

Auditing a Cybersecurity Programme

Professional training programme



SPARK TRAINING

Professional training courses for leaders, specialists, and organizations seeking practical capability development.

info@sparktraining.eu

+31 85 115 0004 | sparktraining.eu

— Workshop Overview

Today, security risks requiring audits are increasing dramatically. To prevent the data breaches that executives fear, auditors must be able to assess the effectiveness of a company's cybersecurity program. This involves understanding the necessary controls, how to implement them, and how to evaluate their effectiveness. Participants in this Auditing a Cybersecurity Programme training course will engage in various exercises designed to solidify their knowledge of creating and executing effective security solutions. This Auditing a Cybersecurity Programme training course will equip them with the skills needed to perform cyber assessments, making them valuable assets to their organization's cyber defense team. This training course will feature:

- Simulations of real cybersecurity program audits
- Tips for effective cybersecurity auditing
- Cyber risk assessments
- Threat analysis
- Case studies of cybersecurity breaches and their consequences

Why Attend

This course uses instructor-led sessions, guided discussion, and practical exercises built around Day One: Introduction to Cybersecurity, Day Two: Inventory Security Management, Day Three: Network Security Management, and day four: data security management.

Who Should Attend

Auditors
IT professionals who are interested in conducting cybersecurity audits, risk assessments, vulnerability and threat analysis or control self-assessments

— Learning Objectives

- Perform risk analysis of IT security breaches
- Get acquainted with ISO 27001 and COBIT5
- Acquire the knowledge of Information Security Management
- Understand the approach for incident response, Crisis Management and Disaster Recovery

Course Outline

DAY
1

Day One: Introduction to Cybersecurity

- Vulnerability assessment
- Threat analysis
- Cybersecurity risk assessment
- Cybersecurity program
- Cybersecurity risk auditing

DAY
2

Day Two: Inventory Security Management

- Inventory authorized and unauthorized devices
- Inventory authorized and unauthorized software
- Secure configurations
- Continuous vulnerability assessment and remediation
- Control use of administrative privileges
- Maintenance, monitoring and analysis of audit logs

DAY
3

Day Three: Network Security Management

- Email and web browser protection
- Malware defenses
- Security configurations for network devices
- Wireless access control
- Limitation and control of network ports, protocols and services

DAY
4

Day Four: Data Security Management

- Data protection
- Controlled data access based on need to know
- Data recovery capability
- Boundary defenses
- Account monitoring and control
- Security skills assessment and training

DAY
5

Day Five: Security Incident Management

- Application software security
- Cybersecurity Incidents

- Incident response management
- Penetration tests
- Red team exercises

— Upcoming Classroom Dates

DATE	LOCATION	FEE
12 - 16 October 2026	Paris - France	€2,250
19 - 23 October 2026	Frankfurt - Germany	€1,625
2 - 6 November 2026	Barcelona - Spain	€1,925
9 - 13 November 2026	Frankfurt - Germany	€1,625
14 - 18 December 2026	Barcelona - Spain	€1,925
21 - 25 December 2026	Frankfurt - Germany	€1,625
18 - 22 January 2027	Barcelona - Spain	€1,925
15 - 19 February 2027	London - United Kingdom	€2,100

— Certificate and Registration

Participants who attend and complete the full programme receive a SPARK Training Certificate of Completion. For registration, in-house delivery, or availability questions, contact info@sparktraining.eu or +31 85 115 0004.