QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1998

Third-Party Risk Management & Vendor Risk Assessment Training Course

THIRD-PARTY & SUPPLY CHAIN RISK MANAGEMENT
RISK, COMPLIANCE & GOVERNANCE

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Third-Party Risk Management & Vendor Risk Assessment Training Course provides a comprehensive and practical framework for identifying, assessing, managing, and monitoring risks arising from suppliers, vendors, contractors, service providers, technology partners, outsourcing arrangements, and other external third parties. The course focuses on strengthening organizational resilience by establishing structured approaches to third-party risk throughout the relationship lifecycle.

Participants will examine the complete third-party risk management lifecycle, from initial risk identification and due diligence through onboarding, contracting, ongoing monitoring, performance assessment, remediation, renewal, and termination. The program addresses key risk dimensions including operational, financial, regulatory, legal, cybersecurity, data privacy, reputational, concentration, business continuity, and strategic risks.

Particular emphasis is placed on developing effective vendor risk assessment methodologies, including risk classification, inherent and residual risk assessment, criticality analysis, due diligence questionnaires, evidence review, control evaluation, scoring models, risk ratings, and escalation criteria. Participants will learn how to distinguish between different levels of third-party exposure and apply proportionate controls according to the criticality and risk profile of each relationship.

The course also addresses governance, accountability, contractual controls, monitoring frameworks, key risk indicators, incident management, third-party resilience, and reporting. Through practical case studies, assessment exercises, risk scenarios, and workshops, participants will develop the capability to build and improve a structured third-party risk management framework aligned with organizational objectives and regulatory expectations.

Objectives

- By the end of the course, participants will be able to:
- Analyze the strategic importance of third-party risk management within enterprise risk frameworks.
- Identify major categories of risk associated with suppliers, vendors, contractors, and service providers.

- Develop structured third-party risk management lifecycle frameworks.
- Classify third parties according to criticality, dependency, exposure, and risk level.
- Design effective vendor due diligence and risk assessment processes.
- Evaluate financial, operational, regulatory, legal, cybersecurity, and reputational risks.
- Apply inherent and residual risk assessment methodologies.
- Develop risk scoring models, rating criteria, and risk-based assessment thresholds.
- Evaluate third-party controls, policies, certifications, evidence, and assurance documentation.
- Establish appropriate contractual risk requirements and control provisions.
- Develop ongoing third-party monitoring and performance management frameworks.
- Identify early warning indicators and emerging risks within third-party relationships.
- Strengthen management of cybersecurity, data privacy, and technology-related vendor risks.
- Integrate business continuity, resilience, and exit planning into third-party risk management.
- Establish effective escalation, remediation, exception, and issue-management processes.
- Develop third-party risk reporting and governance mechanisms for management and decision makers.

Who Should Attend

This course is designed for professionals responsible for third-party risk, vendor management, supplier governance, procurement, outsourcing, operational risk, compliance, information security, cybersecurity, business continuity, and enterprise risk management. It is particularly relevant to third-party risk managers, vendor risk specialists, supplier relationship managers, procurement professionals, contract managers, risk analysts, compliance officers, and internal control specialists.

The program is also suitable for professionals working in information security, cybersecurity, data protection, legal affairs, internal audit, finance, operations, business continuity, technology, procurement, governance, and enterprise risk, as well as managers and decision makers responsible for approving, overseeing, or monitoring material third-party relationships.

The course is highly applicable to government entities, ministries, banks, financial institutions, insurance companies, oil and gas organizations, telecommunications companies, technology providers, healthcare organizations, manufacturing companies, utilities, multinational corporations, and large enterprises with extensive supplier, outsourcing, or service-provider ecosystems.

Learning Outcomes

- Upon successful completion of the course, participants will be able to:
- Map an organization's third-party ecosystem and identify critical external dependencies.
- Apply risk-based segmentation to suppliers, vendors, and service providers.
- Conduct structured vendor due diligence and risk assessments.
- Determine inherent risk based on the nature, scope, and criticality of a third-party relationship.
- Assess the effectiveness of third-party controls and identify control gaps.
- Calculate and interpret residual third-party risk following the application of controls.
- Develop practical vendor risk scoring and rating methodologies.
- Determine appropriate assessment depth and monitoring frequency based on risk.
- Evaluate vendor cybersecurity, data protection, operational resilience, and compliance exposure.
- Identify contractual requirements needed to manage material third-party risks.
- Establish monitoring mechanisms using risk indicators, performance measures, and assurance activities.
- Manage third-party incidents, breaches, control deficiencies, and remediation plans.
- Assess concentration, dependency, subcontracting, and fourth-party risks.
- Integrate business continuity and exit strategies into vendor risk assessments.
- Prepare management-level third-party risk reports and escalation recommendations.
- Develop an actionable third-party risk management framework for organizational implementation.

