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

Updated on 22/08/2025

Sign up

Information Systems Security Manager training course

5 days (35 hours)

Presentation

Our "Information Systems Security Manager" training course will enable you to understand the strategic, organizational and regulatory issues linked to the security of IT services, and to make it a lever of confidence and sustainable performance for your organization.

You'll learn how to design and deploy an ISO 27001-compliant Information Security Management System (ISMS), integrate cybersecurity into your business processes, and implement robust governance that combines operational efficiency with regulatory compliance (RGPD, NIS2, DORA...).

The course will also teach you the basic techniques of the CISO function: drawing up an appropriate security policy, defining and monitoring relevant indicators, and setting up audit and continuous improvement systems. You will learn how to dialogue with management and business units, prioritize actions and manage security projects while reconciling 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, as well as cooperation with control authorities (ANSSI, CNIL, ENISA).
This will enable you to anticipate regulatory changes and position security as a key factor in compliance and trust.

By taking part in this training course, you will develop a leadership posture in cybersecurity, be able to assess your organization's maturity, anticipate technical, legal and reputational risks, and unite management, business lines and employees around a common vision of digital security.

Objectives

- Understand the challenges of IT security within an organization
- Know 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
- Know the regulations and legal aspects of IT systems security

Target audience

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

Prerequisites

- Experience in an IT department
- Basic knowledge of security applied to information systems, and a good command of systems and infrastructures.

Our Information Systems Security Manager (ISSM) Training Program

[Day 1 - Morning]

The role of the CISO in the organization

- Define the key missions of the CISO
- Identify internal and external stakeholders
- Mapping the security scope of action
- Positioning the function within corporate governance
- Decipher management and business expectations
- Practical workshop: Reconstruction of a corporate security organization chart.

The national and international cybersecurity ecosystem

- ANSSI: national authority, standards & supervision of OIV/OSE
- CERT-FR: incident alert and response center
- CNIL: data protection and RGPD compliance
- ENISA: European agency, NIS2 coordination
- OIV/OSE: critical operators subject to enhanced obligations
- Qualified service providers (PASSI, SecNumCloud, PDIS/PRIS): audits, cloud and certified incident response.

[Day 1 - Afternoon]

Fundamentals of information systems security

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

Overview of frameworks and standards

- Security policy vs. IT charter
- Articulating security governance and operational management
- Mastering the best practices of the digital hygiene guide
- Creating a realistic security roadmap
- Practical workshop: Simplified SSI maturity diagnosis.

[Day 2 - Morning]

ISO 27001 standard

- Principles and objectives of ISO 27001
- Areas of control (Annex A)
- Certification process and PDCA cycle
- Conducting a gap analysis
- Roles and responsibilities in compliance
- ISO 27001 vs. NIST Cybersecurity Framework: convergences and differences
- Practical workshop: Mapping ISO 27001 requirements on a business case.

[Day 2 - Afternoon]

Implementation of an ISMS (Information Security Management System)

- Definition and scope of an ISMS
- Governance and integration into the organization
- Security policy and document management
- ISMS risk management
- Performance indicators and continuous improvement
- Document management (ISPS, procedures, audit evidence) and management tools
- Practical workshop: drawing up an ISMS mini-plan for a fictitious organization.

User security and defensive posture

- Raising awareness of cybersecurity: communication levers
- Social engineering: tactics and countermeasures

- MFA, passwords, SSO: balancing security and ergonomics
- Detection and reporting of incidents by users
- Roles of HR, managers and employees in digital hygiene

[Day 3 - Morning]

Drawing up an appropriate security policy

- Objectives of an SSI policy
- Integrating SSI into business processes
- Draw up a clear, communicable and operational policy
- Define levels of criticality and risk exposure
- Set up monitoring indicators: security KPI/KRI, and communicate them to management.
- Practical workshop: Collective drafting of an extract from an SSI policy.

[Day 3 - Afternoon]

Implement effective SSI governance

- Governance structure: committees, reporting, delegation
- Budget, resources and prioritization of actions
- Manage outsourcing (facilities management, cloud, service providers)
- Ensuring RGPD compliance on the security side
- International governance: SOX, PCI-DSS, DORA (finance), HIPAA (healthcare)
- Establish a shared security culture

Plan and manage security actions

- Establish an annual SSI roadmap
- Monitor SSI projects: tools, milestones, reviews
- Arbitrate between urgency and long term (projects, incidents)
- Set up periodic security reviews
- Dialogue with business 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 appropriate treatment measures
- Monitor risks and communicate to decision-makers
- Introduction to the EBIOS Risk Manager (EBIOS-RM) method

- Practical workshop: Risk mapping based on a simulated case.

[Day 4 - Afternoon]

Legal: Meeting regulatory requirements

- Legal and regulatory obligations (RGPD, LPM, NIS2, DORA)
- Review of contractual security clauses (customers/suppliers)
- Traceability, proof and responsibilities
- Cooperation with DPO, group CISO, service providers
- CISO's criminal and civil liability 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 audit (internal, third-party, technical, organizational)
- Audit methods and associated tools
- Gathering, analyzing and evaluating discrepancies
- Follow-up of corrective action plans
- Prepare an educational report for management

[Day 5 - Morning]

Organizing the response to security incidents

- Incident typology (intrusion, fraud, compromise, etc.)
- Detection, qualification and escalation processes
- Constitution and role of a crisis unit
- Contain, eradicate, restore
- Internal and external crisis communication: management, press, authorities (ANSSI, CNIL)
- Post-mortem and feedback
- Practical workshop: Simulation of a cyber incident.

[Day 5 - Afternoon]

Building a continuity and recovery plan (PCA/PRA)

- Differences between BCP and DRP: issues, content, methods
- Identify critical processes and associated resources
- Define RTO/RPO and recovery scenarios
- Test and maintain your BCP/RRP
- Involving business lines and management in resilience

Promote and support the CISO function

- Establish appropriate communications (dashboards, indicators, reports)
- Promote the CISO's actions to management
- Develop CISO soft skills: leadership, pedagogy, conflict management, strategic influence
- Maintain an alert posture without generating fear
- Training, co-responsibility, federating players
- Be part of a continuous improvement dynamic
- Practical workshop: Presenting a fictitious SSI report to the Executive Committee.

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

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

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

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