# Supply Chain Cyber Security Risk Management

Course: **00110**
Filter: **Beginner**
Duration: **2 days**
Category:: **Gouvernance, Risk and Compliance**
Price: **3500,00 €**

## About Course

This course provides an introduction to fundamental cybersecurity risk management concepts and how they are applied to modern supply chains. Attendees will learn how to identify critical suppliers, assess risk in third and fourth-party relationships, and identify mitigation strategies. The course covers risks associated with hardware, software, and services acquired from external sources, and attendees will learn strategies for analyzing, treating, and monitoring cyber risk throughout the supply chain.

## What you'll learn

- Identify supply chain components in modern organizations, including hardware, software, and services
- Inventory critical assets and suppliers, and assess the risks they pose to your organization
- Understand risk mitigation options, and how to adapt them to address complex risks across the supply chain
- Implement risk management frameworks and build a supply chain risk management plan
- Audit and perform oversight of supply chain risk to monitor risk mitigation effectiveness
- Continue learning and face new challenges with after-course one-on-one instructor coaching

## Targeted audience

- Risk managers, looking to extend risk management programs to external third parties, suppliers, and vendors.
- Security practitioners, tasked with holistic risk management.

## Pre-requisites

- To be successful in this course, some experience with risk management and business management is helpful but not required.
- Basic product development knowledge is beneficial, such as software development lifecycles and integrating components into a final product.

## Curriculum

### Module 1: Risk Management Basics

- In this module, you will learn to:
- Define Risk and determine its likelihood and probability.
- Assess Risk's financial, reputational, and revenue impact.
- Define Threats and Threat Actors.
- Identify threat modeling approaches.
- Define Vulnerabilities to networks and organizations.
- Discuss methods of risk assessment: qualitative vs. quantitative.
- Identify ways to mature risk assessment processes over time through an Iterative risk assessment.

### Module 2: Supply Chain Basics

- In this module, you will learn about:
- Define Supply Chain, Vendor, Third/Fourth Party, and key parts of a supply chain.
- Operational risk and understanding the business impact of prioritizing critical suppliers.
- Common supply chain risks arising from Hardware (HW), Software SW), and Open-source software (OSS).

- Inherited/platform risks (e.g., operating system risks that impact an application, underlying modules included in a larger application like Log4j).
- Risks from services such as key vendors, third parties, etc.
- Identifying vulnerabilities - What do attackers target?
- What motivates supply chain attacks, and who are the victims?

**Module 3: SCRM Tools & Practices**

- In this module, you will learn how to:
- Build an SCRM plan.
- Leverage existing security and privacy controls in the organization.
- Identify common framework elements that push compliance to other organizations, such as Business Associates in HIPAA and data subprocessors in GDRP

**Module 4: Compliance Frameworks, SCRM Vendors, and Tools**

- In this module, you will learn about:
- Using a compliance framework to build SCRM capability internal to an organization.
- Requirements to comply with a framework as a vendor to other organizations.
- CMMC & NIST SP 800-171.
- CMMI for Acquisition (CMMI-ACQ).
- SOC 2
- Identify as a proactive measure; service providers can undergo an audit and have a documented report of compliance available to share with business partners.
- Discuss various SOC reports (1, 2, 3) and types (I, II).
- Cloud Security Alliance (CSA), Cloud Controls Matrix (CCM), Consensus Assessment Initiative Questionnaire (CAIQ), and the CSA STAR Registry.