QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1926

Cyber Insurance Fundamentals & Risk Management Training Course

CYBER INSURANCE
INSURANCE & RISK MANAGEMENT

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Cyber Insurance Fundamentals & Risk Management Training Course provides a comprehensive foundation for understanding cyber insurance, cyber exposures, and the principles of managing cyber risks from an insurance and enterprise risk perspective. The course is designed to help insurance professionals, risk managers, and business leaders understand how cyber threats translate into financial, operational, regulatory, and reputational exposures.

Participants will explore the cyber risk landscape, including ransomware, data breaches, privacy incidents, business interruption, technology failures, social engineering, cloud dependencies, supply-chain vulnerabilities, and third-party cyber risks. The course establishes a clear connection between these threats and the insurance mechanisms used to identify, assess, transfer, and manage cyber exposures.

The program covers the fundamentals of cyber insurance products, key coverage components, policy structures, underwriting considerations, exclusions, limits, deductibles, claims processes, and risk transfer strategies. Participants will also examine the relationship between cybersecurity controls, organizational risk maturity, insurance eligibility, pricing considerations, and policy conditions.

In addition, the course addresses cyber risk governance, risk assessment, incident preparedness, business continuity, resilience, third-party risk, regulatory considerations, and emerging cyber threats. Through practical case studies, risk assessment exercises, and insurance scenarios, participants will develop a strong foundation for managing cyber risk and making informed decisions regarding cyber insurance and risk transfer.

Objectives

- By the end of the course, participants will be able to:
- Explain the fundamentals and strategic role of cyber insurance.
- Analyze the evolving cyber risk landscape and its impact on organizations.
- Identify major cyber exposures that can create insurable financial losses.
- Assess ransomware, data breach, business interruption, and technology risks.
- Evaluate the relationship between cybersecurity controls and cyber insurance.

- Understand key cyber insurance coverage structures and policy components.
- Assess limits, deductibles, exclusions, sublimits, and policy conditions.
- Apply structured approaches to cyber risk assessment and management.
- Evaluate third-party, supply-chain, cloud, and technology dependency risks.
- Develop appropriate cyber risk mitigation and risk transfer strategies.
- Understand the role of underwriting, pricing, claims, and reinsurance in cyber insurance.
- Assess cyber risk governance and organizational responsibilities.
- Apply scenario analysis to significant cyber events.
- Strengthen cyber incident preparedness and business continuity planning.
- Develop an integrated framework for cyber insurance and risk management.

Who Should Attend

This course is designed for insurance executives, underwriting professionals, claims managers, risk managers, cyber insurance specialists, and professionals responsible for assessing or managing cyber risks. It is particularly suitable for professionals who require a strong understanding of cyber insurance without necessarily having a technical cybersecurity background.

The program is also relevant to enterprise risk professionals, compliance and governance specialists, internal auditors, information security and technology risk professionals, business continuity managers, insurance brokers, reinsurance specialists, actuaries, legal professionals, and professionals involved in corporate insurance programs.

The course is especially valuable for organizations seeking to strengthen cyber risk awareness, improve insurance readiness, understand cyber risk transfer, enhance resilience, and establish stronger coordination between cybersecurity, risk management, insurance, and business functions.

Learning Outcomes

- By the end of the course, participants will be able to:
- Explain core concepts and principles of cyber insurance.
- Identify major cyber threats and their potential business impacts.
- Assess key cyber exposures from an insurance perspective.

- Distinguish between different types of cyber insurance coverage.
- Evaluate policy limits, deductibles, exclusions, and coverage conditions.
- Assess the role of cybersecurity controls in cyber insurance decisions.
- Identify critical information required for cyber risk assessment.
- Evaluate organizational cyber risk maturity.
- Analyze third-party, cloud, and supply-chain cyber exposures.
- Develop practical cyber risk mitigation strategies.
- Assess appropriate approaches to cyber risk transfer.
- Understand the interaction between underwriting, claims, pricing, and reinsurance.
- Apply scenario analysis to potential cyber incidents.
- Strengthen cyber incident preparedness and business continuity arrangements.
- Support management decisions regarding cyber insurance and risk appetite.
- Develop a practical framework for integrating cyber insurance into enterprise risk management.

