Certified in Risk and Information Systems Control Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Certified in Risk and Information Systems Control Training Course is designed to equip professionals with the cutting-edge expertise required to manage and govern enterprise IT risk and implement effective information systems controls. This program goes beyond traditional compliance by integrating advanced concepts like AI risk assessment, Zero Trust architecture, and digital transformation resilience. Participants will gain the strategic skills to identify, assess, respond to, and monitor IT risks that could significantly impact business objectives, ensuring the organization maintains a strong risk-aware culture and achieves its strategic goals in a volatile global landscape.

The certification is globally recognized, validating a professional?ÇÖs ability to bridge the gap between business strategy and IT operations by establishing a common language for risk across the enterprise. The curriculum aligns with the latest ISACA CRISC job practice areas, focusing on practical application through real-world case studies and exercises. This immersive training is essential for career acceleration, offering the validated proficiency necessary to safeguard organizational assets, manage third-party vendor risk, and ensure robust business continuity management amidst evolving cybersecurity threats and complex regulatory requirements like data privacy and GDPR/CCPA compliance.

Programme Curriculum

Certified in Risk and Information Systems Control Training Course

Introduction

Certified in Risk and Information Systems Control Training Course is designed to equip professionals with the cutting-edge expertise required to manage and govern enterprise IT risk and implement effective information systems controls. This program goes beyond traditional compliance by integrating advanced concepts like AI risk assessment, Zero Trust architecture, and digital transformation resilience. Participants will gain the strategic

skills to identify, assess, respond to, and monitor IT risks that could significantly impact business objectives, ensuring the organization maintains a strong risk-aware culture and achieves its strategic goals in a volatile global landscape.

The certification is globally recognized, validating a professional?ÇÖs ability to bridge the gap between business strategy and IT operations by establishing a common language for risk across the enterprise. The curriculum aligns with the latest ISACA CRISC job practice areas, focusing on practical application through real-world case studies and exercises. This immersive training is essential for career acceleration, offering the validated proficiency necessary to safeguard organizational assets, manage third-party vendor risk, and ensure robust business continuity management amidst evolving cybersecurity threats and complex regulatory requirements like data privacy and GDPR/CCPA compliance.

Course Duration

10 days

Course Objectives

1. Strategize and Govern Enterprise IT Risk aligned with corporate objectives.
2. Master Risk Assessment Methodologies including BIA and scenario development.
3. Implement Zero Trust and Cloud Security principles for modern IT environments.
4. Analyze and Mitigate Emerging Technology Risks, including AI Risk Assessment and Quantum Computing threats.
5. Develop robust Risk Response Plans and mitigation strategies.
6. Design and Validate Information Systems Controls for effectiveness.
7. Establish continuous Risk Monitoring and key indicator reporting.
8. Manage Third-Party and Supply Chain Risk exposure comprehensively.
9. Ensure Regulatory Compliance and adherence to Data Privacy standards
10. Foster an organization-wide Risk-Aware Culture through effective governance.
11. Implement Technology Resilience and effective Disaster Recovery/Business Continuity plans.
12. Use COBIT and ISO 31000 frameworks to enhance risk governance.
13. Report risk posture effectively to C-level executives using Risk Dashboards and scorecards.

Target Audience

1. IT Risk Managers and Analysts
2. Compliance Officers and Governance Professionals
3. Information Security Managers/Consultants
4. IT Auditors and Control Professionals
5. Chief Information Officers (CIOs) and CISOs
6. Business Analysts focused on IT projects
7. Project Managers involved in IT implementation
8. Third-Party and Vendor Risk Managers

Course Modules

Module 1: Governance, Risk, and Compliance (GRC) Foundation

- Organizational Governance.
- Enterprise Risk Management (ERM) Frameworks.
- The Three Lines of Defense Model.

- Risk Culture and Ethics.
- Regulatory Requirements.
- Case Study: Analysis of a Financial Services Firm's ERM integration with its regulatory compliance obligations

Module 2: IT Risk Identification and Scenario Development

- Threat Modeling.
- Vulnerability Management.
- Risk Events.
- Risk Scenario Development.
- Risk Register and Profile.
- Case Study: Developing worst-case "Black Swan" IT failure scenarios for a large e-commerce platform following a major security incident.

Module 3: IT Risk Analysis and Evaluation

- Risk Assessment Methodologies.
- Business Impact Analysis.
- Likelihood and Impact Assessment.
- Inherent vs. Residual Risk.
- Risk Appetite and Tolerance.
- Case Study: Using a quantitative approach to justify a security investment for a data center.