Course Outline

DAY 01

Foundations of Third-Party Risk Management & Risk Governance

- The strategic role of third parties in modern organizations
- Understanding the third-party risk landscape
- Third-party risk categories and exposure areas
- Supplier, vendor, contractor, outsourcing, and service-provider relationships
- Third-party risk management lifecycle

DAY 01 — CONTINUED

- Governance structures, roles, and accountability
- Risk ownership and responsibilities across business functions
- Criticality and materiality assessment
- Third-party inventory and risk mapping
- Risk appetite and third-party risk tolerance
- Integrating third-party risk with enterprise risk management

PRACTICAL APPLICATION:

- Participants develop a third-party inventory and classify relationships according to business criticality, dependency, and initial risk exposure.

DAY 02

Vendor Due Diligence & Risk Assessment Methodologies

- Principles of risk-based vendor due diligence
- Pre-engagement risk assessment
- Vendor onboarding and qualification
- Risk assessment questionnaires and information requirements
- Evaluating vendor financial stability and business capability
- Operational and service delivery risk assessment
- Regulatory, legal, and compliance assessment
- Cybersecurity and information security assessment
- Data privacy and information handling risks
- Business continuity and disaster recovery assessment
- Subcontractors and fourth-party exposure
- Risk scoring, rating models, and assessment thresholds

PRACTICAL APPLICATION:

- Participants complete a structured vendor risk assessment using a sample supplier profile, supporting evidence, risk criteria, and scoring methodology.

DAY 03

Third-Party Controls, Contracts & Risk Treatment

- Evaluating the effectiveness of vendor controls
- Control design versus control operating effectiveness
- Reviewing policies, procedures, certifications, audit reports, and assurance evidence
- Identifying control gaps and risk deficiencies
- Risk treatment and mitigation strategies
- Risk acceptance, transfer, reduction, and avoidance
- Contractual requirements for third-party risk management
- Service-level agreements and performance obligations
- Security, privacy, confidentiality, audit, and reporting provisions
- Incident notification and regulatory cooperation requirements
- Managing exceptions and compensating controls
- Remediation planning and corrective action management

PRACTICAL APPLICATION:

- Participants analyze a third-party control assessment, identify material gaps, and develop a risk treatment and remediation plan.

DAY 04

Ongoing Monitoring, Resilience & Third-Party Incident Management

- Continuous third-party risk monitoring
- Vendor performance and risk indicators
- Key risk indicators and early warning signals
- Periodic reassessment and risk rating updates
- Monitoring material suppliers and critical service providers
- Third-party cybersecurity and data incidents
- Vendor-related operational disruptions
- Incident escalation and response coordination

DAY 04 — CONTINUED

- Business continuity and third-party resilience
- Concentration and dependency risk
- Exit strategies and transition planning
- Managing changes in vendor ownership, services, systems, or subcontractors

PRACTICAL APPLICATION:

- Participants work through a third-party disruption scenario and develop monitoring, escalation, continuity, remediation, and exit actions.

DAY 05

Third-Party Risk Governance, Reporting & Continuous Improvement

- Third-party risk governance frameworks
- Management committees and oversight structures
- Risk reporting and executive dashboards
- Third-party risk aggregation and portfolio analysis
- Risk trends, emerging risks, and exposure analysis
- Monitoring compliance with third-party risk policies
- Internal audit and assurance over third-party risk management
- Measuring third-party risk management effectiveness
- Program maturity assessment
- Digital tools and automation for vendor risk management
- Improving assessment efficiency and data quality
- Building a sustainable third-party risk culture

FINAL WORKSHOP:

- Participants develop an integrated Third-Party Risk Management & Vendor Risk Assessment Framework covering governance, third-party classification, due diligence, risk scoring, control assessment, contractual requirements, ongoing monitoring, incident management, resilience, reporting, and continuous improvement.

QUEST
Professional Center

Register or Request More Information

Course page: https://quest-training.com/courses/third-party-risk-management-vendor-risk-assessment-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440