MERCURY

Cyber Risk Management & IT Supply Chain Security

14 - 18 Feb 2027
Istanbul (Turkey)

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Cyber Risk Management & IT Supply Chain Security

Ref.: 121382_1030274 **Date:** 14 - 18 Feb 2027 **Location:** Istanbul (Turkey) **Fees:** 5500 **Euro**

Introduction

The Cyber Risk Management & IT Supply Chain Security course equips participants with an understanding of digital supply chain risk management and IT security practices. It focuses on identifying cyber threats targeting suppliers and partners within digital ecosystems and assessing their impact on organizational IT infrastructure. It covers risk management policies, best practices for threat identification, and mitigation strategies to reduce exposure to digital threats. Participants will explore frameworks for evaluating vulnerabilities and developing proactive security controls. The course enhances analytical and strategic decision-making skills. Learners can design and implement resilient risk management plans that safeguard IT supply chains.

Targeted Groups

This Cyber Risk Management & IT Supply Chain Security training targets professionals seeking knowledge and skills:

- Information Security Managers and Cybersecurity Officers.
- Network Engineers and IT Infrastructure Leaders.
- IT Risk and Supply Chain Risk Analysts.
- Compliance, Governance, and Internal Control Officers.
- Procurement and IT Vendor Management Professionals.
- IT Project Leaders and Security Consultants.
- Digital Security Researchers and Technical Analysts.

Course Objectives

Participants will achieve the following objectives by completing the Cyber Risk Management & IT Supply Chain Security course:

- Understand core principles of digital supply chain security and cyber risk management.
- Distinguish between internal and external risks affecting IT supply chains.
- Analyze common cyber attacks targeting supplier ecosystems.
- Learn how to develop policies for documenting and evaluating vendor security postures.
- Build frameworks to identify threats and assess the impact of vulnerabilities.
- Plan mitigation techniques to strengthen data protection and operational resilience.
- Implement advanced security controls aligned with risk assessment outcomes.
- Enhance compliance with data protection regulations and governance standards.
- Develop responses for incident handling and continuity planning.
- Strengthen organizational readiness for evolving cyber threats affecting supply networks.

Targeted Competencies

Participants will gain the following competencies during the Cyber Risk Management & IT Supply Chain Security program:

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

- Ability to assess digital supply chain risk using advanced risk analysis tools.
- Proficiency in applying cybersecurity standards in vendor environments.
- Competence in drafting risk evaluation reports clearly and accurately.
- Skills in identifying and prioritizing vulnerabilities for mitigation.
- The capability to monitor suspicious activities within shared networks.
- Proficiency in selecting and implementing effective digital security controls.
- Ability to plan and execute incident response and recovery actions.
- Skills in internal communication and multi-team coordination.
- Knowledge of regulatory and legal requirements for secure IT supply chains.

Studying Scenarios

In this Cyber Risk Management & IT Supply Chain Security training, participants develop skills through the following scenarios:

- Evaluating the impact of a cyber attack on a key technology supplier.
- Analyzing a digital supply chain breach and estimating effects on customer data.
- Planning incident response to secure breached vendor infrastructure.
- Simulating vendor security patch rollout and monitoring results.
- Prioritizing security controls based on risk, cost, and exposure levels.
- Conducting vendor compliance reviews against cyber risk criteria.
- Collaborating across teams to resolve a simulated supply chain attack.

Course Content

Unit 1: Fundamentals of Cyber Risk Management & IT Supply Chain Security

- Introduction to cyber threats and their relevance to IT supply chains.
- Key principles of cyber risk management in organizational contexts.
- Overview of digital supply chain vulnerabilities and attack vectors.
- Differentiating between internal and external risks within IT networks.
- Common types of cyberattacks targeting vendors and third-party partners.
- Assessing the impact of cyber risks on operational performance.
- Understanding governance frameworks and their role in digital supply chain security.
- Integrating risk awareness into organizational culture and IT operations.

Unit 2: Policies and Frameworks for Supply Chain Risk Management

- Establishing a unified cyber risk management policy for vendors.
- Criteria for vendor selection based on security posture and compliance.
- Documentation and verification of vendor cybersecurity practices.
- Controlling access privileges and monitoring network activity.
- Risk assessment models and methodologies for supplier ecosystems.
- Procedures for continuous monitoring of third-party systems.
- Legal and regulatory requirements for IT supply chain security.
- Aligning policy frameworks with organizational compliance standards.

Unit 3: Threat Identification and Vulnerability Assessment

- Techniques for analyzing system vulnerabilities in supplier networks.
- Tools and technologies for threat detection and assessment.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

- Evaluating dependencies between vendors and internal IT systems.
- Threat modeling to classify and prioritize risks.
- Indicators of compromise and early warning signs in supply chains.
- Documenting vulnerabilities and determining mitigation priorities.
- Quantitative and qualitative methods to measure exposure levels.
- Linking risk assessment outcomes to decision-making processes.

Unit 4: Risk Impact Evaluation & Mitigation Planning

- Measuring the operational and financial impact of potential cyber incidents.
- Techniques for assessing data loss and reputational damage.
- Designing mitigation strategies aligned with risk analysis.
- Applying preventive measures to reduce exposure in vendor systems.
- Cloud security and third-party service provider risk management.
- Conducting tabletop exercises and simulations for incident response.
- Evaluating the effectiveness of mitigation measures and controls.
- Updating plans based on post-incident reviews and lessons learned.

Unit 5: Advanced Frameworks & Sustainable Security Practices

- Integrating supply chain security into enterprise governance and risk management.
- Continuous improvement and regular security updates for vendors.
- Developing ongoing training programs for IT and security teams.
- Leveraging AI and predictive analytics for threat forecasting.
- Business continuity planning and recovery strategies post-incident.
- Monitoring and auditing security improvements over time.
- Building a collaborative security culture with suppliers and partners.
- Scaling security measures for global and multi-tier supply chains.

Final Insights & Key Takeaways

Participants will leave the course with the ability to design, implement, and continuously improve IT supply chain security strategies against cyber threats. The course enhances resilience, supports informed decision-making, and promotes adherence to modern cybersecurity standards across organizational networks and vendor ecosystems.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Registration form on the :
Cyber Risk Management & IT Supply Chain Security

code: 121382 **From:** 14 - 18 Feb 2027 **Venue:** Istanbul (Turkey) **Fees:** 5500 **Euro**

Complete & Mail or fax to Mercury Training Center at the address given below

Delegate Information

Full Name (Mr / Ms / Dr / Eng):
.....
Position:
.....
Telephone / Mobile:
.....
Personal E-Mail:
.....
Official E-Mail:
.....

Company Information

Company Name:
.....
Address:
.....
City / Country:
.....

Person Responsible for Training and Development

Full Name (Mr / Ms / Dr / Eng):
.....
Position:
.....
Telephone / Mobile:
.....
Personal E-Mail:
.....
Official E-Mail:
.....

Payment Method

☐ Please invoice me

☐ Please invoice my company