Advanced Third-Party Risk and Supply Chain Security Training Course



16 - 20 Nov 2026

Milan

5900 € (Per Person)

Ref: #CYB4059_89231

Course Introduction / Overview:

In today's hyper-connected global economy, organizations are increasingly reliant on a complex web of third-party vendors, suppliers, and partners. While these relationships drive innovation and efficiency, they also introduce significant vulnerabilities, from cybersecurity breaches to operational disruptions. This course provides a comprehensive framework for managing these intricate risks. We will explore the complete Third-Party Risk Management (TPRM) lifecycle, from initial due diligence and vendor onboarding to continuous monitoring and strategic offboarding. Furthermore, the curriculum delves deep into the critical domain of supply chain security, addressing both digital and physical threats. As highlighted by Dr. Yossi Sheffi in his work, including "The New (Ab)Normal," building resilience is no longer optional but a core strategic imperative. This program, offered by BIG BEN Training Center, moves beyond theoretical concepts to provide actionable strategies for developing robust governance structures, implementing effective risk assessment methodologies, and fostering a culture of security throughout your extended enterprise. Participants will learn to navigate the complex regulatory landscape and build a resilient supply chain capable of withstanding modern-day threats, ensuring business continuity and protecting organizational reputation.

Target Audience / This training course is suitable for:

- Supply Chain and Logistics Managers.
- Procurement and Sourcing Professionals.
- Vendor and Contract Managers.
- Risk and Compliance Officers.
- IT Security and Cybersecurity Specialists.
- Internal Auditors and Governance Professionals.
- Operations Managers.
- Legal and Corporate Counsel.
- Business Continuity and Resilience Planners.

Target Sectors and Industries:

- Manufacturing and Industrial Production.
- Financial Services and Banking.
- Healthcare and Pharmaceuticals.
- Technology and Telecommunications.
- Retail and Consumer Goods.
- Energy and Utilities.
- Transportation and Logistics.
- Government Agencies and Public Sector Organizations.

Target Organizations Departments:

- Procurement and Sourcing.
- Supply Chain Management.
- Information Technology and Cybersecurity.
- Risk Management and Compliance.
- Legal and Contract Management.
- Internal Audit.
- Operations.
- Finance.

Course Offerings:

By the end of this course, the participants will have able to:

- Develop and implement a comprehensive Third-Party Risk Management (TPRM) framework.
- Conduct thorough due diligence and risk assessments for new and existing vendors.
- Master techniques for negotiating robust contracts with clear security and performance clauses.
- Establish effective continuous monitoring programs for third-party relationships.
- Identify and mitigate cybersecurity risks within the software and hardware supply chain.
- Enhance supply chain resilience against geopolitical, environmental, and operational disruptions.
- Develop and test incident response plans for third-party and supply chain breaches.
- Align TPRM and supply chain security programs with international standards like ISO 28000.
- Create meaningful risk reports and communicate effectively with senior leadership and stakeholders.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be immersive, interactive, and highly practical. We believe that adult learning is most effective when it combines expert knowledge with hands-on application. This course moves beyond traditional lectures to foster a dynamic learning environment where participants actively engage with the material. Sessions will feature a blend of expert-led presentations, in-depth case study analyses of real-world supply chain disruptions, and collaborative group exercises. Participants will work in teams to solve complex vendor risk scenarios, develop risk assessment matrices, and draft key contractual clauses. Interactive workshops and facilitated discussions will encourage the sharing of experiences and best practices among peers from various industries. Ample time is allocated for Q&A sessions to ensure all concepts are clearly understood. The focus is on providing practical tools, templates, and frameworks that participants can immediately apply to strengthen their organization's third-party risk and supply chain security posture upon returning to the workplace.

Course Agenda (Course Units):

Unit One: Foundations of Third-Party Risk and Supply Chain Security

- Introduction to the modern extended enterprise.
- Defining Third-Party Risk Management (TPRM) and its core components.
- Understanding the convergence of TPRM and supply chain security.
- Key drivers for TPRM including regulatory pressures and business demands.
- The global regulatory landscape (GDPR, CCPA, etc.).
- Introduction to key frameworks and standards (NIST, ISO 28000).
- Establishing a business case for a robust TPRM program.

Unit Two: The TPRM Lifecycle: Onboarding and Due Diligence

- Phase 1: Planning and vendor identification.
- Phase 2: Initial risk stratification and inherent risk assessment.
- Phase 3: Comprehensive due diligence across multiple risk domains.
- Assessing financial viability and operational stability.
- Evaluating information security and data privacy controls.
- Conducting reputational and compliance checks.
- Phase 4: Risk-based decision-making and vendor selection.

Unit Three: Contract Management and Continuous Monitoring

- The critical role of contracts in risk mitigation.
- Negotiating key security, privacy, and performance clauses.
- Defining Service Level Agreements (SLAs) and Key Performance Indicators (KPIs).
- Establishing a framework for continuous monitoring.
- Leveraging technology for automated monitoring and alerts.
- Conducting periodic risk reviews and performance assessments.
- Managing the vendor offboarding and data exit strategy.

Unit Four: Advanced Supply Chain Security and Resilience

- Mapping your supply chain to identify critical nodes and dependencies.
- Cybersecurity Supply Chain Risk Management (C-SCRM).
- Securing the software development lifecycle and open-source components.
- Mitigating physical security risks in logistics and transportation.
- Developing a supply chain threat intelligence program.
- Building operational resilience and business continuity plans.
- Incident response planning for supply chain disruptions.

Unit Five: Governance, Reporting, and Future Trends

- Establishing a clear TPRM governance structure with defined roles.
- Developing effective risk appetite statements and tolerance levels.
- Creating insightful dashboards and reports for stakeholders and the board.
- Managing fourth-party risk (your vendors' vendors).
- Addressing emerging threats like geopolitical risk and climate change.
- The role of Artificial Intelligence and Machine Learning in TPRM.
- Cultivating a risk-aware culture across the organization.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

Considering the increasing complexity and geopolitical tensions, how can an organization balance the efficiency gains from global sourcing with the escalating security risks in its supply chain?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by offering a holistic and integrated perspective that bridges the often-siloed disciplines of Third-Party Risk Management (TPRM) and Supply Chain Security. While many programs focus on one area, we recognize that in the modern enterprise, these risks are deeply intertwined. Our curriculum is meticulously designed to address this convergence, providing a unified framework for managing the entire extended enterprise. The program emphasizes practical, actionable strategies over purely theoretical knowledge. Participants will not just learn about risk assessment models; they will build them. They will not just hear about contract clauses; they will analyze and debate them in realistic scenarios. Furthermore, the course is forward-looking, dedicating significant time to emerging threats such as fourth-party risk, software supply chain vulnerabilities, and the impact of geopolitical instability. By focusing on building strategic resilience rather than just tactical compliance, this training equips professionals with the advanced competencies needed to protect their organizations from complex, multi-faceted threats and build a truly secure and resilient operational ecosystem.