Quest Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1922

Cyber Insurance Underwriting Training Course

CYBER INSURANCE
INSURANCE & RISK MANAGEMENT

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Cyber Insurance Underwriting Training Course provides a comprehensive and practical framework for assessing, pricing, and managing cyber insurance risks. The course is designed to help insurance professionals understand the unique characteristics of cyber exposures and develop disciplined underwriting approaches that balance risk selection, policy design, pricing, capacity, and portfolio profitability.

Participants will examine the evolving cyber threat landscape and its impact on organizations, including ransomware, data breaches, business interruption, technology failures, social engineering, supply-chain incidents, cloud dependencies, and third-party cyber events. The course connects these exposures to the underwriting process, enabling participants to evaluate cyber risk from both technical and insurance perspectives.

The program explores cyber risk assessment, underwriting information requirements, security controls, risk classification, exposure analysis, aggregation risk, policy wording, coverage structures, exclusions, limits, deductibles, and risk selection. Particular attention is given to the challenges of underwriting risks where historical loss data may be limited and the threat environment changes rapidly.

Participants will also learn how to apply analytical approaches to cyber insurance pricing, portfolio management, risk accumulation, scenario analysis, and underwriting decision-making. Through practical case studies, underwriting exercises, risk assessment scenarios, and simulated decision-making, the course enables participants to strengthen cyber underwriting capabilities and develop more consistent and risk-sensitive underwriting practices.

Objectives

- By the end of the course, participants will be able to:
- Analyze the evolving cyber threat landscape and its implications for insurance underwriting.
- Identify key cyber exposures affecting different types of organizations and industries.
- Assess an applicant’s cyber risk profile using structured underwriting information.
- Evaluate cybersecurity controls and their relevance to insurance risk selection.
- Apply risk classification techniques to cyber insurance underwriting.

- Assess potential cyber losses arising from data breaches, ransomware, and business interruption.
- Evaluate third-party, supply-chain, cloud, and technology-related cyber exposures.
- Develop appropriate underwriting questions and information requirements for cyber risks.
- Assess coverage needs, policy limits, deductibles, exclusions, and sublimits.
- Apply risk-based approaches to cyber insurance pricing and terms.
- Evaluate aggregation and accumulation risks within cyber insurance portfolios.
- Apply scenario analysis and stress testing to significant cyber events.
- Strengthen underwriting decisions through data, analytics, and risk indicators.
- Identify underwriting red flags and circumstances requiring enhanced risk assessment.
- Develop practical strategies for improving cyber portfolio quality and profitability.

Who Should Attend

This course is designed for insurance executives, underwriting managers, senior underwriters, risk professionals, and specialists responsible for evaluating and managing cyber insurance risks. It is particularly relevant to professionals working in commercial insurance, specialty insurance, corporate underwriting, risk assessment, insurance product development, and portfolio management.

The program is also suitable for claims professionals, brokers, insurance risk managers, compliance and governance professionals, actuarial and pricing teams, reinsurance specialists, and professionals involved in cyber risk assessment and insurance product strategy.

It is especially valuable for professionals who need to understand the relationship between cybersecurity controls, organizational risk exposure, insurance coverage, pricing, policy conditions, portfolio accumulation, and overall cyber insurance profitability.

Learning Outcomes

- By the end of the course, participants will be able to:
- Explain the fundamental principles of cyber insurance underwriting.
- Interpret major cyber threats and their potential insurance implications.

- Identify critical cyber exposures during the underwriting process.
- Evaluate an organization's cybersecurity maturity from an underwriting perspective.
- Assess applicant information and identify missing or inconsistent risk data.
- Develop structured cyber risk profiles for insurance applicants.
- Evaluate ransomware, data breach, business interruption, and technology failure exposures.
- Assess third-party and supply-chain cyber dependencies.
- Evaluate cloud and outsourced technology risks.
- Identify underwriting red flags and high-risk characteristics.
- Structure appropriate coverage terms, limits, deductibles, and exclusions.
- Apply risk-sensitive approaches to pricing and underwriting decisions.
- Evaluate cyber accumulation and systemic risk exposures.
- Use scenario analysis to assess potential large-loss events.
- Integrate analytics and risk indicators into underwriting decisions.
- Develop an improved cyber insurance underwriting framework for organizational implementation.

