QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1921

Cyber Risk Assessment for Insurance Professionals Training Course

CYBER INSURANCE
INSURANCE & RISK MANAGEMENT

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Cyber Risk Assessment for Insurance Professionals Training Course provides a practical and strategic framework for identifying, assessing, evaluating, and managing cyber risks within insurance organizations. The course focuses on understanding how cyber threats can affect insurance operations, customer information, underwriting activities, claims processes, digital services, third-party relationships, and overall business resilience.

Participants will explore the insurance cyber risk landscape, including cyber threats, vulnerabilities, attack scenarios, data exposure, technology dependencies, operational disruption, third-party risks, and emerging digital risks. The course emphasizes the ability to assess cyber risk from both technical and business perspectives without requiring participants to become cybersecurity specialists.

The program also examines cyber risk assessment methodologies, risk identification, risk scoring, likelihood and impact analysis, risk scenarios, control effectiveness, residual risk, risk appetite, and treatment strategies. Participants will learn how to translate cybersecurity findings into business-oriented risk information that can support management decisions, underwriting considerations, governance, and resource allocation.

Particular attention is given to cyber insurance implications, regulatory expectations, data privacy, incident response, business continuity, third-party risk, and cyber resilience. Through practical exercises, insurance case studies, risk assessment workshops, and scenario analysis, participants will develop the skills required to establish and maintain a structured cyber risk assessment approach within an insurance environment.

Objectives

- By the end of this course, participants will be able to:
- Analyze the cyber risk landscape affecting insurance organizations.
- Identify key cyber threats, vulnerabilities, assets, and business dependencies.
- Assess cyber risks across insurance operations, digital services, and customer processes.
- Apply structured methodologies for identifying and evaluating cyber risk.
- Analyze cyber risk likelihood, impact, exposure, and potential business consequences.

- Develop and assess cyber risk scenarios relevant to insurance organizations.
- Evaluate the effectiveness of cybersecurity controls and identify control gaps.
- Calculate and interpret inherent and residual cyber risk.
- Develop cyber risk ratings and prioritization criteria.
- Align cyber risk assessments with organizational risk appetite and governance frameworks.
- Evaluate third-party and technology-related cyber risks.
- Assess cyber risks associated with customer data and digital insurance services.
- Develop appropriate cyber risk treatment and mitigation strategies.
- Integrate cyber risk information into enterprise risk management and decision-making.
- Develop a practical cyber risk assessment framework for an insurance organization.

Who Should Attend

This course is designed for insurance executives, senior managers, risk professionals, compliance officers, governance specialists, and decision makers responsible for managing operational, technology, information, and emerging risks. It is particularly relevant to professionals working in enterprise risk management, information security, cybersecurity, compliance, internal audit, technology, digital transformation, operations, claims, underwriting, and customer services.

The program is also suitable for insurance professionals involved in cyber insurance, risk assessment, third-party risk management, business continuity, data protection, technology governance, and regulatory risk who need a stronger understanding of cyber risk from a business and insurance perspective.

The course is especially valuable for insurance organizations seeking to strengthen cyber resilience, improve risk visibility, protect sensitive customer information, enhance technology risk governance, and make better-informed decisions regarding cyber risk exposure and mitigation.

Learning Outcomes

- Upon successful completion of the course, participants will be able to:
- Establish a structured approach to cyber risk assessment within an insurance organization.
- Identify critical information assets, systems, processes, and business dependencies.

- Identify relevant cyber threats and vulnerabilities affecting insurance operations.
- Develop realistic cyber risk scenarios and assess their potential consequences.
- Evaluate cyber risk based on likelihood, impact, exposure, and control effectiveness.
- Distinguish between inherent, controlled, and residual cyber risk.
- Identify weaknesses and gaps in cybersecurity controls.
- Develop cyber risk ratings and prioritization mechanisms.
- Assess cyber risks associated with third parties, suppliers, and technology providers.
- Evaluate risks related to customer data, digital platforms, and online services.
- Develop risk treatment and mitigation plans.
- Align cyber risk management with risk appetite and enterprise risk management.
- Support management reporting and decision-making using cyber risk information.
- Integrate cyber risk considerations into business continuity and resilience planning.
- Strengthen governance and accountability for cyber risk.
- Develop an actionable cyber risk assessment and improvement roadmap.

