INDEX



CERTIFIED NIST CYBERSECURITY PROFESSIONAL TRAINING COURSE

Table of contents

I. Detailed agenda of the training course 3
Day 1 3
Day 2 4
Day 3 5
Day 4 6
Day 5 7
II. Standards cited in this training course 8
III. Bibliography 9
IV. List of acronyms 14

I. Detailed agenda of the training course

Day 1 Introduction to NIST cybersecurity standards and principles

Section 1: Training course objectives and structure 5
- General information
- Educational approach
- Agenda of the training course
- Learning objectives
- Examination and certification
- About PECB

Section 2: Frameworks and standards for information security and cybersecurity 17
- Defense Federal Acquisition Regulation Supplement
- Federal Information Security Modernization Act
- ISO/IEC 27000 Series
- CIS Controls
- Payment Card Industry Data Security Standard
- Cloud Security Alliance

Section 3: Introduction to NIST and its role in cybersecurity 30
- Overview of NIST and its mission
- NIST Cybersecurity Framework (CSF)
- Overview of the NIST Special Publication (SP) 800 Series
- Importance and benefits of adhering to NIST guidelines

Section 4: Introduction to cybersecurity 42
- Cybersecurity
- Information security
- CIA triad
- Common cybersecurity threats
- Types of security controls
- Physical, network, application, and cloud security
- Malicious hackers

Section 5: The organization and its context 59
- Cybersecurity governance
- Mission, objectives, values, and strategies
- Cybersecurity objectives
- Internal and external environment
- Key processes and activities

- Interested parties
- Gap analysis

Section 6: Roles, responsibilities, and authorities 78
- Cybersecurity organizational structure
- Cybersecurity program roles and responsibilities
- The RASCI model

Section 7: Cybersecurity policy 110
- Cybersecurity policy development
- The difference between policy and guideline
- Types of policies
- Control, review, and evaluation of the policy

Day 2 Risk management strategy and supply chain risk management

Section 8: Risk management strategy 3
- Overview of the NIST Risk Management Framework (RMF)
- RMF alignment with the SDLC
- RMF steps: prepare, categorize, select, implement, assess, authorize, and monitor

Section 9: Supply chain risk management 36
- Cybersecurity supply chain risk management
- Dimensions of C-SCRM
- Main C-SCRM roles and responsibilities
- Multilevel enterprise-wide risk management
- Essential C-SCRM practices

Section 10: Asset management 53
- Definition of asset
- Categories of assets
- IT asset life cycle
- IT asset management system
- Inventory of information and other associated assets
- Acceptable use of information and other associated assets
- Return of assets
- System component inventory

Section 11: Risk assessment 69
- Applications of risk assessment
- Risk assessment process

- Risk assessment methodology
- Risk models
- Preparing for risk assessment
- Conducting the assessment
- Communicating the results
- Maintaining the assessment

Section 12: improvement 100
- Continual improvement in cybersecurity
- Information security incident response plan
- Cyber Incident response plan
- Disaster recovery plan
- System security plan (SSP)
- Overview of key components of the SSP
- NIST checklist repository

Day 3 Selecting security controls, awareness and training, and continuous monitoring

Section 13: Security control selection 3
- Key considerations for effective control implementation
- Control implementation approaches
- Control structure and organization
- Privacy and security controls

Section 14: Awareness and training 40
- Information security awareness, training, and education
- Literacy training and awareness
- Cybersecurity and privacy learning program (CPLP) life cycle
- Awareness session topics
- Evaluating program success

Section 15: Security measures 61
- System backup
- Information backup
- Types of information backup
- Account management
- Remote access
- Configuration management
- Identification and authorization
- Boundary protection
- Cryptographic key establishment and management

- Protection of information at rest
- System and information integrity
- Media protection
- Personnel security
- Acquisition process

Section 16: Security continuous monitoring 95
- Continuous monitoring
- Key components of continuous monitoring
- Continuous monitoring strategy
- Monitoring methods and tools
- NIST reporting
- Reporting best practices

