

Audit Planning
Effect of Laws and Regulations on IS Audit Planning
Performing the Audit
ISACA IT Audit and Assurance Tools and Techniques
ISACA IT Audit and Assurance Standards Framework
Relationship Among Standards, Guidelines and Tools and Techniques
ISACA IT Audit and Assurance Standards Framework cont.
Evidence
Gathering Evidence
Sampling
Compliance vs. Substantive Testing
Testing Controls
Integrated Auditing
Using the Services of Auditors and Experts
Audit Risk
Computer-assisted Audit Techniques

Chapter One Section D – Reporting on Audit

Audit Analysis and Reporting
Audit Documentation
Automated Work Papers
Automated Work Papers cont.
Evaluation of Audit Strengths and Weaknesses
Communicating Audit Results
Management Implementation of Audit Recommendations

Chapter Two Section A – IT Governance and Management of IT

Exam Relevance
Agenda
Task Statements
Governance and Management of IT
Corporate Governance
IT Governance
Information Technology Monitoring and Assurance Practices for Management
Best Practices for IT Governance
Information Security Governance
Result of Security Governance

Chapter Two Section B – Strategic Planning and Models

IS Strategy
Strategic Enterprise Architecture Plans
IT Strategy Committee
Standard IT Balanced Scorecard
Enterprise Architecture
Maturity and Process Improvement Models
IT Investment and Allocation Practices
Auditing IT Governance Structure and Implementation
Policies, Standards and Procedures
Policies and Procedures
Policies
Procedures
Standards
Risk Management
Risk Management Process
Risk Analysis Methods
Risk Mitigation

Chapter Two Section C – Resource Management

Organization of the IT Function
IS Roles and Responsibilities
Segregation of Duties Within IS
Segregation of Duties Controls
Human Resource Management
Sourcing Practices
Management of IT Functional Operations
Organizational Change Management
Change Management cont.
Quality Management
Performance Optimization
Reviewing Documentation
Reviewing Contractual Commitments

Chapter Two Section D – Business Continuity Planning

Business Continuity Planning
IS Business Continuity Planning
Disasters and Other Disruptive Events
Business Continuity Planning Process
Business Continuity Policy
Business Continuity Planning Incident Management
Business Impact Analysis cont.
Development of Business Continuity Plans
Other Issues in Plan Development
Components of a Business Continuity Plan
Components of a Business Continuity Plan cont.

Insurance
Plan Testing
Summary of Business Continuity
Auditing Business Continuity
Reviewing the Business Continuity Plan
Evaluation of Prior Test Results
Evaluation of Offsite Storage
Interviewing Key Personnel
Evaluation of Security at Offsite Facility
Reviewing Alternative Processing Contract
Reviewing Insurance Coverage
End of Domain

Chapter Three Section A – Information Systems Acquisition, Development and Implementation

Exam Relevance
Agenda
Learning Objectives
Learning Objectives cont.
Program and Project Management
Portfolio/Program Management
Portfolio/Program Management cont.
Business Case Development and Approval
Benefits Realization Techniques
General IT Project Aspects
Project Context and Environment
Project Organizational Forms
Project Communication
Project Objectives
Roles and Responsibilities of Groups and Individuals
Project Management Practices
Project Planning
Project Planning cont.
General Project Management
Project Controlling
Project Risk
Closing a Project

Chapter Three Section B – Systems Development Models

Business Application Development
Traditional SDLC Approach
Traditional SDLC Approach cont.
Traditional SDLC Approach cont.
Requirements Definition
Business Process Reengineering and Process Change Projects
Business Process Reengineering and Process Change Projects cont.
Risk Associated with Software Development
Use of Structures Analysis, Design and Development Techniques
Alternative Development Methods
Agile Development
Agile Development
Prototyping
Rapid Application Development
Other Alternative Development Methods
Computer-aided Software Engineering
Fourth-generation Languages

Chapter Three Section C – Types of Specialized Business Applications

Electronic Commerce
Electronic Data Interchange
Electronic Mail
Electronic Banking
Electronic Finance
Electronic Funds Transfer
Automated Teller Machine
Artificial Intelligence and Expert Systems
Business Intelligence
Decision Support Systems
Decision Support Systems cont.
Acquisition
Infrastructure Development / Acquisition Practices
Project Phases of Physical Architecture Analysis
Hardware Acquisition
System Software Acquisition
Auditing Systems Development, Acquisition and Maintenance
Auditing Systems Development Acquisition
System Software Change Control Procedures

Chapter Three Section D – Application Controls

Application Controls
Input/Origination Controls
Processing Procedures and Controls
Output Controls
Types of Output Controls
Business Process Control Assurance
Auditing Application Controls
Application Testing
Precautions Regarding Testing
System Change Procedures and the Program Migration Process
System Change Procedures and the Program Migration Process cont.
End of Chapter Three

Chapter Four Section A – Information Systems Operations, Maintenance and Support

Exam Relevance
Agenda
Learning Objectives
Learning Objectives cont.
Information Security Management
Information Systems Operations
Management of IS Operations
IT Service Management
Infrastructure Operations
Monitoring Use of Resources
Support / Help Desk
Change Management Process
Release Management

