Training Course on Managing Third-Party and Vendor Incidents

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s rapidly evolving digital landscape, organizations are more dependent than ever on third-party vendors, partners, and contractors. While these relationships bring efficiency and cost-effectiveness, they also introduce significant cybersecurity, data protection, compliance, and operational risks. A single incident involving a vendor can lead to reputational damage, legal liabilities, and business continuity disruptions. That’s why understanding how to manage third-party risks and respond swiftly to vendor-related incidents is crucial for safeguarding organizational resilience.

Training course on managing third-party and vendor incidents is designed to equip professionals with cutting-edge tools and methodologies to identify, mitigate, and respond to external threats posed by third-party ecosystems. Through real-world case studies, compliance frameworks, and strategic risk assessments, participants will gain hands-on knowledge on how to build a robust vendor risk management (VRM) program and enforce effective incident response plans (IRPs) aligned with NIST, ISO 27001, and GDPR standards.

Programme Curriculum

Training Course on Managing Third-Party and Vendor Incidents

Introduction

In today’s rapidly evolving digital landscape, organizations are more dependent than ever on third-party vendors, partners, and contractors. While these relationships bring efficiency and cost-effectiveness, they also introduce significant cybersecurity, data protection, compliance, and operational risks. A single incident involving a vendor can lead to reputational damage, legal liabilities, and business continuity disruptions. That’s why understanding how to manage third-party risks and respond swiftly to vendor-related incidents is crucial for safeguarding organizational resilience.

Training course on managing third-party and vendor incidents is designed to equip professionals with cutting-edge tools and methodologies to identify, mitigate, and respond to external threats posed by third-party ecosystems. Through real-world case studies, compliance frameworks, and strategic risk assessments, participants will gain hands-on knowledge on how to build a robust vendor risk management (VRM) program and enforce effective incident response plans (IRPs) aligned with NIST, ISO 27001, and GDPR standards.

Course Objectives

1. Understand the fundamentals of third-party risk management (TPRM)
2. Identify early signs of vendor-related cybersecurity incidents
3. Develop incident response strategies for outsourced services
4. Map supply chain risk exposure across vendors and partners
5. Perform vendor due diligence and monitoring
6. Evaluate compliance obligations under GDPR, HIPAA, and CCPA
7. Create vendor-specific risk mitigation plans
8. Learn to analyze third-party breach impacts on business continuity
9. Implement automated vendor assessment tools
10. Build a scalable vendor risk register
11. Establish a third-party incident communication plan
12. Use contractual clauses to enforce incident accountability
13. Align with NIST SP 800-161, ISO/IEC 27036, and SOC 2 frameworks

Target Audience

1. Information Security Officers (CISOs)
2. Risk and Compliance Managers
3. Procurement Professionals
4. Vendor Relationship Managers
5. IT Auditors and Consultants
6. Cybersecurity Analysts
7. Legal and Contracts Managers
8. Third-Party Risk Analysts and GRC Teams

Course Duration: 10 days

Course Modules

Module 1: Introduction to Third-Party Risk Management

- Define third-party relationships
- Understand external threat vectors
- Identify high-risk vendor categories
- Explore the risk lifecycle
- Overview of regulatory drivers
- **Case Study:** SolarWinds Supply Chain Attack

Module 2: Vendor Risk Profiling and Tiering

- Set risk assessment criteria
- Classify vendors by criticality
- Evaluate data access levels
- Score vendors by impact potential
- Prioritize mitigation efforts
- **Case Study:** Equifax’s Vendor Risk Oversight Gaps

Module 3: Third-Party Due Diligence

- Perform security questionnaires
- Conduct onsite audits
- Assess data handling policies
- Evaluate compliance certificates
- Monitor vendor financial health
- **Case Study:** Target's HVAC Vendor Breach

Module 4: Vendor Contracts and Security Clauses

- Insert data protection clauses
- Define SLAs and liability
- Address breach notification timelines
- Include audit rights
- Use indemnity clauses
- **Case Study:** British Airways GDPR Violation & Third Party

Module 5: Monitoring Third-Party Risks

- Automate risk detection
- Conduct continuous assessments
- Use threat intelligence feeds
- Perform regular penetration tests
- Monitor key risk indicators
- **Case Study:** Accellion File Transfer Vendor Breach

Module 6: Incident Detection and Reporting

- Set escalation protocols
- Define incident types
- Establish reporting timelines
- Use third-party alerts
- Map internal/external responsibilities
- **Case Study:** Marriott/Starwood Vendor Breach Timeline

Module 7: Incident Response Planning

- Build vendor-specific IRPs
- Align plans with NIST
- Define communication flow
- Assign roles & responsibilities
- Test IRP effectiveness
- **Case Study:** Colonial Pipeline Incident Response Gap

Module 8: Regulatory and Legal Compliance

- Map data regulations (GDPR, HIPAA, etc.)
- Identify jurisdictional challenges
- Understand breach reporting laws
- Align contracts with regulators
- Conduct compliance audits
- **Case Study:** Facebook–Cambridge Analytica Data Mishandling

Module 9: Cyber Insurance and Vendor Liability

- Define insurance requirements

- Include vendor coverage clauses
- Understand coverage limits
- Prepare claims procedures
- Link insurance to contracts
- **Case Study:** Merck & NotPetya Insurance Dispute

Module 10: Business Continuity and Resilience

- Define BCP expectations
- Test third-party DRPs
- Integrate with your resilience plans
- Review backup/recovery processes
- Evaluate alternate supplier options
- **Case Study:** Kaseya Ransomware & Customer Impact

Module 11: Vendor Offboarding and Data Retention

- Revoke system access
- Enforce data return/destruction
- Conduct exit audits
- Archive contracts & documents
- Ensure compliance at offboarding
- **Case Study:** Boeing Insider Vendor Risk Exit Failure

Module 12: Automation in Vendor Risk Management

- Implement TPRM platforms
- Streamline onboarding
- Auto-score assessments
- Generate real-time dashboards
- Use AI for anomaly detection
- **Case Study:** IBM TPRM Automation Success

Module 13: Cross-Departmental Collaboration

- Engage Legal, IT, Procurement
- Align goals across departments
- Set shared KPIs
- Promote awareness training
- Use centralized communication tools
- **Case Study:** Uber’s Interdepartmental Failure Post-Breach

Module 14: Metrics, KPIs, and Reporting

- Define vendor risk KPIs
- Use metrics for board reporting
- Track vendor SLAs
- Identify trends & root causes
- Optimize risk dashboards
- **Case Study:** Deloitte’s Vendor KPI Framework

Module 15: Future Trends in Vendor Risk Management

- Predict AI-driven vendor risks
- Prepare for supply chain attacks
- Embrace zero trust architecture

- Shift to continuous trust verification
- Invest in predictive analytics
- **Case Study:** Microsoft's Evolution in Vendor Risk Defense

Training Methodology

- Interactive lectures and expert-led sessions
- Real-world case studies and incident simulations
- Group workshops and scenario-based learning
- Hands-on sessions with tools and frameworks
- Role-play activities and crisis communication drills
- Assessments and quizzes after each module

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
28 Sep 2026	09 Oct 2026	Online	$2,000
28 Sep 2026	09 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
28 Sep 2026	09 Oct 2026	Physical	$0
28 Sep 2026	09 Oct 2026	Physical	$0
28 Sep 2026	09 Oct 2026	Physical	$0
28 Sep 2026	09 Oct 2026	Physical	$0
28 Sep 2026	09 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com