Course Outline

DAY 01

Cyber Risk Landscape and Foundations of Cyber Insurance

- Fundamentals of cyber risk and cyber insurance.
- Evolution of cyber threats and emerging risk patterns.
- Ransomware, malware, phishing, and social engineering.
- Data breaches and privacy-related exposures.
- Business interruption and technology failure risks.
- Cloud computing and digital dependency risks.
- Third-party and supply-chain cyber exposures.
- Financial, operational, regulatory, and reputational consequences.
- The role of cyber insurance within enterprise risk management.
- Key stakeholders in cyber risk and insurance management.

DAY 01 — CONTINUED

> **PRACTICAL APPLICATION**
> Analyze a series of cyber incidents and identify their potential financial and insurance implications.

DAY 02

Cyber Risk Assessment and Risk Management

- Principles of cyber risk identification and assessment.
- Identifying critical assets, systems, processes, and dependencies.
- Threat and vulnerability analysis.
- Assessing cybersecurity controls and organizational maturity.
- Risk likelihood, impact, and exposure assessment.
- Cyber risk classification and prioritization.
- Risk appetite and cyber risk tolerance.
- Risk mitigation and control improvement.
- Incident preparedness and response capabilities.
- Business continuity and cyber resilience.

> **PRACTICAL APPLICATION**
> Conduct a structured cyber risk assessment for a simulated organization and develop a prioritized risk treatment plan.

DAY 03

Cyber Insurance Products, Coverage and Policy Structures

- Overview of cyber insurance products and market structures.
- First-party and third-party cyber coverage.
- Data breach and privacy incident coverage.
- Cyber business interruption coverage.
- Cyber extortion and ransomware coverage.
- Data restoration and incident response expenses.

DAY 03 — CONTINUED

- Network security and technology liability.
- Policy limits, deductibles, and sublimits.
- Exclusions, conditions, warranties, and risk requirements.
- Understanding coverage triggers and policy response.
- Relationship between cyber risk controls and insurance conditions.

PRACTICAL APPLICATION

Review a simulated cyber insurance policy and identify key coverage areas, limitations, exclusions, and risk requirements.

DAY 04

Cyber Risk Transfer, Underwriting, Claims and Emerging Risks

- Principles of cyber risk transfer.
- Cyber insurance underwriting fundamentals.
- Information requirements for cyber risk assessment.
- Cyber risk selection and classification.
- Pricing considerations and relationship to risk quality.
- Cyber claims lifecycle and claims management.
- Incident investigation and loss assessment.
- Fraud, misrepresentation, and claims risk.
- Reinsurance and portfolio risk considerations.
- Systemic cyber events and accumulation risk.
- Emerging cyber risks and their insurance implications.

PRACTICAL APPLICATION

Evaluate a simulated cyber risk from underwriting through claims and determine appropriate risk transfer and management actions.

DAY 05

Cyber Insurance Governance, Resilience and Strategic Implementation

- Cyber insurance governance and organizational responsibilities.
- Integrating cyber insurance with enterprise risk management.
- Cyber risk appetite and insurance strategy.
- Developing cyber insurance readiness frameworks.
- Incident response coordination between insurance and cybersecurity teams.
- Business continuity and resilience considerations.
- Third-party and supply-chain risk management.
- Monitoring changes in cyber exposure.
- Management reporting and cyber risk indicators.
- Reviewing insurance adequacy and coverage requirements.
- Building a sustainable cyber risk management and insurance strategy.

> **FINAL WORKSHOP**
> Develop an integrated cyber insurance and risk management framework covering cyber exposure identification, risk assessment, cybersecurity controls, insurance coverage, risk transfer, incident response, business continuity, governance, and strategic implementation.

Register or Request More Information

Course page: https://quest-training.com/courses/cyber-insurance-fundamentals-risk-management-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440