Day 4 Cybersecurity incident management

Section 17: Incident management and analysis 3
- Information security incident
- NIST SP 800-61 recommendations
- Cybersecurity incident management
- Cyber incident response team (CIRT)
- Security operations center (SOC)
- Incident analysis
- Incident detection systems

Section 18: Incident response, mitigation, and reporting 27
- Responding to cybersecurity events
- Incident mitigation
- Incident reporting
- Incident recording

Section 19: Incident recovery and lessons learned 43
- Incident recovery plan execution
- Recovery of assets and backups
- Incident recovery plan completion and communication
- Contingency planning process
- Lessons learned
- Incident response training
- Disaster recovery planning

Section 20: Closing of the training course 81
- PECB certification scheme
- Attestation of course completion
- PECB certification process
- Other PECB services
- Other PECB training courses and certifications

Day 5 Certification exam

II. Standards cited in this training course

- ISO 55000:2024, Asset management — Vocabulary, overview and principles
- 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
- ISO/IEC 27003:2017, Information technology — Security techniques — Information security management systems — Guidance
- ISO/IEC 27032:2023, Cybersecurity — Guidelines for internet security
- ISO/IEC 27035-2:2023, Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response
- ISO/IEC TS 27100:2020, Information technology — Cybersecurity — Overview and concepts
- ISO/IEC TS 27110:2021, Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines
- The NIST Cybersecurity Framework (CSF) 2.0
- NIST SP 1800-5, IT Asset Management
- NIST SP 800-12 Rev. 1, An Introduction to Information Security
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-161 Rev. 1, Cyber Supply Chain Risk Management Practices for Systems and Organizations
- NIST SP 800-171 Rev. 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-50 Rev. 1, Building a Cybersecurity and Privacy Learning Program
- NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations
- NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management : A CSF 2.0 Community Profile
- NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)

III. Bibliography

Section 3: Introduction to NIST and its role in cybersecurity

[1] NIST. "About NIST." Last modified January 11, 2022. https://www.nist.gov/about-nist

[2] NIST. "Questions and Answers." Last modified September 24, 2024. https://www.nist.gov/cyberframework/faqs

[3] Wilson, Bridget. "NIST Compliance & Its Benefits." *NetCov*. Last modified April 28, 2021. https://www.netcov.com/nist-compliance-its-benefits/

Section 4: Introduction to cybersecurity

[1] Von Solms, Rossouw, and Johan Van Niekerk. "From Information Security to Cyber Security" *Computers & Security 38* (2013): 97-102. https://profsandhu.com/cs6393_s20/Solms-Niekerk-2013.pdf

[2] CISCO. "What Is Malware?" Accessed October 29, 2024. https://www.cisco.com/site/us/en/products/security/what-is-malware.html#title-6af94cb24a

[3] IBM. "What Is Social Engineering?" Accessed March 15, 2023. https://www.ibm.com/topics/social-engineering

[4] IBM. "What Are Security Controls?" Accessed March 13, 2023. https://www.ibm.com/topics/security-controls

[5] Maxsenti, Mike. "What Is Physical Security? Overview & How To Reduce Risk." Genea. Accessed March 15, 2023. https://www.getgenea.com/blog/physical-security/

[6] CISCO. "What Is Network Security?" Accessed March 15, 2023. https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

[7] Wmware. "What Is Application Security?" Accessed March 15, 2023. https://www.vmware.com/topics/glossary/content/application-security.html#

[8] Kaspersky. "What Is Cloud Security?" Accessed March 15, 2023. https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security

Section 5: The organization and its context

[1] Australian Institute of Company Directors. "Cyber Security Governance Principles." Last Modified October, 2022. https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/board/cyber-security-governance-principles-web3.pdf

[2] Post, James E., Anne T. Lawrence, and James Weber. *Business and Society: Corporate Strategy, Public Policy and Ethics*. McGraw-Hill/Irwin, 2002.