Course Outline

DAY 01

Cyber Risk Landscape in the Insurance Industry

- Understanding cyber risk and its strategic importance to insurance organizations.
- The evolving cyber threat landscape affecting insurers.
- Common cyber threats, vulnerabilities, and attack vectors.
- Critical information assets and technology dependencies.
- Cyber risks across underwriting, claims, policy administration, payments, and customer services.
- Risks associated with digital insurance platforms and remote operations.
- Customer data exposure and information security risks.
- Business, financial, operational, legal, and reputational consequences of cyber incidents.
- Building a cyber risk-aware organizational culture.

DAY 01 — CONTINUED

> **PRACTICAL APPLICATION**
>
> Identify critical assets, processes, dependencies, and cyber threats within a representative insurance organization.

DAY 02

Cyber Risk Identification and Assessment Methodologies

- Principles of cyber risk identification and assessment.
- Asset-based and scenario-based risk assessment approaches.
- Identifying cyber threats, vulnerabilities, and risk events.
- Developing insurance-specific cyber risk scenarios.
- Assessing likelihood and potential impact.
- Evaluating financial, operational, regulatory, customer, and reputational impacts.
- Developing cyber risk matrices and scoring models.
- Assessing control effectiveness.
- Determining inherent and residual cyber risk.
- Prioritizing cyber risks based on exposure and business criticality.

> **PRACTICAL APPLICATION**
>
> Conduct a structured cyber risk assessment for selected insurance processes and develop risk ratings.

DAY 03

Cyber Controls, Third-Party Risk and Data Protection

- Understanding preventive, detective, and corrective cybersecurity controls.
- Evaluating cybersecurity control effectiveness.
- Identifying control weaknesses and remediation priorities.
- Cyber risks associated with technology providers and third parties.
- Assessing supplier, outsourcing, and cloud-related cyber risks.
- Customer data protection and privacy risks.

DAY 03 — CONTINUED

- Risks associated with digital customer platforms and applications.
- Managing access, authentication, data security, and information protection risks.
- Assessing cyber resilience across critical service providers.
- Integrating third-party cyber risk into enterprise risk assessments.

PRACTICAL APPLICATION

Evaluate the cyber risk profile of a critical third-party provider and develop a risk treatment plan.

DAY 04

Cyber Risk Treatment, Resilience and Insurance Implications

- Developing cyber risk treatment strategies.
- Risk avoidance, reduction, transfer, acceptance, and mitigation.
- Aligning cyber risk treatment with risk appetite.
- Cyber incident response and escalation considerations.
- Business continuity and disaster recovery for cyber events.
- Cyber resilience and recovery of critical insurance services.
- Cyber risk implications for insurance underwriting and risk selection.
- Understanding cyber insurance exposure and risk transfer considerations.
- Scenario analysis and cyber stress testing.
- Developing early-warning indicators for emerging cyber risks.

PRACTICAL APPLICATION

Analyze a major cyber incident scenario affecting an insurance company and develop a comprehensive response, mitigation, and resilience plan.

DAY 05

Cyber Risk Governance, Reporting and Strategic Implementation

- Cyber risk governance and accountability.
- Roles of executive management, risk functions, technology, security, compliance, and internal audit.
- Integrating cyber risk into enterprise risk management.
- Cyber risk appetite and tolerance.
- Developing cyber risk indicators and management dashboards.
- Reporting cyber risk to senior management and decision makers.
- Monitoring emerging cyber risks and changing threat conditions.
- Establishing continuous cyber risk assessment processes.
- Prioritizing cybersecurity investments based on risk exposure.
- Building a sustainable cyber risk management framework.
- Developing a cyber risk assessment implementation roadmap.

FINAL WORKSHOP

Develop an integrated cyber risk assessment framework for an insurance organization, including critical assets, threat scenarios, risk ratings, control assessment, residual risk, third-party exposure, mitigation strategies, governance, reporting, and an implementation roadmap.

Register or Request More Information

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