Chapter Four Section B – System and Communications Hardware

Computer Hardware Components and Architectures
Computer Hardware Components and Architectures cont.
Security Risks with Portable Media
Security Controls for Portable Media
Hardware Maintenance Program
Hardware Monitoring Procedures
Capacity Management
IS Architecture and Software
Operating Systems
Access Control Software
Data Communications Software
Data Management
Database Management System cont.
Tape and Disk Management Systems
Utility Programs
Software Licensing Issues
Digital Rights Management
Auditing Networks
Network Infrastructure
Enterprise Network Architectures
Types of Networks
Network Standards and Protocol
OSI Architecture
OSI Architecture (continued)
Application of the OSI Model in Network Architectures cont.
Network Architectures
Network Components
Communications Technologies
Communications Technology cont.
Wireless Networking
Risks Associated with Wireless Communications
Internet Technologies
Auditing of Network Management
Auditing of Applications Management
Hardware Reviews
Operating System Reviews
Database Reviews
Network Infrastructure and Implementation Reviews
Network Infrastructure and Implementation Reviews
Physical Security Audits
Access Controls Review
Scheduling Reviews
Scheduling Reviews; Questions to Consider
Auditing Job Scheduling
Job Scheduling Reviews
Personnel Reviews
Business Continuity and Disaster Recovery

Audits
Auditing of Business Continuity Plans
Recovery Point Objective and Recovery Time Objective
Business Continuity Strategies
Recovery Strategies
Recovery Alternatives
Audit of Third Party Recovery Agreements
Organization and Assignment of Responsibilities
Team Responsibilities
Backup and Restoration

Chapter Four Section C – Auditing Networks

Network Infrastructure
Enterprise Network Architectures
Types of Networks
Network Services
Network Standards and Protocols
OSI Architecture
OSI Architecture (continued)
Application of the OSI Model in Network Architectures cont.
Network Architectures
Network Components
Communications Technologies
Communications Technology cont.
Wireless Networking
Risk Associated with Wireless Communications
Internet Technologies
Auditing of Network Management
Auditing of Applications Management
Hardware Reviews
Operating Systems Reviews
Database Reviews
Network Infrastructure and Implementation Reviews
Network Infrastructure and Implementation Reviews
Physical Security Audits
Access Controls Review
Access Controls Review cont.
Scheduling Reviews
Scheduling Reviews; Questions to Consider
Auditing Job Scheduling
Job Scheduling Reviews
Personnel Reviews

Chapter Four Section D – Business Continuity and Disaster Recovery Audits

Auditing of Business Continuity Plans
Recovery Point Objective and Recovery Time Objective
Business Continuity Strategies
Recovery Strategies
Recovery Alternatives
Audit of Third Party Recovery Agreements
Organization and Assignment of Responsibilities
Team Responsibilities
Backup and Restoration
End of Domain Four

Chapter Five Section A – Protection of Information Assets

Exam Relevance
Course Agenda
Chapter 5 Task Statements
Knowledge Areas
Information Security Management
Importance of Information Security Management
Key Elements of Information Security Management
Critical Success Factors to Information Security Management
Inventory and Classification of Information Assets
Privacy Management Issues and the Role of IS Auditors
Social Media Risks

Chapter Five Section B – Access Controls

System Access Permission
Mandatory and Discretionary Access Controls
IAAA
Authentication
Authorization
Challenges with Identity Management
Identification and Authentication
Logical Access Exposures
Paths of Logical Access
Logical Access Control Software
Auditing Logical Access
Access Control Lists
Centralized versus Decentralized Access
Decentralized Access Risks
Single Sign-on (SSO)
Single Sign-on Advantages
Single Sign-on Disadvantages
Familiarization with the Organization's IT Environment
Remote Access
Remote Access Security
Auditing Remote Access
Auditing Remote Access (cont.)
Logging All System Access

Chapter Five Section C – Equipment and Network Security

Security of Portable Media
Mobile Device Security
Storing, Retrieving, Transporting and Disposing of Confidential Information
Concerns Associated with Storage Media
Network Infrastructure Security

Network Infrastructure Security cont.
LAN Security Issues
Client-server Security
Wireless Security Threats
Wireless Security Threats cont.
Audit Log Analysis Tools
Internet Threats and Security
Causes of Internet Attacks
Firewalls
Firewall Issues
Network Security Architectures
Honeypots and Honeynets
Intrusion Detection and Prevention Systems
IDS / IPS Components
IDS / IPS Features
Voice-Over IP (VoIP)
Techniques for Testing Security
Auditing Network Infrastructure Security

Chapter Five Section D – Encryption

Encryption Definition
Encryption
Symmetric Encryption
Asymmetric Algorithms
Hashing Algorithms
Digital Signatures
Digital Envelope
Public Key Infrastructure (PKI)
Uses of Encryption in Communications
Auditing Encryption Implementations
Malware
Viruses
Virus Protection
Other Forms of Malware
Incident Handling and Evidence
Security Incident Handling and Response
Evidence Handling
Physical and Environmental Controls
Physical Access Issues and Exposures
Physical Access Issues and Exposures cont.
Physical Access Controls
Controls for Environmental Exposures
Controls for Environmental Exposures cont.
Controls for Environmental Exposures cont.
Electrical Problems
Auditing Physical Access
End of Domain Five