Section 6: Roles, responsibilities, and authorities

[1] National Cyber Security Centre. "Governance Step Two: Establishing Roles & Responsibilities." Accessed July 4, 2023.

https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-2-Nov-2019.pdf

Section 7: Cybersecurity policy

[1] Australian Government Business. "Create a Cyber Security Policy." Last modified March 7, 2023. https://business.gov.au/online/cyber-security/create-a-cyber-security-policy

[2] Babu. Sabdeeo "What Is a Cybersecurity Policy and How to Create One?" *Small Business Trends*. Last modified August 30, 2022. https://smallbiztrends.com/2022/08/cybersecurity-policy.html

Section 8: Risk management strategy

[1] Zieleniewski, Jan, and Stanisław Szczypiorski. *Principles of Organization and Techniques of Foreign Trade*. PWE. 1963.

[2] NIST. "FIPS 200: Minimum Security Requirements for Federal Information Systems." *National Institute of Standards and Technology (NIST)*, 2006. Accessed February 5, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

Section 10: Asset management

[1] Canadian Center for Cyber Security. "Using Information Technology Asset Management (ITAM) to Enhance Cyber Security – ITSM.10.004." Last modified April 2023. https://www.cyber.gc.ca/en/guidance/using-information-technology-asset-management-itam-enhance-cyber-security-itsm10004

Section 11: Improvement

[1] Chachak, Elias. "Why Continuous Improvement of Cybersecurity in Business Is Essential." *CyberDB*. Accessed August 7, 2023. https://www.cyberdb.co/why-continuous-improvement-of-cybersecurity-in-business-is-essential/

[2] Kiteworks. "System Security Plan." Accessed August 6, 2024. https://www.kiteworks.com/risk-compliance-glossary/system-security-plan/

Section 13: Awareness and training

[1] National Institute of Standards and Technology. "NIST CSF 2.0 Implementation Examples." Last modified February 26, 2024. https://www.nist.gov/system/files/documents/2024/02/21/CSF%202.0%20Implementation%20Examples.pdf

Section 14: Security measures

[1] Nath, Bipasha. "7 Data Backup Best Practices Everyone Should Follow." Geekflare. Last modified November 2, 2022. https://geekflare.com/data-backup-best-practices/

[2] Fellows, Russ, and Paul Crocetti. "Types of Backup Explained: Full, Incremental, Differential, Etc." *Data Backup*, December 14, 2022.

https://www.techtarget.com/searchdatabackup/feature/Full-incremental-or-differential-How-to-choose-the-correct-backup-type

[3] Lewis, Sara. "Differential Backup." *TechTarget*. Accessed November 17, 2021. https://searchdatabackup.techtarget.com/definition/differential-backup

[4] Pemble, Matthew W.A, and Wendy F. Goucher. *The CIO's Guide to Information Security Incident Management*. Auerbach Publications, 2019.

[5] Ikarus. "Account management: The Underestimated Risk of Forgotten User Accounts." Last modified April 10, 2024. https://www.ikarussecurity.com/en/security-news-en/account-management-the-underestimated-risk-of-forgotten-user-accounts/

[6] ManageEninge. "Secure Remote Access: A Complete Guide." Accessed October 19, 2024. https://www.manageengine.com/privileged-session-management/what-is-secure-remote-access.html

[7] European Union Agency for Cybersecurity. "Tips for cybersecurity when working from home." *ENISA*. Accessed March 16, 2022. https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home

[8] RedHat. "What Is Configuration Management?" Last modified June 22, 2023. https://www.redhat.com/en/topics/automation/what-is-configuration-management

[9] Wallix. "Identify, Authenticate, Authorize: The Three Key Steps in Access Security." Accessed October 19, 2024. https://www.wallix.com/identify-authenticate-authorize-the-three-key-steps-in-access-security-2/

[10] Fricke, Jason, and F.Hoover, Andrew. "Cybersecurity Architecture, Part 2: System Boundary and Boundary Protection." *Carnegie Mellon University*. Last modified September 6, 2018. https://insights.sei.cmu.edu/blog/cybersecurity-architecture-part-2-system-boundary-and-boundary-protection/

