

Certified Information Systems Auditor (CISA) Boot Camp

Overview

The CISA Boot Camp is specifically designed to provide CISA candidates with the effective skills necessary to develop, manage, and supervise programs to defend against unauthorized admittance to information.

Target Audience

Course Objectives

Upon the completion of our CISA course, students will have:

- The Knowledge to perform comprehensive systems security audits
- Knowledge of the six core competencies that make up the CISA:
 - o IS Audit Process
 - o Protection of Information Assets
 - o IT Governance
 - o Systems and Infrastructure Life Cycle Management
 - o IT Service Delivery and Support
 - o Business Continuity and Disaster Recovery
- The required knowledge and ability to provide effective security audits

Course Outline

The IS Audit Process

ISACA IS Auditing Standards, Guidelines and Procedures and Code of Professional Ethics
IS auditing practices and techniques
Techniques to gather information and preserve evidence (e.g., observation, inquiry, interview, CAATs, electronic media)
The evidence life cycle (e.g., the collection, protection, chain of custody)
Control objectives and controls related to IS (e.g., CobiT)
Risk assessment in an audit context
Audit planning and management techniques
Reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution)
Control self-assessment (CSA)
Continuous audit techniques

[Register Online](#)

Schedule

Class Length: 5 Days

G2R = "Guaranteed to Run" | OLL = "Online LIVE"
ILT = "Instructor-Led-Training"

This course is not currently available on the public schedule. Please contact us using the information in the footer below to inquire about future dates or to schedule a private class.

IT Governance

The purpose of IT strategies, policies, standards and procedures for an organization and the essential elements of each IT governance frameworks

The processes for the development, implementation and maintenance of IT strategies, policies, standards and procedures (e.g., protection of information assets, business continuity and disaster recovery, systems and infrastructure lifecycle management, IT service delivery and support)

Quality management strategies and policies

Organizational structure, roles and responsibilities related to the use and management of IT

Generally accepted international IT standards and guidelines

Enterprise IT architecture and its implications for setting long-term strategic directions

Risk management methodologies and tools

The use of control frameworks (e.g., CobiT, COSO, ISO 17799)

The use of maturity and process improvement models (e.g., CMM, CobiT)

Contracting strategies, processes and contract management practices 2.12 practices for monitoring and reporting of IT performance (e.g., balanced scorecards, key performance indicators [KPI])

Relevant legislative and regulatory issues (e.g., privacy, intellectual property, corporate governance requirements)

IT human resources (personnel) management

IT resource investment and allocation practices (e.g., portfolio management return on investment (ROI))

Systems and Infrastructure Life Cycle

Benefits management practices, (e.g., feasibility studies, business cases)

Project governance mechanisms (e.g., steering committee, project oversight board)

Project management practices, tools, and control frameworks

Risk management practices applied to projects

Project success criteria and risks

Configuration, change and release management in relation to development and maintenance of systems and/or infrastructure

Control objectives and techniques that ensure the completeness, accuracy, validity, and authorization of transactions and data within IT systems applications

Enterprise architecture related to data, applications, and technology (e.g., distributed applications, web-based applications, web services, n-tier applications)

Requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis)

Acquisition and contract management processes (e.g., evaluation of vendors, preparation of contracts, vendor management, escrow)

System development methodologies and tools and an understanding of their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques)

Quality assurance methods

The management of testing processes (e.g., test strategies, test plans, test environments, entry and exit criteria)

Data conversion tools, techniques, and procedures

System and/or infrastructure disposal procedures

Software and hardware certification and accreditation practices

Post-implementation review objectives and methods (e.g., project closure, benefits realization, performance measurement)

System migration and infrastructure deployment practices

IT Service Delivery and Support

Service level management practices
Operations management best practices (e.g., workload scheduling, network services management, preventive maintenance)
Systems performance monitoring processes, tools, and techniques (e.g., network analyzers, system utilization reports, load balancing)
The functionality of hardware and network components (e.g., routers, switches, firewalls, peripherals)
Database administration practices
The functionality of system software including operating systems, utilities, and database management systems
Capacity planning and monitoring techniques
Processes for managing scheduled and emergency changes to the production systems and/or infrastructure including change, configuration, release, and patch management practices
Incident/problem management practices (e.g., help desk, escalation procedures, tracking)
Software licensing and inventory practices
System resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering)

Protection of Information Assets

The techniques for the design, implementation and monitoring of security (e.g., threat and risk assessment, sensitivity analysis, privacy impact assessment)
Logical access controls for the identification, authentication, and restriction of users to authorized functions and data (e.g., dynamic passwords, challenge/response, menus, profiles)
Logical access security architectures (e.g., single sign-on, user identification strategies, identity management)
Attack methods and techniques (e.g., hacking, spoofing, Trojan horses, denial of service, spamming)
Processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)
Network and Internet security devices, protocols, and techniques (e.g., SSL, SET, VPN, NAT)
Intrusion detection systems and firewall configuration, implementation, operation, and maintenance
Encryption algorithm techniques (e.g., AES, RSA)
Public key infrastructure (PKI) components (e.g., certification authorities, registration authorities) and digital signature techniques
Virus detection tools and control techniques
Security testing and assessment tools (e.g., penetration testing, vulnerability scanning)
Environmental protection practices and devices (e.g., fire suppression, cooling systems, water sensors)
Physical security systems and practices (e.g., biometrics, access cards, cipher locks, tokens)
Data classification schemes (e.g., public, confidential, private, and sensitive data)
Voice communications security (e.g., voice over IP)
The processes and procedures used to store, retrieve, transport, and dispose of confidential information assets
Controls and risks associated with the use of portable and wireless devices (e.g., PDAs, USB devices, Bluetooth devices)

Business Continuity and Disaster Recovery

Data backup, storage, maintenance, retention and restoration processes, and practices

Regulatory, legal, contractual, and insurance issues related to business continuity and disaster recovery

Business impact analysis (BIA)

The development and maintenance of the business continuity and disaster recovery plans

Business continuity and disaster recovery testing approaches and methods

Human resources management practices as related to business continuity and disaster recovery (e.g., evacuation planning, response teams)

Processes used to invoke the business continuity and disaster recovery plans

Types of alternate processing sites and methods used to monitor the contractual agreements (e.g., hot sites, warm sites, cold sites)

Related Courses, Certifications, Exams

- Certified Information Systems Auditor (CISA)
 - CISA
-