

Table of contents

Detailed agenda of the training course..... 2

Day 1 2

Day 2 3

Day 3 4

Day 4 5

Standards cited in this training course 8

List of acronyms 10

Detailed agenda of the training course

Day 1 Introduction to NIS 2 Directive and initiation of the NIS 2 Directive implementation

Section 1: Training course objectives and structure5

- Introduction
- General information
- Learning objectives
- Educational approach
- Examination and certification
- About PECB

Section 2: Standards and regulatory frameworks17

- ISO standards
- Digital Markets Act
- Digital Services Act
- Digital Operational Resilience Act
- EU Cybersecurity Act
- European Cyber Resilience Act
- Data Governance Act
- GDPR
- NIST Cybersecurity Framework
- CIS Controls
- Payment Services Directive 2
- NIS Directive
- NIS 2 Directive

Section 3: NIS 2 Directive.....51

- NIS 2 Directive structure, objectives, and subject matter
- NIS 2 Directive scope
- NIS Directive and NIS 2 Directive
- The impact of NIS 2 Directive
- Essential and important entities
- Transposition
- Administrative fines
- Important EU organizations

Section 4: NIS 2 Directive requirements.....72

- Overview of NIS 2 Directive requirements
- NIS 2 definitions
- Competent authority and single point of contact
- National cyber crisis management frameworks
- Cybersecurity risk-management measures
- Union level coordinated security risk assessments of critical supply chains
- Reporting obligations
- Use of European cybersecurity certification schemes
- General aspects concerning supervision and enforcement

Section 5: Initiation of the NIS 2 Directive implementation104

- Defining an approach for the NIS 2 Directive implementation
- Proposing implementation approaches
- Adopting the proposed implementation approaches
- Choosing a methodological framework to manage the implementation of the NIS 2 Directive
- Aligning with best practices

Section 6: The organization and its context.....115

- Determining the organization’s alignment with the scope of NIS 2 Directive
- Mission, objectives, values, and strategies
- Cybersecurity objectives
- Business requirements
- Internal and external environment
- Key processes and activities
- Interested parties
- Gap analysis

Day 2 Analysis of NIS 2 Directive compliance program, asset management, and risk management

Section 7: Cybersecurity governance4

- Cybersecurity governance
- National cybersecurity strategy

- Security policies
- Regulatory and compliance requirements

Section 8: Cybersecurity roles and responsibilities34

- Organizational structure
- Roles and responsibilities of involved parties
- RASCI model
- Leadership and project approval
- The cybersecurity team

Section 9: Asset management.....55

- Assets in cybersecurity
- Asset management system
- Asset management program
- Inventory of information and other associated assets
- Acceptable use of information and other associated assets
- Return of assets
- System component inventory

Section 10: Risk management69

- Context establishment
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment
- Communication and consultation
- Recording and reporting
- Monitoring and reviewing

Day 3 Cybersecurity controls, incident management, and crisis management

Section 11: Cybersecurity controls.....4

- Human resources security
- Types of access controls
- Use of cryptography
- Secure authentication
- Security of network services

Section 12: Supply chain security45

- Strengthening supply chain cybersecurity elements
- Managing supply chain risk
- Addressing vulnerabilities
- Ensuring information security in supplier relationships
- Overseeing information security in the ICT supply chain
- Ensuring the quality of products and services

Section 13: Incident management74

- Cybersecurity incident management objectives
- Plan and prepare
- Detect and report
- Assess and decide
- Respond
- Learn lessons

Section 14: Crisis management125

- NIS 2 Directive requirements
- Crisis management
- Characteristics of a crisis
- Crisis management plan
- Crisis communication
- Organizational leadership in crisis management

Day 4 Communication, testing, monitoring, and continual improvement in cybersecurity

Section 15: Business continuity4

- Business continuity management
- Business continuity strategies and solutions
- Backup management
- Business continuity plan
- Disaster recovery plan
- Tiers of disaster recovery

Section 16: Awareness and training28

- Competence definition

- Determining competence needs
- Competence development activities
- Competence development program type and structure
- Training provision and evaluation
- Cybersecurity awareness and strategy
- Cybersecurity awareness plan

