Certified Information Systems Auditor Training Course

Professional Development Training Course Outline

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

Course Introduction

The Certified Information Systems Auditor credential, globally recognized and awarded by ISACA, is the definitive mark of excellence for professionals who audit, control, monitor, and assess an organization's information technology and business systems. In today's landscape of escalating cyber threats, complex regulatory mandates, and accelerated Digital Transformation, the role of the CISA-certified professional has become more critical than ever. Certified Information Systems Auditor Training Course is designed to equip participants with the essential risk-based auditing skills and comprehensive knowledge across the five CISA domains. By mastering modern IT Governance, advanced security controls, Business Resilience planning, and the full System Development Life Cycle, participants will be prepared to successfully pass the CISA exam and immediately add tangible value in ensuring their enterprise's Information Assets are secure, reliable, and compliant.

This course moves beyond theoretical concepts, focusing heavily on practical application through real-world case studies and a hands-on training methodology that simulates actual audit scenarios. We emphasize understanding the convergence of IT Audit, Cybersecurity, and Enterprise Risk Management, which are top-tier organizational concerns. Successful completion empowers you to assess vulnerabilities, report on compliance assurance, and recommend robust control implementation strategies. Earning the CISA certification elevates your professional standing, demonstrating a commitment to the highest standards of digital trust and offering a competitive advantage in a high-demand global job market for IT Audit Managers and Information Security Analysts. Invest in this training to solidify your expertise and become a key assurance professional in the era of pervasive digital risk.

Programme Curriculum

Certified Information Systems Auditor Training Course

Introduction

The Certified Information Systems Auditor credential, globally recognized and awarded by ISACA, is the definitive mark of excellence for professionals who audit, control, monitor, and assess an organization's information technology and business systems. In today's landscape of escalating cyber threats, complex regulatory mandates, and accelerated Digital Transformation, the role of the CISA-certified professional has become more critical than ever. Certified Information Systems Auditor Training Course is designed to equip participants with the essential risk-based auditing skills and comprehensive knowledge across the five CISA domains. By mastering modern IT Governance, advanced security controls, Business Resilience planning, and the full System Development Life Cycle, participants will be prepared to successfully pass the CISA exam and immediately add tangible value in ensuring their enterprise's Information Assets are secure, reliable, and compliant.

This course moves beyond theoretical concepts, focusing heavily on practical application through real-world case studies and a hands-on training methodology that simulates actual audit scenarios. We emphasize understanding the convergence of IT Audit, Cybersecurity, and Enterprise Risk Management, which are top-tier organizational concerns. Successful completion empowers you to assess vulnerabilities, report on compliance assurance, and recommend robust control implementation strategies. Earning the CISA certification elevates your professional standing, demonstrating a commitment to the highest standards of digital trust and offering a competitive advantage in a high-demand global job market for IT Audit Managers and Information Security Analysts. Invest in this training to solidify your expertise and become a key assurance professional in the era of pervasive digital risk.

Course Duration

5 days

Course Objectives

1. Execute Risk-Based Audit Strategy using contemporary Data Analytics and Continuous Auditing techniques.
2. Evaluate and assure modern IT Governance Frameworks and alignment with business strategy.
3. Assess Cybersecurity posture, including advanced threats, Zero Trust principles, and security awareness programs.
4. Conduct comprehensive audits of Cloud Computing environments, focusing on IaaS, PaaS, SaaS, and Cloud Governance.
5. Validate the effectiveness of controls throughout the System Development Life Cycle and in Agile/DevOps methodologies.
6. Analyze and evaluate Business Continuity Planning and Disaster Recovery strategies for enterprise resilience.
7. Design and test robust Access Controls and Identity and Access Management solutions, including Multi-Factor Authentication.
8. Master the auditing of Information Assets Protection, covering data classification, encryption, and Data Privacy regulations
9. Review and assure IT Operations Management, including incident, problem, and Change Management processes.
10. Evaluate an organization's Enterprise Risk Management policies to identify and mitigate significant Digital Risk.
11. Apply professional IS Audit Standards and the Code of Ethics in all engagement planning and reporting.

12. Assess the security and compliance of emerging technologies like IoT, Mobile Computing, and Artificial Intelligence governance.
13. Prepare for and pass the CISA Certification Exam by mastering all five job practice domains and scenario-based questions.

Target Audience

1. IT Auditors
2. Information Security Managers/Analysts
3. Risk and Compliance Professionals
4. IT Consultants
5. Chief Information Officers and IT Directors
6. Internal Control Professionals
7. Data Privacy Officers and Compliance Auditors
8. IT Project Managers seeking a foundation in control and risk.

Course Modules

Module 1: Information System Auditing Process

- The Risk-Based Audit Approach.
- ISACA IT Audit and Assurance Standards and Code of Ethics.
- General, Application, Preventive, Detective, Corrective.
- Audit Evidence Collection and Data Analytics techniques.
- Case Study: Auditing a new Cloud Migration project scope and inherent risks.

Module 2: Governance and Management of IT

- Evaluating IT Governance Frameworks.
- Assessing IT Strategy alignment with business objectives and Enterprise Architecture.
- Reviewing IT Resource Management.
- Evaluating the Enterprise Risk Management process and risk tolerance.
- Case Study: Assuring the effectiveness of an organization's Data Governance program following a major data breach.

Module 3: IS Acquisition, Development, and Implementation

- Auditing the System Development Life Cycle and Project Management controls.
- Reviewing controls in Agile, DevOps, and rapid application development environments.
- Assessing System Testing methodologies
- Evaluating Change, Configuration, and Release Management processes.
- Case Study: Post-implementation review of an organization's new ERP System for control deficiencies.

Module 4: Information Systems Operations and Business Resilience

- Auditing IT Service Management processes.
- Evaluating System Performance and Capacity Management.
- Reviewing Business Continuity Plan and Disaster Recovery Plan testing.
- Assessing controls over Database Management and data integrity.
- Case Study: Analyzing the effectiveness of a Disaster Recovery test scenario involving a major regional power outage.

Module 5: Protection of Information Assets

- Evaluating the Information Security Program and associated frameworks
- Assessing Identity and Access Management, provisioning, and least privilege principles.
- Reviewing Network Security and Vulnerability Management.
- Auditing Cryptography, Data Encryption, and Key Management practices.
- Case Study: Evaluating security controls for Mobile Computing and Bring Your Own Device policies.

Module 6: Advanced Cloud and Cybersecurity Audit

- Deep dive into Cloud Security Controls
- Auditing the security of Virtualization and containerization technologies.
- Assessing compliance with major Data Privacy Regulations
- Reviewing Security Event Management and Incident Response procedures.
- Case Study: Conducting a compliance audit of a Third-Party Cloud Service Provider environment.

Module 7: Emerging Technologies and Regulatory Compliance

- Auditing emerging technologies like IoT and Operational Technology systems.
- Assessing controls for Artificial Intelligence and Machine Learning models.
- Reviewing adherence to financial and regulatory requirements.
- Evaluating Vendor Management and third-party risk assurance.
- Case Study: Developing an audit plan for an organization utilizing Blockchain technology for supply chain tracking.

Module 8: CISA Exam Preparation and Practice

- Review of all five CISA Domains with weighted focus.
- Test-taking strategies for Scenario-Based Questions.
- Timed Practice Exams and performance analysis.
- Discussion of complex/tricky concepts and common exam errors.
- Case Study: Mock Audit Report writing and presentation of findings to simulated management.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now