Table of contents

Detailed agenda of the training course

Day 1 Fundamentals of information security and the role of a CISO

- Organizational structure
- Information security program scope
- Information security program resources
- Information security strategy

Day 2 Information security compliance program, risk management, and security architecture and design

- Organization's security architecture
- Information security systems and infrastructure
- Network infrastructure security and segmentation
- Application security architecture and management
- Encryption technologies
- Software defined networking (SDN)
- Network function virtualization (NFV)
- Zero-trust principle
- SASE and SSE
- Overlay network service
- Multi-cloud architecture

Day 3 Security controls, incident management, and change management

Day 4 Information security awareness, monitoring and measurement, and continual improvement

- 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

- ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO 9000:2015, Quality management systems — Fundamentals and vocabulary
- ISO 10015:2019, Quality management — Guidelines for competence management and people development
- ISO 31000:2018, Risk management — Guidelines
- ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC TS 27100:2020, Information technology — Cybersecurity — Overview and concepts
- NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide
- NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

List of acronyms

ABAC: Attribute-Based Access Control
ACL: Audit Command Language
AES: Advanced Encryption Standard
AI: Artificial Intelligence
ALE: Annual Loss Exposure
ARS: The Argentine Peso
AST: Application Security Testing
AUD: The Australian Dollar
BCMS: Business Continuity Management System
BIA: Business Impact Analysis
C&C Servers: Command and Control Servers
CAB: Change Advisory Board
CCPA: California Consumer Privacy Act
CCTA: Central Communication and Telecommunication Agency
CCTV: Closed Circuit Television
CEO: Chief Executive Officer
CFO: Chief Financial Officer
CIA: Confidentiality, Integrity, and Availability
CIO: Chief Information Officer
CIS: Center for Internet Security
CISA: Cybersecurity and Infrastructure Security Agency
CISO: Certified Information Security Officer
CMDB: Configuration Management Database
COBIT: Control Objectives for Information and Related Technologies
CRAMM: CCTA Risk Analysis and Management Method
CRM: Customer Relationship Management
CSA: Cloud Security Alliance
CSE: Communications Security Establishment
CTO: Chief Information Technology
DAC: Discretionary Access Control
DAD: Disclosure, Alteration, Denial
DAST: Dynamic Application Security Testing
DDoS: Distributed Denial-of-Service
DES: Data Encryption Standard
DLP: Data Loss Prevention
DoS: Denial of Service
DPO: Data Privacy Officer
E2EE: End-to-End Encryption

EDR: Endpoint Detection and Response
EPHI: Electronic Protected Health Information
ERM: Enterprise Risk Management
EU: European Union
FAIR: Factor Analysis of Information Risk
FDE: Full Disk Encryption
GDPR: General Data Protection Regulation
GLBA: Gramm-Leach-Bliley Act
GRC: Governance, Risk, and Compliance
GSP: Government Security Policy
HIPAA: The Health Insurance Portability and Accountability Act
HMAC: Hash-based Message Authentication Code
HR: Human Resources
IAAA: Identification, Authentication, Authorization, and Accountability
IAM: Identity Access Management
IAST: Interactive Application Security Testing
ICT: Information and Communications Technology
IDP: Intrusion Detection Systems
IDS: Intrusion Detection System
IoT: Internet of Things
IP: Intellectual Property
IPS: Intrusion Prevention System
IRM: Information Resources Management
ISCM: Information Security Continuous Monitoring
ISMS: Information Security Management System
ISO: International Organization for Standardization
IT: Information Technology
ITIL: IT Infrastructure Library
JIT: Just-in-Time
KPI: Key Performance Indicator
LGPD: Lei Geral de Proteção de Dados Pessoais
MAC: Mandatory Access Control
MAC: Media Access Control
MAST: Mobile Application Security Testing
MTTD: Mean Time to Detect
MTTC: Mean Time to Contain
MTTR: Mean Time to Remediate
NDPR: Nigeria Data Protection Regulation
NDR: Network Detection and Response
NFV: Network Function Virtualization

NIS: Network and Information Security
NIST: National Institute of Standards and Technology
NYCRR: New York State Department of Financial Services Cybersecurity Regulation
OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation
OECD: Organization for Economic Co-operation and Development
PCI DSS: The Payment Card Industry Data Security Standard
PECB: Professional Evaluation and Certification Board
PHI: Protected Health Information
PII: Personal Identifiable Information
PIPA: Personal Information Protection Act
PIPEDA: Personal Information Protection and Electronic Documents Act
PKA: Public Key Authentication
PMO: Program Management Officer
POPIA: Protection of Personal Information Act
PR: Public Relations
RADIUS: Remote Authentication Dial-In User Service
RASP: Runtime Application Self-Protection
RBAC: Role-Based Access Control
RCE: Remote Code Execution
RCMP: Royal Canadian Mounted Police
RFC: Request for Change
RMF: Risk Management Framework
RSA: Rivest-Shamir-Adleman
RSO: Reduced-Sign-On
SA: Security Architecture
SABSA: Sherwood applied business security architecture
SASE: Secure Access Service Edge
SAST: Static Application Security Testing
SCA: Software Composition Analysis
SDLC: Software Development Lifecycle
SDN: Software-Defined Networking
SEIM: Security Event Information Management
SGD: The Singapore Dollar
SIEM: Security Information and Event Management
SMART: Specific, Measurable, Attainable, Relevant, and Time-Bound
SMEs: Small and Medium Sized Enterprises
SOC: Security Operations Centre
SOX: Sarbanes-Oxley Act
SSE: Security Service Edge
SSO: Single Sign-On

STAR: Security, Trust, and Assurance Registry
TACACS+: Terminal Access Controller Access-Control System Plus
TND: The Tunisian Dinar
TOGAF: The Open Group Architecture Framework
TRA: Harmonized Threat and Risk Assessment
UIT: Tax Units
USD: United States Dollar
VLAN: Virtual Local Area Networks
VPN: Virtual Private Network
WAF: Web Application Firewall
ZAR: The South African Rand