[11] SSL. "Key Management Best Practices: A Practical Guide." Last modified May 3, 2024. https://www.ssl.com/article/key-management-best-practices-a-practical-guide/

[12] AWS. "Protecting Data at Rest." Accessed October 19, 2024. https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/protecting-data-at-rest.html

[13] PrivacyEngine. "Flaw Remediation." Accessed October 20, 2024. https://www.privacyengine.io/resources/glossary/flaw-remediation/

[14] Wibu Systems. "Protecting the Integrity of Software." Accessed October 24, 2024. https://www.wibu.com/magazine/keynote-articles/article/detail/protecting-the-integrity-of-software.html

[15] National Cyber Security Centre. "Managing Device Firmware." Accessed October 20, 2024. https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/managing-device-firmware

[16] IRS. "Media Sanitization Guidelines." Accessed October 20, 2024. https://www.irs.gov/privacy-disclosure/media-sanitization-guidelines#:~:text=Media%20sanitization%20overview&text=There%20are%20four%20categories%20of,not%20an%20acceptable%20sanitization%20method.

[17] Lord, Nate. "Data Protection: Data In transit vs. Data At Rest." *Fortra*. Last modified May 6, 2023. https://www.digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest

Section 15: Security continuous monitoring

[1] Ward, Lewis. "About Continuous Monitoring in NIST." MCWG. Last modified August 15, 2023. https://mcwg.org/about-continuous-monitoring-in-nist/
[2] Miller, Jason. "IDS vs IPS vs SIEM: What You Should Know."*BitLyft*. Last modified December 15, 2020. https://www.bitlyft.com/resources/ids-vs-ips-vs-siem#
[3] Fruhlinger, Josh. "What Is SIEM? Security Information and Event Management Explained." *CSO*. Last modified March 16, 2022. https://www.csoonline.com/article/2124604/what-is-siem-security-information-and-event-management-explained.html
[4] Palo Alto Networks. "What Is Security Information and Event Management (SIEM)?" Accessed April 24, 2023. https://www.paloaltonetworks.com/cyberpedia/what-is-security-information-and-event-management
[5] Knowledge Base Modules. "NIST User Guide – Reports and Reporting Packages," Accessed August 12, 2024. https://docs.logrhythm.com/kbmodules/docs/nist-user-guide-reports-and-reporting-packages
[6] University of Wisconsin-Madison. "Incident Reporting Best Practices." Accessed October 21, 2024. https://cms.library.wisc.edu/staff/wp-content/uploads/sites/37/2019/10/Incident-report-best-practices.pdf

Section 16: Incident management and analysis

[1] Ward, Lewis. "About Continuous Monitoring in NIST." MCWG. Last modified August 15, 2023. https://mcwg.org/about-continuous-monitoring-in-nist/
[2] Federal Communications Commission. *Cyber Security Planning Guide.* Createspace Independent Pub, 2014.
[3] Diogenes, Yuri, and Erdal Ozkaya. *Cybersecurity — Attack and Defense Strategies: Improve Your Security Posture to Mitigate Risks and Prevent Attackers from Infiltrating Your System*. Birmingham: Packt Publishing, 2022.
[4] IBM. "What Is UEBA?" Accessed July 6, 2023. https://www.ibm.com/topics/ueba

Section 17: Incident response and reporting

[1] Conrad, Eric, Joshua Feldman, and Seth Misenar. *Eleventh Hour CISSP: Study Guide*. Syngress, 2017.
[2] TechTarget. "IT Incident Report." Last modified April, 2023. https://www.techtarget.com/searchitoperations/definition/IT-incident-report

Section 18: Incident recovery and lessons learned

[1] National Institute of Standards and Technology. “The NIST Cybersecurity Framework (CSF) 2.0.” Last modified February 26, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] Canner, Ben. “The Secret to Great Incident Response Is Employee Training.” *Solutions Review*. Last modified October 18, 2019. https://solutionsreview.com/endpoint-security/the-secret-to-great-incident-response-is-employee-training/

