+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 01/23/2026

Register

Information Systems Security Manager Training

5 days (35 hours)

Overview

Our "Information Systems Security Manager" training course will enable you to understand the strategic, organizational, and regulatory issues related to IT security, and to use them as a lever for trust and sustainable performance for your organization.

You will learn how to design and deploy an Information Security Management System (ISMS) that complies with the ISO 27001 standard, integrate cybersecurity into your business processes, and implement robust governance that combines operational efficiency and regulatory compliance (GDPR, NIS2, DORA, etc.).

The training will also teach you the basic techniques of the CISO role: developing an appropriate security policy, defining and monitoring relevant indicators, and implementing audit and continuous improvement mechanisms. You will learn how to communicate with management and business units, prioritize actions, and manage security projects while balancing technical constraints, regulatory requirements, and business challenges.

A specific section will be devoted to legal and regulatory aspects: legal obligations, civil and criminal liability of the CISO, management of contractual clauses with service providers, and cooperation with supervisory authorities (ANSSI, CNIL, ENISA).
You will thus be able to anticipate regulatory changes and position security as a key factor in compliance and trust.

By participating in this training, you will develop a leadership position in cybersecurity, learn how to assess the maturity of your organization, anticipate technical, legal, and reputational risks, and unite management, business lines, and employees around a common vision of digital security.

Like all our training courses, this one will introduce you to **the latest stable version** of the

technology and its new features.

Objectives

- Understand the challenges of IT service security in an organization
- Learn the basic techniques of the CISO function
- Master the ISO 27001 standard and implement an ISMS in your organization
- Understand security policy and audit security and indicators
- Understand the regulations and legal aspects of IT system security

Target audience

- Anyone required to perform the role of information systems security manager

Prerequisites

- Experience working in an IT department
- Basic knowledge of information system security and a good understanding of systems and infrastructure

Our Information Systems Security Manager (RSSI) Training Program

[Day 1 - Morning]

The role of the CISO in the organization

- Defining the key missions of the CISO
- Identify internal and external stakeholders
- Mapping the scope of security actions
- Positioning the role within corporate governance
- Deciphering the expectations of management and business lines
- Practical workshop: Reconstructing a corporate security organization chart.

The national and international cybersecurity ecosystem

- ANSSI: national authority, standards, and supervision of OIVs/OSEs
- CERT-FR: incident alert and response center
- CNIL: data protection and GDPR compliance
- ENISA: European agency, NIS2 coordination

- OIV/OSE: critical operators subject to enhanced obligations
- Qualified service providers (PASSI, SecNumCloud, PDIS/PRIS): certified audits, cloud and incident response.

[Day 1 - Afternoon]

Fundamentals of information system security

- Defining key concepts: availability, integrity, confidentiality, traceability
- Understanding current threats (malware, phishing, ransomware, etc.)
- Identify key technical vulnerabilities
- Reviewing layers of defense (network, system, application)
- Integrate security into the design process
- Practical workshop: Mapping major macro threats: cybercrime, state cyberdefense, espionage, geopolitical and economic issues.

Overview of frameworks and standards

- Security policy vs. IT charter
- Articulate security governance and operational management
- Mastering best practices from the digital hygiene guide
- Initiating a realistic security roadmap
- Practical workshop: Simplified ISS maturity assessment.

[Day 2 - Morning]

ISO 27001 standard

- Principles and objectives of ISO 27001
- Control areas (Annex A)
- Certification process and PDCA cycle
- Conducting a gap analysis
- Roles and responsibilities in compliance
- Comparison of ISO 27001 and NIST Cybersecurity Framework: similarities and differences
- Practical workshop: Mapping ISO 27001 requirements to a business case.

[Day 2 - Afternoon]

Implementing an ISMS (Information Security Management System)

- Definition and scope of an ISMS
- Governance and integration within the organization
- Security policy and document management

- Risk management in an ISMS
- Performance indicators and continuous improvement
- Document management (PSSI, procedures, audit evidence) and management tools
- Practical workshop: Developing a mini-ISMS plan for a fictional organization.

