

Course No. 1944

Advanced Cybersecurity Risk Management Training Course

CYBERSECURITY & INFORMATION SECURITY
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION

5 Days

DELIVERY

Classroom



Course Overview

The Advanced Cybersecurity Risk Management Training Course provides an advanced, strategic, and practical approach to managing cybersecurity risks across complex organizational environments. The course moves beyond basic risk identification to focus on risk quantification, strategic prioritization, governance, resilience, decision-making, and the integration of cybersecurity risk with enterprise risk management.

Participants will examine how organizations can identify evolving cyber risks, assess their potential business impact, determine risk appetite and tolerance, and make informed decisions about risk treatment and cybersecurity investments. The program addresses technical, operational, financial, regulatory, third-party, cloud, data, and emerging cybersecurity risks.

The course emphasizes the connection between cybersecurity risk and executive decision-making. Participants will learn how to translate technical vulnerabilities and threat intelligence into business risk scenarios, quantify potential losses where appropriate, establish meaningful risk indicators, and communicate cybersecurity exposure to senior management and boards.

Through advanced risk scenarios, quantitative analysis exercises, risk workshops, cyber-risk simulations, investment prioritization activities, and strategic planning, participants will develop the capabilities required to build mature cybersecurity risk management programs and strengthen organizational resilience against evolving cyber threats.

Objectives

- By the end of the course, participants will be able to:
- Analyze advanced cybersecurity risk concepts and their impact on organizational strategy.
- Assess complex cyber risks across technology, operations, finance, compliance, and third-party environments.
- Develop advanced cybersecurity risk assessment and quantification methodologies.
- Evaluate cyber risk using likelihood, impact, exposure, and loss scenarios.
- Establish cybersecurity risk appetite, tolerance, and escalation thresholds.
- Prioritize cybersecurity risks based on business criticality and potential impact.

- Develop advanced risk treatment and mitigation strategies.
- Evaluate cybersecurity investments using risk-based decision-making principles.
- Integrate cybersecurity risk with enterprise risk management.
- Establish meaningful cybersecurity risk indicators and executive dashboards.
- Assess emerging, systemic, and interconnected cybersecurity risks.
- Strengthen third-party, supply-chain, cloud, and technology risk management.
- Develop cyber resilience strategies aligned with critical business services.
- Improve executive and board-level cybersecurity risk reporting.
- Establish a mature cybersecurity risk management operating model and improvement roadmap.

Who Should Attend

This course is designed for cybersecurity and information security managers, cybersecurity risk professionals, enterprise risk managers, security architects, governance and compliance specialists, security operations leaders, technology risk professionals, and senior IT managers.

It is also suitable for internal auditors, business continuity and resilience professionals, cloud security managers, third-party risk specialists, technology assurance professionals, and executives involved in cybersecurity governance, risk oversight, investment decisions, and organizational resilience.

The course is particularly relevant for organizations seeking to move from traditional cybersecurity risk assessment toward a mature, business-aligned risk management approach capable of supporting strategic decisions, investment prioritization, regulatory expectations, and resilience planning.

Learning Outcomes

- By the end of the course, participants will be able to:
- Evaluate complex cybersecurity risks within an enterprise risk context.
- Develop advanced cybersecurity risk assessment methodologies.
- Analyze cyber risk scenarios and potential business consequences.
- Apply quantitative and qualitative approaches to cyber risk analysis.

- Estimate potential financial and operational exposure from major cyber risks.
- Establish cybersecurity risk appetite and tolerance frameworks.
- Prioritize risks using business criticality, exposure, likelihood, and impact.
- Develop risk treatment strategies for high-priority cyber risks.
- Evaluate the effectiveness of cybersecurity controls and residual risk.
- Integrate threat intelligence into cybersecurity risk decisions.
- Assess third-party, supply-chain, cloud, and emerging cyber risks.
- Develop cybersecurity key risk indicators and executive reporting.
- Align cybersecurity investments with organizational risk priorities.
- Strengthen cyber resilience and critical-service protection.
- Support executive and board-level cybersecurity risk decisions.
- Develop a mature cybersecurity risk management transformation roadmap.