Section 17: Communication60

- Principles of an effective communication strategy
- Establishing communication objectives
- Identifying with whom to communicate
- Planning communication activities
- Performing a communication activity
- Evaluating communication

Section 18: Testing in cybersecurity.....74

- Testing stages
- Testing techniques
- Preparing the test and documentation
- Post-testing activities

Section 19: Internal audit.....90

- ENISA self-assessment framework
- NIS 2 Directive audit
- Knowledge and competence to audit
- Internal compliance audit
- Collecting and verifying information
- Following up on nonconformities

Section 20: Measuring, monitoring, and reporting performance and metrics103

- Measurement objectives
- What needs to be monitored and measured
- Monitoring cybersecurity
- Performance indicators
- The frequency and method of monitoring and measurement
- Reporting the results

Section 21: Continual improvement.....119

- Continual monitoring of change factors

- Maintenance and improvement of the NIS 2 Directive compliance program
- Continual update of the documented information
- Documentation of improvements

Section 22: Closing of the training course131

- PECB certification scheme
- PECB certification process
- Other PECB services
- Other PECB training courses and certifications

To optimize the learning experience, PECB recommends scheduling two short breaks (15 minutes) and a lunch break (one hour) per training day. The time of the breaks can be adjusted accordingly.

Standards cited in this training course

- Directive (EU) 2022/2555, NIS 2 Directive
- ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls
- IEC 31010:2019, Risk management — Risk assessment techniques
- ISO 10015:2019, Quality management — Guidelines for competence management and people development
- ISO 19011:2018, Guidelines for auditing management systems
- ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements
- ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO 22361:2022, Security and resilience — Crisis management — Guidelines
- ISO 31000:2018, Risk management — Guidelines
- ISO 55000:2014, Asset management — Overview, principles and terminology
- ISO 9000:2015, Quality management systems — Fundamentals and vocabulary
- ISO 9001:2015, Quality management systems — Requirements
- ISO 22300:2021, Security and resilience — Vocabulary
- ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27031:2011, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27032:2023, Cybersecurity — Guidelines for internet security
- ISO/IEC 27035-1:2023, Information technology — Information security incident management — Part 1: Principles and process
- ISO/IEC 27035-2:2023, Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response
- ISO/IEC 27701:2019, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- ISO/IEC 30111:2019, Information technology — Security techniques — Vulnerability handling processes

- ISO/IEC TR 27103:2018, Information technology — Security techniques — Cybersecurity and ISO and IEC standards
- ISO/IEC TS 27100: 2020, Information technology — Cybersecurity — Overview and concepts
- NIST SP 800-115, Technical guide to information security testing and assessment
- NIST SP 800-133 Rev. 2, Recommendation for cryptographic key generation
- NIST SP 800-34 Rev. 1, Contingency planning guide for federal information systems
- NIST SP 800-53 Rev 5, Security and privacy controls for information systems and organizations
- NIST SP 800-61 Rev. 2, Computer security incident handling guide
- NIST SP 800-82 Rev 2, Guide to industrial control systems (ICS) security
- NIST SP 800-86, Guide to integrating forensic techniques into incident response

List of acronyms

ABAC: Attribute-based Access Control
AES: Advanced Encryption Standard
AMF: Annual Maintenance Fee
APIDS: Application Protocol-based Intrusion Detection System
BCM: Business Continuity Management
BCMS: Business Continuity Management System
BCP: Business Continuity Plan
BYOD: Bring Your Own Device
CA: Certificate Authority
CA: Competent Authorities
CAB: Change Advisory Board
CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart
CAT: Cybersecurity Awareness Team
CCP: Crisis Communication Plan
CDN: Content Deliver Network
CERT: Computer Emergency Response Team
CIA: Central Intelligence Agency
CII: Critical Information Infrastructure
CIO: Chief Information Officer
CIS: Center for Internet Security
CISO: Chief Information Security Officer
CMM: Capability Maturity Model
CMP: Crisis Management Plan
COBIT: Control Objectives for Information and Related Technologies
COO: Chief Operating Officer
CP: Corporation Group
CPD: Continuing Professional Development
CRA: Cyber Resilience Act
CSDP: Common Security and Defence Policy
CSF: Cybersecurity Framework
CSIRT: Computer Security Incident Response Team
CSO: Chief Security Officer
CTO: Chief Technology Officer
CV: Curriculum Vitae
CVD: Coordinated Vulnerability Disclosure
DAC: Discretionary Access Control
DES: Data Encryption Standard
DGA: Data Governance Act

