MERCURY

IT Supply Chain Risk Management

7 – 11 December 2026
Milan (Italy)



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

MERCURY

IT Supply Chain Risk Management

Ref: 121381_1030247 **Date:** 7 – 11 December 2026 **Location:** Milan (Italy) **Fees:** 6200 Euro

Introduction

The IT Supply Chain Risk Management course equips participants with a comprehensive understanding of cyber risks in IT supply chains. It covers international standards and policies for supply chain risk management, as well as various compliance requirements. Participants learn to identify potential threats and vulnerabilities and assess their impact on organizational operations. The course emphasizes developing mitigation plans and enhancing cybersecurity across the supply chain. It enables participants to use risk assessment tools and techniques both practically and theoretically. The content supports applied and theoretical learning with a focus on global best practices in risk management.

Targeted Groups

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

- IT staff and cybersecurity officers.
- Supply chain managers and operations specialists.
- Compliance and risk management professionals.
- System audit and internal control experts.
- Business continuity leaders and executives.
- Cyber risk assessment consultants.
- Professionals working with vendors or technology partners.

Course Objectives

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

- Understand concepts of cyber risk management in supply chains.
- Learn supply chain risk management policies and standards.
- Identify threats and vulnerabilities related to IT systems.
- Assess the impact of risks on organizational operations.
- Develop strategic mitigation plans.
- Enhance decision-making skills based on risk assessments.
- Strengthen monitoring of compliance and internal policies.
- Integrate global best practices for supply chain security.
- Manage vendor relationships to ensure sustainable security.
- Use risk assessment tools and techniques effectively.

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

Targeted Competencies

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

- Ability to analyze risks and identify threats.
- Deep knowledge of supply chain protection policies.
- Skills in evaluating vulnerabilities and potential impacts.
- Ability to develop mitigation and emergency response plans.
- Cyber risk management skills within enterprise environments.
- Understanding methods to measure cybersecurity performance.
- Ability to engage with vendors to ensure compliance.
- Strategic and effective security decision-making skills.
- Competence in using modern tools and technologies for risk assessment.
- Awareness of cyber threats and protection of sensitive information.

Studying Scenarios

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

- Analyze supply chain threats to identify vulnerabilities.
- Study cybersecurity failure cases and organizational impact.
- Assess vendors' procedures and security practices.
- Develop response plans for potential risks.
- Test risk reduction techniques in virtual environments.
- Simulate cyberattacks on supply chains.
- Review compliance strategies and internal policies.

Course Content

Unit 1: Concepts and Fundamentals of Supply Chain Risk Management

- Define supply chain risk management and its importance.
- Explore the relationship between cybersecurity and supply chains.
- Identify the types of cyber threats and their impacts on supply chains.
- Review international standards and policies for risk management.
- Recognize essential elements of digital supply chains.
- Understand core concepts for risk assessment and vulnerabilities.

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

Unit 2: Policies and Risk Management Standards

- Review internal and external risk management policies.
- Study international standards for IT supply chain protection.
- Understand compliance requirements and their importance.
- Examine the role of procedures and policies in risk prevention.
- Develop security policies aligned with best practices.
- Integrate cybersecurity into supply chain operations.

Unit 3: Identifying Threats and Vulnerabilities

- Methods to detect digital threats and supplier risks.
- Tools for assessing vulnerabilities and potential impacts.
- Evaluate risks associated with contracts and partners.
- Study potential attack scenarios on supply chains.
- Prioritize risks based on operational impact.
- Use performance indicators to monitor vulnerabilities.

Unit 4: Mitigation Strategies and Contingency Plans

- Develop mitigation plans for potential risks.
- Continuous cyber risk management strategies.
- Prepare emergency response and business continuity plans.
- Integrate cybersecurity plans into operational continuity.
- Methods to protect sensitive data and critical information.
- Periodically review and update plans to ensure effectiveness.

Unit 5: Performance Evaluation and Continuous Improvement

- Measure the effectiveness of risk management plans.
- Use KPIs to evaluate cybersecurity performance.
- Review evaluation results and identify improvements.
- Develop continuous improvement plans for supply chain security.
- Integrate global best practices for sustainable protection.
- Monitor innovations and modern technologies in cybersecurity.
- Provide comprehensive reports to senior management on the status of risks and policies.

Final Insights & Key Takeaways

The course enhances participants' ability to manage IT supply chain risks effectively. It provides practical tools and strategies to mitigate threats and strengthen cybersecurity within organizations.