Module 4: Risk Response and Treatment Options

- Risk Treatment Options.
- Risk and Control Ownership.
- Risk Treatment Plan Development.
- Cost-Benefit Analysis.
- Issue and Exception Management.
- Case Study: Evaluating the "Transfer" option through cyber insurance and contractual liability for a new cloud service provider.

Module 5: Control Design and Implementation

- Control Types and Classifications
- Control Frameworks.
- Control Design Principles.
- System Development Life Cycle (SDLC) Controls
- Control Implementation and Documentation.
- Case Study: Designing a set of logical access controls and security policies for a newly deployed Enterprise Resource Planning (ERP) system.

Module 6: Risk Monitoring and Reporting

- Key Risk Indicators.
- Key Control Indicators.
- Risk and Control Dashboards.
- Data Aggregation and Validation.
- Continuous Risk Monitoring.

- Case Study: Developing a KRI/KCI scorecard for a managed security service provider (MSSP) to proactively identify service degradation or potential breaches.

Module 7: Information Technology Principles

- Enterprise Architecture (EA) Risk.
- IT Operations Management Risk.
- Emerging Technologies Risk.
- Data Lifecycle Management
- Project Management Risk: Integrating risk activities into the IT project life cycle.
- Case Study: Reviewing the security and operational risks introduced by adopting a new global cloud-based Human Resources Information System.

Module 8: Information Security and Control Frameworks

- Information Security Concepts.
- Security Frameworks and Standards.
- Security Architecture.
- Information Security Awareness.
- Data Privacy and Protection
- Case Study: Mapping an organization's current security controls to the NIST Cybersecurity Framework to identify major gaps in risk coverage.

Module 9: Third-Party and Vendor Risk Management (TPRM)

- **Vendor Due Diligence:** Assessing a third party's security posture before contracting.
- **Contractual Requirements:** Defining risk-specific clauses in Service Level Agreements (SLAs) and contracts.
- **Ongoing Monitoring:** Establishing continuous oversight of third-party compliance and control performance.
- **Supply Chain Risk:** Managing interconnected risk across the entire digital supply chain ecosystem.
- **Exit Strategy and Off-boarding:** Planning for risk mitigation upon termination of a vendor relationship.
- **Case Study:** Developing a risk-based due diligence checklist for selecting a new mission-critical Software-as-a-Service (SaaS) provider.

Module 10: Cyber Risk and Resilience Strategies

- Threat Intelligence Integration.
- Advanced Persistent Threats.
- Zero Trust Architecture.
- Cloud Security Risk.
- Cyber Resilience Planning.
- Case Study: Implementing a Zero Trust strategy across a remote workforce to mitigate risks associated with unmanaged endpoints.

Module 11: Business Continuity and Disaster Recovery

- Business Continuity Management.
- Disaster Recovery (DR) Planning.
- Recovery Objectives
- Testing and Exercises.

- Organizational Resilience.
- Case Study: Critiquing the BCM/DR plan of an organization following a simulated regional power grid failure.

Module 12: Managing Emerging and AI-Related Risk

- Artificial Intelligence (AI) Risk.
- Data Governance for AI.
- Quantum Computing Threats.
- Non-Traditional IT Risk
- Risk Management of Digital Transformation.
- Case Study: Developing a pre-deployment AI risk checklist to address data bias and decision-making transparency in a credit scoring application.

Module 13: Risk Assurance and Control Effectiveness

- Control Testing Methodologies.
- Maturity Models.
- Self-Assessment Techniques.
- Audit Integration.
- Post-Implementation Review.
- Case Study: Conducting an RCSA workshop for the human resources team to assess controls around employee data access and onboarding/off-boarding.

Module 14: Risk Reporting and Stakeholder Communication

- Executive Reporting
- Key Performance Indicators.
- Communicating Emerging Risks.
- Heatmaps and Risk Matrices.
- Risk Aggregation and Interdependencies.
- Case Study: Creating a three-slide executive summary deck to present the top five organizational IT risks and the associated mitigation costs/progress.

Module 15: CRISC Exam Preparation and Application

- CRISC Domain Deep Dive.
- Exam Strategies.
- Time Management.
- Mock Exam and Debrief.
- Certification Application Process
- Case Study: Reviewing complex, multi-layered CRISC-style scenarios to practice selecting the most appropriate next action for a risk manager.

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
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

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

Register Online Now

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