DHS: Department of Homeland Security
DMA: Digital Markets Act
DNS: Domain Name System
DORA: Digital Operational Resilience Act
DPO: Data Privacy Officer
DRP: Disaster Recovery Plan
DS: Digital Service
DSA: Digital Services Act
EC: European Commission
EDA: European Defence Agency
EDPS: European Data Protection Supervisor
EEA: European Economic Area
ENISA: European Union Agency for Cybersecurity
ERP: Enterprise Resource Planning
EU: European Union
EU-CyCLONe: EU-Cyber Crises Liaison Organization Network
FBI: Federal Bureau of Investigation
FTP: File Transfer Protocol
GHDB: Google Hacking Database
GRC: Governance, Risk, and Compliance
HIDS: Host-based Intrusion Detection System
HIPAA: Health Insurance Portability and Accountability Act
HMAC: Hash-based Message Authentication Code
HSM: Hardware Security Module
HVAC: Heating, Ventilation, and Air Conditioning
ICT: Information and Communications Technology
IDEA: International Data Encryption Algorithm
IDS: Intrusion Detection System
IEC: International Electrotechnical Commission
IoC: Indicators of Compromise
IPS: Intrusion Prevention System
IPsec: Internet Protocol Security
IRT: Incident Response Team
ISACs: Information Sharing and Analysis Centers
ISAOs: Information Sharing and Analysis Organizations
ISM: Information Security Manager
ISMS: Information Security Management System
ISO: International Organization for Standardization
ITIL: Information Technology Infrastructure Library
ITSRM²: Information Technology Security Risk Management Methodology

MAC: Mandatory Access Control
MD5: Message Digest 5
MFA: Multi-factor Authentication
MSP: Managed Service Provider
MSSP: Managed Security Service Provider
NAC: Network Access Controller
NAP: Network Access Protection
NCAA: National Cybersecurity Certification Authority
NCSS: National Cybersecurity Strategy
NDA: Non-disclosure Agreements
NIDS: Network Intrusion Detection System
NSA: National Security Agency
NVB: National Vulnerability Database
OJEU: Official Journal of EU
OSSTMM: Open Source Security Testing Methodology Manual
OT: Operational Technology
OTP: One-time Password
PCI DSS: Payment Card Industry Data Security Standard
PECB: Professional Evaluation and Certification Board
PEST: Political, Economic, Social, and Technological
PIDS: Protocol-based Intrusion Detection System
PII: Personally Identifiable Information
PIMS: Privacy Information Management System
PKA: Public Key Authentication
PKI: Public Key Infrastructure
PMO: Program Management Office
POC: Point of Contact
PSD2: Payment Service Directive 2
QTS: Qualified Trust Service
QTSP: Qualified Trust Service Provider
RA: Registration Authority
RASCI: Responsible, Accountable, Supporting, Consulted, and Informed
RBAC: Role-based Access Control
RBG: Random Bit Generator
RCE: Resilience of Critical Entities
RMF: Risk Management Framework
RPO: Recovery Point Objective
RSA: Rivest-Shamir-Adleman
RTO: Recovery Time Objective
SAIR: Situational Awareness and Incident Response

SCRM: Supply Chain Risk Management
SFA: Single-factor Authentication
SHA1: Secure Hash Algorithm 1
SIEM: Security Information and Event Management
SMART: Specific, Measurable, Achievable, Relevant, and Time-bound
SNS: Social Networking Service
SOC: Security Operations Center
SP: Special Publication
SPOC: Single Point of Contact
SQL: Structured Query Language
SSL: Secure Sockets Layer
STE: Security Testing and Evaluation
SWOT: Strengths, Weaknesses, Opportunities, and Threats
TLD: Top-level Domain
TLS: Transport Layer Security
TQM: Total Quality Management
TSP: Trust Service Provider
UEBA: User and Entity Behavior Analytics
VA: Validation Authority
VLAN: Virtual Area Network
VLOP: Very Large Online Platform
VLOSE: Very Large Online Search Engine
VPN: Virtual Private Network
XP: Internet Exchange Point