Risk Management and Cyber Risk Assessment Essentials 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

In today's hyper-connected and rapidly evolving digital landscape, effective Cyber Risk Management is not just an IT concern, but a critical Business Resilience imperative. Organizations face an increasing volume and sophistication of threats, from AI-Powered Cyber-Attacks and Ransomware to complex supply chain vulnerabilities, making a robust defense mechanism essential for Strategic Decision-Making. Risk Management and Cyber Risk Assessment Essentials Training Course provides professionals with the Essential Frameworks and Practical Methodologies needed to systematically identify, assess, quantify, and mitigate cyber threats. Participants will master industry-leading standards like NIST RMF and ISO 27005, transforming their approach from reactive security to Proactive Risk Posture and building a culture of Organizational Cyber Resilience.

This intensive program focuses on integrating technical risk analysis with Enterprise Risk Management (ERM), ensuring that security investments align directly with strategic business objectives and regulatory compliance, including frameworks like GDPR and HIPAA. Through real-world Case Studies and hands-on exercises, attendees will gain the skills to perform Quantitative and Qualitative Risk Assessments, effectively communicate risk to executive leadership, and implement Defense-in-Depth strategies. By the end of this course, you will be equipped to establish a defensible, continuous Risk Governance program that secures your organization's most valuable assets in the face of the dynamic Threat Landscape of 2025 and beyond.

Programme Curriculum

Risk Management and Cyber Risk Assessment Essentials Training Course

Introduction

In today's hyper-connected and rapidly evolving digital landscape, effective Cyber Risk Management is not just an IT concern, but a critical Business Resilience imperative. Organizations face an increasing volume and sophistication of threats, from AI-Powered Cyber-Attacks and Ransomware to complex supply chain vulnerabilities, making a robust defense mechanism essential for Strategic Decision-Making. Risk Management and Cyber Risk Assessment Essentials Training Course provides professionals with the Essential Frameworks and Practical Methodologies needed to systematically identify, assess, quantify, and mitigate cyber threats. Participants will master industry-leading standards like NIST RMF and ISO 27005, transforming their approach from reactive security to Proactive Risk Posture and building a culture of Organizational Cyber Resilience.

This intensive program focuses on integrating technical risk analysis with Enterprise Risk Management (ERM), ensuring that security investments align directly with strategic business objectives and regulatory compliance, including frameworks like GDPR and HIPAA. Through real-world Case Studies and hands-on exercises, attendees will gain the skills to perform Quantitative and Qualitative Risk Assessments, effectively communicate risk to executive leadership, and implement Defense-in-Depth strategies. By the end of this course, you will be equipped to establish a defensible, continuous Risk Governance program that secures your organization's most valuable assets in the face of the dynamic Threat Landscape of 2025 and beyond.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Master the fundamental principles and Cyber Risk Lifecycle.
2. Apply current industry frameworks, including NIST RMF and ISO 27005.
3. Conduct comprehensive Quantitative and Qualitative Risk Assessments.
4. Identify and analyze the latest Emerging Cyber Threats like AI-driven attacks and deepfakes.
5. Develop robust Risk Mitigation Strategies and implement effective security controls.
6. Assess and manage Third-Party and Supply Chain Cyber Risks.
7. Translate technical vulnerabilities into actionable Business Impact and financial terms
8. Design and implement a continuous Risk Monitoring and reporting program.
9. Align cyber risk strategy with overall Enterprise Risk Management
10. Navigate key Regulatory Compliance requirements
11. Communicate complex cyber risks effectively to Executive Stakeholders and the Board.
12. Strengthen Incident Response and Business Continuity Planning capabilities.
13. Foster an organization-wide Cyber Security Awareness and Risk-Aware Culture.

Target Audience

1. Risk Managers and Enterprise Risk Professionals.
2. Information Security Managers and CISOs
3. IT Directors and IT Governance Professionals.
4. Compliance and Audit Officers
5. Security Analysts and Consultants.
6. Business Continuity and Disaster Recovery Planners.
7. Financial and Operational Risk Leaders.
8. System Owners and Technical Security Architects.

Course Modules

Module 1: Foundational Principles of Cyber Risk Management

- The Evolving Threat Landscape
- Risk Governance and Culture.
- Key Risk Frameworks.
- Asset and Threat Modeling.
- Case Study: Analysis of a major Supply Chain Cyber-Attack to illustrate cascading risk and the failure of siloed risk management.

Module 2: Qualitative Cyber Risk Assessment

- Risk Identification Techniques.
- Likelihood and Impact Analysis
- Building the Risk Register.
- Vulnerability Assessment Essentials.
- Case Study: Simulating a Phishing/Social Engineering campaign and using the results to conduct an initial qualitative risk assessment on human factors.

Module 3: Quantitative Cyber Risk Assessment

- Introduction to Risk Quantification.
- Factor Analysis of Information Risk
- Data Gathering and Calibration.
- Translating Risk to Business Language.
- Case Study: Applying the FAIR Methodology to calculate the projected financial impact of a successful Ransomware attack on a critical business system.

Module 4: Risk Treatment and Mitigation Strategies

- The Four Risk Responses
- Selecting and Implementing Controls.
- Defense-in-Depth and ZTA.
- Managing Emerging Technology Risks.
- Case Study: Developing a Risk Treatment Plan for high-priority risks identified in a cloud migration project, including cost-benefit analysis of specific security controls.

Module 5: Third-Party and Supply Chain Risk Management (TPRM)

- Understanding TPRM Complexity.
- TPRM Lifecycle.
- Security Questionnaires and Audit.
- Contractual Risk Transfer.
- Case Study: Evaluating the security risks posed by a key Software-as-a-Service provider and drafting a Mitigation Plan based on contractual terms.

Module 6: Regulatory Compliance and Cyber Risk

- Key Global Regulations.
- Compliance as a Risk Driver.
- Internal and External Audits.
- Data Protection Impact Assessments.

- Case Study: Reviewing an organization?ÇÖs response to a GDPR violation scenario, focusing on the steps taken to assess the risk, report the breach, and implement corrective controls.

Module 7: Incident Response and Business Continuity

- The Incident Response Lifecycle.
- Developing BCP and DRP.
- Crisis Communication.
- Digital Forensics and Evidence.
- Case Study: A tabletop exercise simulating a major Data Breach requiring participants to manage the immediate incident response and BCP activation.

Module 8: Continuous Risk Monitoring and Reporting

- Key Risk Indicators (KRIs) and Metrics.
- Risk Reporting for Stakeholders.
- Integrating Risk Monitoring.
- Continuous Improvemen.
- Case Study: Critiquing a sample Executive Risk Report and Dashboard, redesigning the metrics to be more aligned with Strategic Business Objectives and Risk Appetite.

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

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