Course Outline

DAY 01

Cyber Risk Landscape and Foundations of Cyber Insurance Underwriting

- Fundamentals of cyber insurance and the role of cyber underwriting.
- Evolution of cyber threats and their impact on insured organizations.
- Ransomware, malware, phishing, social engineering, and cyber extortion.
- Data breaches, privacy incidents, and information security exposures.
- Business interruption and technology-dependent operational risks.
- Cloud computing, digital platforms, and technology concentration risks.
- Third-party and supply-chain cyber exposures.
- Cyber risk characteristics across different industries and business models.
- Challenges associated with rapidly changing cyber threats and limited historical loss data.

DAY 01 — CONTINUED

> **PRACTICAL APPLICATION**
> Analyze a range of cyber incidents and identify their potential insurance exposures and underwriting implications.

DAY 02

Cyber Risk Assessment and Underwriting Information

- Principles of cyber risk assessment for insurance underwriting.
- Understanding the cyber underwriting submission.
- Essential information and data requirements for cyber risk evaluation.
- Assessing organizational structure, technology dependencies, and critical systems.
- Evaluating cybersecurity governance and risk management practices.
- Security controls, access management, authentication, backup, and recovery capabilities.
- Vulnerability management and incident detection capabilities.
- Assessing business continuity and cyber incident response preparedness.
- Identifying underwriting red flags and information gaps.
- Developing a structured cyber risk classification framework.

> **PRACTICAL APPLICATION**
> Complete a cyber underwriting assessment using a simulated insurance submission and identify key risk factors and information gaps.

DAY 03

Cyber Coverage, Policy Structure and Risk Selection

- Cyber insurance coverage structures and key coverage components.
- First-party and third-party cyber exposures.
- Data breach response and privacy-related costs.
- Cyber business interruption and dependent business interruption.
- Cyber extortion and ransomware-related exposures.
- Network security and technology liability.

DAY 03 — CONTINUED

- Media liability and digital content exposures.
- Policy limits, deductibles, sublimits, waiting periods, and coverage conditions.
- Exclusions and major underwriting considerations.
- Risk selection and referral criteria for complex cyber risks.

PRACTICAL APPLICATION

Review a simulated cyber insurance risk and design appropriate coverage terms based on the organization's exposure profile.

DAY 04

Cyber Insurance Pricing, Aggregation and Portfolio Risk

- Principles of cyber insurance pricing.
- Risk-based pricing approaches and underwriting factors.
- Exposure-based and analytics-supported pricing considerations.
- Loss frequency and severity in cyber insurance.
- Scenario-based loss estimation.
- Cyber accumulation and aggregation risk.
- Systemic cyber events and correlated losses.
- Cloud service providers and technology concentration risk.
- Stress testing and scenario analysis for large cyber events.
- Portfolio-level underwriting strategy and risk appetite.
- Balancing growth, capacity, risk quality, and profitability.

PRACTICAL APPLICATION

Conduct a cyber loss scenario and assess its potential impact on individual risks and the wider insurance portfolio.

DAY 05

Advanced Cyber Underwriting, Governance and Strategic Implementation

- Advanced cyber underwriting decision-making.
- Integrating cybersecurity maturity into underwriting decisions.
- Using data, analytics, and risk indicators to strengthen underwriting.
- Monitoring changes in insured cyber risk throughout the policy lifecycle.
- Cyber risk appetite and underwriting authority.
- Referral and escalation frameworks for complex or high-risk accounts.
- Underwriting governance, documentation, and quality assurance.
- Managing portfolio concentrations and accumulation exposures.
- Collaboration between underwriting, claims, risk, actuarial, reinsurance, and cybersecurity functions.
- Developing underwriting performance indicators.
- Continuous improvement of cyber underwriting frameworks and practices.

> **FINAL WORKSHOP**
>
> Develop an integrated cyber insurance underwriting framework covering risk assessment, information requirements, risk classification, coverage structure, pricing considerations, accumulation risk, referral criteria, governance, and portfolio management.

Register or Request More Information

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