Course Outline

DAY 01

Advanced Cybersecurity Risk Management Strategy and Governance

- Evolution of cybersecurity risk management.
- Cybersecurity risk as an enterprise business risk.
- Strategic, operational, financial, regulatory, and reputational cyber risks.
- Cybersecurity risk governance structures.
- Roles and responsibilities of executives, risk owners, and security teams.
- Cybersecurity risk appetite and tolerance.
- Risk ownership and accountability.
- Risk escalation and decision-making mechanisms.
- Integrating cybersecurity with enterprise risk management.
- Cybersecurity risk maturity models.
- Building a business-aligned cybersecurity risk management program.

DAY 01 — CONTINUED

PRACTICAL APPLICATION

Assess the maturity of a representative organization's cybersecurity risk management program and develop a strategic improvement plan.

DAY 02**Advanced Cybersecurity Risk Assessment and Quantification**

- Advanced cybersecurity risk assessment methodologies.
- Asset criticality and business impact analysis.
- Threat, vulnerability, exposure, and consequence analysis.
- Developing sophisticated cybersecurity risk scenarios.
- Qualitative and quantitative risk assessment approaches.
- Probability and impact modeling.
- Estimating financial and operational losses.
- Scenario-based cyber risk quantification.
- Residual risk analysis.
- Risk aggregation and interconnected risks.
- Cyber risk scoring and prioritization models.
- Building advanced cybersecurity risk registers.

PRACTICAL APPLICATION

Develop and quantify a set of cyber risk scenarios and create a prioritized enterprise cybersecurity risk register.

DAY 03**Threat Intelligence, Emerging Risks, and Advanced Risk Analysis**

- Integrating threat intelligence into risk management.
- Threat actor capabilities, motivations, and targeting.
- Advanced persistent and targeted threats.

DAY 03 — CONTINUED

- Identity-based and privilege-related risks.
- Cloud and digital transformation risks.
- Application and data security risks.
- Third-party and supply-chain cyber risks.
- Artificial intelligence-related cybersecurity risks.
- Emerging technologies and new attack surfaces.
- Systemic and interconnected cybersecurity risks.
- Scenario analysis and cyber risk forecasting.
- Identifying changes in organizational cyber exposure.

PRACTICAL APPLICATION

Analyze an advanced cyber threat scenario using threat intelligence and determine its potential impact on critical business services and organizational risk exposure.

DAY 04

Cyber Risk Treatment, Investment, and Organizational Resilience

- Advanced cybersecurity risk treatment strategies.
- Risk avoidance, reduction, transfer, and acceptance.
- Selecting controls based on risk and business value.
- Evaluating cybersecurity control effectiveness.
- Managing residual cybersecurity risk.
- Cybersecurity investment prioritization.
- Cost-benefit considerations for cybersecurity controls.
- Risk-based security architecture decisions.
- Cyber resilience and protection of critical business services.
- Incident response and recovery risk considerations.
- Business continuity and disaster recovery integration.
- Developing cybersecurity risk mitigation portfolios.

DAY 04 — CONTINUED

PRACTICAL APPLICATION

Prioritize a cybersecurity investment portfolio based on risk exposure, business impact, control effectiveness, and available resources.

DAY 05

Executive Cybersecurity Risk Reporting, Measurement, and Transformation

- Cybersecurity risk reporting for senior management and boards.
- Translating technical security findings into business risk language.
- Cybersecurity key risk indicators and performance measures.
- Executive dashboards and risk visualization.
- Risk trends, thresholds, and early-warning indicators.
- Monitoring changes in cyber risk exposure.
- Cybersecurity risk assurance and audit readiness.
- Integrating cyber risk into enterprise governance.
- Measuring cybersecurity risk management maturity.
- Building a target operating model.
- Continuous improvement and strategic risk management.
- Developing a cybersecurity risk transformation roadmap.

FINAL WORKSHOP

Develop an Advanced Cybersecurity Risk Management Framework covering governance, risk appetite, risk assessment, quantification, threat intelligence, emerging risks, risk treatment, investment prioritization, resilience, executive reporting, measurement, maturity, and a strategic implementation roadmap.



Register or Request More Information

Course page: <https://quest-training.com/courses/advanced-cybersecurity-risk-management-training-course>

Website: <https://quest-training.com>

Email: info@quest-training.com

Phone: +905016771440