User security and defensive posture

- Cybersecurity awareness: communication levers
- Social engineering: tactics and countermeasures
- MFA, passwords, SSO: balancing security and usability
- Incident detection and reporting by users
- The roles of HR, managers, and employees in digital hygiene

[Day 3 - Morning]

Developing an appropriate security policy

- Objectives of an ISS policy
- Integrating ISS into business processes
- Write a clear, communicable, and operational policy
- Define levels of criticality and risk exposure
- Establish monitoring indicators: security KPIs/KRIs and their promotion to management
- Practical workshop: Collective drafting of an extract from an ISS policy.

[Day 3 - Afternoon]

Implement effective ISS governance

- Governance structure: committee, reporting, delegation
- Budget, resources, and prioritization of actions
- Managing outsourcing (IT outsourcing, cloud, service providers)
- Ensuring GDPR compliance on the security side
- International governance: SOX, PCI-DSS, DORA (finance), HIPAA (healthcare)
- Establishing a shared security culture

Planning and managing security actions

- Establish an annual ISS roadmap
- Monitoring ISS projects: tools, milestones, reviews
- Balance between urgent and long-term needs (projects, incidents)
- Implement periodic security reviews
- Liaise with business units and management

[Day 4 - Morning]

Apply a risk management approach

- Identify critical assets to be protected
- Map threats and vulnerabilities
- Assess the likelihood and impact of scenarios
- Select relevant treatment measures
- Monitor risks and communicate with decision-makers
- Introduction to the EBIOS Risk Manager (EBIOS-RM) method
- Practical workshop: Risk mapping using a simulated case study.

[Day 4 - Afternoon]

Legal: Meeting regulatory requirements

- Legal and regulatory obligations (GDPR, LPM, NIS2, DORA)
- Review of security contract clauses (customers/suppliers)
- Traceability, evidence, and responsibilities
- Cooperation with the DPO, group CISO, service providers
- Criminal and civil liability of the CISO and delegation of responsibilities
- International conventions (Budapest Convention, extraterritoriality, compliance outside the EU)
- Preparing for a security audit or inspection

Assessing and auditing IS security

- Types of audits (internal, third-party, technical, organizational)
- Audit methods and associated tools
- Collecting, analyzing, and evaluating discrepancies
- Monitoring corrective action plans
- Prepare an educational report for management

[Day 5 - Morning]

Organizing the response to security incidents

- Types of incidents (intrusion, fraud, compromise, etc.)
- Detection, classification, and escalation processes
- Establishment and role of a crisis unit
- Containment, eradication, recovery
- Internal and external crisis communication: management, press, authorities (ANSSI, CNIL)
- Post-mortem and feedback
- Practical workshop: Simulation of a cyber incident.

[Day 5 - Afternoon]

Developing a continuity and recovery plan (PCA/PRA)

- Differences between BCP and DRP: challenges, content, methods
- Identifying critical processes and associated resources
- Defining RTOs/RPOs and recovery scenarios
- Testing and maintaining your BCP/DRP
- Involve business units and management in resilience

Promote and bring to life the role of the CISO

- Establish appropriate communication (dashboards, indicators, reports)
- Promote the actions of the CISO to management
- Develop the CISO's soft skills: leadership, teaching, conflict management, strategic influence
- Maintain a state of alert without generating fear
- Train, empower, and unite stakeholders
- Be part of a continuous improvement process
- Practical workshop: Present a fictitious ISS report to the Executive Committee.

Companies concerned

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific professional knowledge or modern methods.

Positioning at the start of training

The positioning at the start of the training course complies with Qualiopi quality criteria. Once they have finalized their registration, learners receive a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives for the upcoming training course, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training course.

Training organization registered under number 11 75 54743 75. This registration does not constitute state approval.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg