Security Auditing and Testing (CISA Prep) Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Security Auditing and Testing (CISA Prep) Training Course equips IT, cybersecurity, and audit professionals with the critical skills, methodologies, and frameworks necessary to effectively assess, evaluate, and enhance information systems security. Participants will gain hands-on knowledge in auditing practices, risk assessment, control evaluation, compliance verification, and reporting standards. The course emphasizes real-world applications, preparing candidates for the CISA certification by covering essential auditing processes, technical testing tools, and governance structures that protect organizational assets from internal and external threats.

Participants will explore the full lifecycle of information security auditing, including planning, risk-based testing, evidence collection, system evaluation, and audit reporting. Through practical exercises, case studies, and industry-standard tools, learners will develop competencies to identify vulnerabilities, measure controls effectiveness, and ensure compliance with global IT security regulations. The course also highlights emerging threats, cybersecurity frameworks, and audit best practices, ensuring participants are prepared to proactively safeguard enterprise systems and support organizational resilience.

Programme Curriculum

Security Auditing and Testing (CISA Prep) Training Course

Introduction

Security Auditing and Testing (CISA Prep) Training Course equips IT, cybersecurity, and audit professionals with the critical skills, methodologies, and frameworks necessary to effectively assess, evaluate, and enhance information systems security. Participants will gain hands-on knowledge in auditing practices, risk assessment, control evaluation, compliance verification, and reporting standards. The course emphasizes real-world applications, preparing candidates for the CISA certification by covering essential auditing processes, technical

testing tools, and governance structures that protect organizational assets from internal and external threats.

Participants will explore the full lifecycle of information security auditing, including planning, risk-based testing, evidence collection, system evaluation, and audit reporting. Through practical exercises, case studies, and industry-standard tools, learners will develop competencies to identify vulnerabilities, measure controls effectiveness, and ensure compliance with global IT security regulations. The course also highlights emerging threats, cybersecurity frameworks, and audit best practices, ensuring participants are prepared to proactively safeguard enterprise systems and support organizational resilience.

Course Objectives

1. Understand the fundamentals of information systems auditing and the CISA framework.
2. Apply risk assessment methodologies to evaluate information security programs.
3. Develop audit plans and perform effective control testing.
4. Assess compliance with IT governance, policies, and regulatory standards.
5. Identify vulnerabilities and evaluate the effectiveness of security controls.
6. Use automated and manual testing tools for system auditing.
7. Implement data integrity, confidentiality, and availability assessment techniques.
8. Conduct security audits across networks, applications, databases, and cloud systems.
9. Prepare professional audit reports and actionable recommendations.
10. Evaluate business continuity, disaster recovery, and incident response frameworks.
11. Apply IT general controls (ITGC) and application controls testing procedures.
12. Integrate emerging cybersecurity risks into auditing and testing strategies.
13. Prepare effectively for CISA certification exam objectives and domains.

Organizational Benefits

- Improved internal controls and IT security compliance
- Enhanced risk management and threat mitigation
- Stronger audit readiness for regulatory inspections
- Increased efficiency in IT governance practices
- Reduced vulnerabilities in information systems
- Strengthened business continuity and disaster recovery planning
- Enhanced staff competencies in auditing and testing techniques
- Improved decision-making through accurate audit reporting
- Better alignment with international standards and best practices
- Competitive advantage in cybersecurity assurance and certifications

Target Audiences

- IT auditors and internal audit staff
- Information security and cybersecurity professionals
- Risk management officers
- Compliance and governance specialists
- IT managers and system administrators
- Consultants in information systems auditing
- Aspiring CISA certification candidates
- Technology and cybersecurity trainers

Course Duration: 5 days

Course Modules

Module 1: Introduction to Information Systems Auditing

- Overview of IS auditing principles and frameworks
- CISA certification domains and exam structure
- Audit lifecycle and methodology
- Key IT governance concepts and standards
- Audit planning and risk identification techniques
- Case Study: Audit of an enterprise network for compliance gaps

Module 2: Risk Assessment and Control Evaluation

- Conducting risk assessments in IT environments
- Evaluating control objectives and key controls
- Prioritizing audit focus areas based on risk
- Assessing control design and operational effectiveness
- Documentation and evidence collection best practices
- Case Study: Risk-based audit of a cloud-based system

Module 3: Security Testing Techniques

- Manual and automated vulnerability testing
- Network penetration testing methods
- Application security testing and assessment
- Database auditing for data integrity and security
- Cloud security evaluation techniques
- Case Study: Penetration testing results and remediation analysis

Module 4: IT Governance and Compliance

- Understanding IT governance frameworks (COBIT, ISO 27001)
- Mapping regulatory requirements to organizational policies
- Assessing policy adherence and control effectiveness
- Evaluating vendor and third-party compliance
- Auditing IT compliance across departments
- Case Study: Compliance audit of an outsourced IT service provider

Module 5: Audit Reporting and Recommendations

- Structuring audit reports for clarity and impact
- Communicating findings to stakeholders and management
- Prioritizing recommendations based on risk
- Follow-up mechanisms for audit remediation
- Tools for audit report preparation and tracking
- Case Study: Reporting security audit findings to executive management

Module 6: IT General Controls (ITGC)

- Understanding ITGC frameworks and scope
- Access controls, change management, and backup procedures
- Evaluating ITGC for applications and infrastructure

- Monitoring user activity and segregation of duties
- Continuous auditing and control monitoring techniques
- Case Study: ITGC audit for a financial institution

Module 7: Business Continuity and Incident Response

- Reviewing business continuity management plans
- Evaluating disaster recovery strategies
- Assessing incident detection and response procedures
- Testing continuity plans through simulations
- Integrating audit findings into operational improvements
- Case Study: Incident response audit of a cyberattack scenario

Module 8: Preparing for CISA Certification

- Understanding exam domains and weightings
- Exam strategies, question types, and practice exercises
- Mapping course content to CISA learning objectives
- Self-assessment and readiness evaluations
- Study plans and resource recommendations
- Case Study: Mock CISA audit scenario with real-time assessment

Training Methodology

- Instructor-led presentations and expert demonstrations
- Hands-on lab exercises and practical testing simulations
- Group discussions and peer-to-peer learning sessions
- Case study analysis and problem-solving workshops
- Templates and tools for audit planning, testing, and reporting
- Continuous assessment, feedback, and exam preparation exercises

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
02 Nov 2026	06 Nov 2026	Online	$1,000
02 Nov 2026	06 Nov 2026	Physical	$1,500
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 Nov 2026	Physical	$4,500
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com