Certified Information Systems Auditor (CISA)

Overview

This course is designed to help candidates prepare for sitting the ISACA CISA certification examination. By taking this course and obtaining CISA certification, your experience and skills in auditing and securing the organization's information systems will be validated. Securing the organization's information is a critical business objective in today's business environment. The information that an organization depends on to be successful can be at risk from numerous sources. By effectively managing audit processes, controls, and other security aspects of the business, you will greatly contribute to the overall security of the organization.

Prerequisites

- CompTIA Network+ Certification
- CompTIA Security+ Certification

Prerequisite Comments

To ensure your success, you should have at least five years of professional experience in information systems auditing, control, or security. You are also required to prove this level of experience to ISACA in order to obtain certification. The major areas of work experience are described in the CISA job practice domains:
- The process of auditing information systems
- Governance and management of IT
- Information systems acquisition, development, and implementation
- Information systems operations, maintenance, and service management
- Protection of information assets

Target Audience

The intended audience for this course is information security and IT professionals, particularly internal auditors, who are interested in earning the CISA certification. The course is also applicable to individuals who are interested in learning about information security audits, controls, and security.

Course Objectives

Upon successful completion of this course, students will be able to:
- implement information systems audit services in accordance with information

Register Online

Schedule

Class Length: 5 Days

G2R = "Guaranteed to Run" | OLL = "Online LIVE"
ILT = "Instructor-Led-Training" | HDL = "Hosted Distance Learning"

11/09/20	G2R	6:00AM - 2:00PM	HDL - All Locations (Pacific Time)	HDL	$3,475.00
11/09/20	G2R	6:00AM - 2:00PM	Online LIVE - Remote Learning (Pacific Time)	OLL	$3,475.00
03/15/21		6:00AM - 2:00PM	HDL - All Locations (Pacific Time)	HDL	$3,475.00
03/15/21		6:00AM - 2:00PM	Online LIVE - Remote Learning (Pacific Time)	OLL	$3,475.00
06/21/21		8:00AM - 4:00PM	HDL - All Locations (Pacific Time)	HDL	$3,475.00
06/21/21		8:00AM - 4:00PM	Online LIVE - Remote Learning (Pacific Time)	OLL	$3,475.00

systems audit standards, guidelines, and best practices.
- evaluate an organizations structure, policies, accountability, mechanisms, and monitoring practices.
- evaluate information systems acquisition, development, and implementation.
- evaluate the information systems operations, maintenance, and support of an organization; and evaluate the business continuity and disaster recovery processes used to provide assurance that in the event of a disruption, IT services are maintained.
- define the protection policies used to promote the confidentiality, integrity, and availability of information assets.

Course Outline

1 - The Process of Auditing Information Systems

ISACA Information Systems Auditing Standards and Guidelines
Fundamental Business Processes
Develop and Implement an Information Systems Audit Strategy
Plan an Audit
Conduct an Audit
The Evidence Life Cycle
Communicate Issues, Risks, and Audit Results
Support the Implementation of Risk Management and Control Practices

2 - IT Governance and Management

Evaluate the Effectiveness of IT Governance
Evaluate the IT Organizational Structure and HR Management
Evaluate the IT Strategy and Direction
Evaluate IT Policies, Standards, and Procedures
Evaluate the Effectiveness of Quality Management Systems
Evaluate IT Management and Monitoring of Controls
IT Resource Investment, Use, and Allocation Practices
Evaluate IT Contracting Strategies and Policies
Evaluate Risk Management Practices
Performance Monitoring and Assurance Practices
Evaluate the Organizations Business Continuity Plan

3 - Information Systems Acquisition, Development, and Implementation

Evaluate the Business Case for Change
Evaluate Project Management Frameworks and Governance Practices
Development Life Cycle Management
Perform Periodic Project Reviews
Evaluate Control Mechanisms for Systems
Evaluate Development and Testing Processes
Evaluate Implementation Readiness
Evaluate a System Migration
Perform a Post-Implementation System Review

4 - Information Systems Operations, Maintenance, and Support

Perform Periodic System Reviews
Evaluate Service Level Management Practices
Evaluate Third-Party Management Practices
Evaluate Operations and End User Management Practices
Evaluate the Maintenance Process
Evaluate Data Administration Practices
Evaluate the Use of Capacity and Performance Monitoring Methods
Evaluate Change, Configuration, and Release Management Practices
Evaluate Problem and Incident Management Practices
Evaluate the Adequacy of Backup and Restore Provisions

5 - Protection of Information Assets

Information Security Design
Encryption Basics
Evaluate the Functionality of the IT Infrastructure
Evaluate Network Infrastructure Security
Evaluate the Design, Implementation, and Monitoring of Logical Access Controls
Risks and Controls of Virtualization
Evaluate the Design, Implementation, and Monitoring of Data Classification Process
Evaluate the Design, Implementation, and Monitoring of Physical Access Controls
Evaluate the Design, Implementation, and Monitoring of Environmental Controls

Related Courses, Certifications, Exams

- Certified Information Systems Auditor (CISA)
- CISA - Certified Information Systems Auditor (CISA)