[3] IBM. “Section 1. Example: Major Goals of a Disaster Recovery Plan.” Last modified April 14, 2021. https://www.ibm.com/docs/en/i/7.3?topic=edrp-section-1-example-major-goals-disaster-recovery-plan

[4] IBM. “Section 6. Disaster Recovery Procedures.” Last modified April 11, 2023. https://www.ibm.com/docs/en/i/7.3?topic=plan-section-6-disaster-recovery-procedures

[5] IBM. “Section 11. Testing the Disaster Recovery Plan.” Last modified April 11, 2023. https://www.ibm.com/docs/en/i/7.3?topic=plan-section-11-testing-disaster-recovery

IV. List of acronyms

AC: Access Control
AM: Asset Management
AO: Authorizing Official
AT: Awareness and Training
AU: Audit and Accountability
BCP: Business Continuity Plan
BD: Business Development
BIA: Business Impact Analysis
BYOD: Bring Your Own Device
CA: Assessment, Authorization and Monitoring
CAO: Chief Acquisition Officer
CEO: Chief Executive Officer
CIA: Confidentiality, Integrity, Availability
CIO: Chief Information Officer
CIRC: Computer Incident Response Center/Capability
CIRT: CYBER Incident Response Team
CIS: Center for Internet Security
CISO: Chief Information Security Officer
CM: Configuration Management
CMDB: Configuration Management Database
CMMC: Cybersecurity Maturity Model Certification
CONOPS: Concept of Operations
COOP: Continuity of Operations
CP: Contingency Planning
CPLP: Cybersecurity and Privacy Learning Program
CPO: Chief Privacy Officer
CRO: Chief Risk Officer
CSA: Cloud Security Alliance
C-SCRM: Cyber Supply Chain Risk Manager
CSF: Cybersecurity Framework
CSIRT: Computer Security Incident Response Team
CUI: Controlled Unclassified Information
CV: Curriculum Vitae
DDoS: Distributed Denial of Service
DE: Detect
DFARS: Defense Federal Acquires Regulation Supplement
DLP: Data Loss Prevention
DMZ: Demilitarized Zone
DNS: Domain Name System
DNSSEC: DNS Security Extensions
DoD: Department of Defense

DoS: Denial of Service
DRP: Disaster Recovery Plan
EDR: Endpoint Detection and Response
EEPROM: Electrically Erasable Programmable Read-Only Memory
EMP: Electromagnetic Pulse
ERP: Enterprise Resource Planning
FAR: Federal Acquisition Regulation
FIPS: Federal Information Processing Standards
FISMA: Federal Information Security Modernization Act
GV: Govern
HIDS: Host-Based Intrusion Detection Systems
HR: Human Resources
IA: Identification and Authentication
IAM: Identity and Access Management
ID: Identify
IDPS: Intrusion Detection and Prevention Systems
IDS: Intrusion Detection System
IEC: International Electrotechnical Commission
IMT: Incident Management Team
IoT: Internet of Things
I**P:** Internet Protocol
IPS: Intrusion Prevention System
IR: Incident Response
IRT: Incident Response Team
ISCP: Information System Contingency Plan
ISMS: Information Security Management System
ISO: International Organization for Standardization
IT: Information Technology
ITAM: Information Technology Asset Management
ITL: Information Technology Laboratory
LAN: Local Area Network
MA: Maintenance
MDM: Mobile Device Management
MP: Media Protection
MTD: Maximum Tolerable Downtime
MTTF: Mean Time To Failure
NAC: Network Access Control
NAP: Network Access Protection
NIDS: Network-based intrusion detection system
NIST: National Institute of Standards and Technology
NIST-SP: National Institute of Standards and Technology Special Publications
NVD: National Vulnerability Database
OPSEC: Operations Security
OS: Operating System

P2P: Peer-to-Peer
PAM: Privileged Access Management
PCI DSS: The Payment Card Industry Data Security Standard
PDS: Protected Distribution System
PECB: Professional Evaluation and Certification Board
PEST: Political, Economic, Social, and Technological
PII: Personally Identifiable Information
PIV: Personal Identity Verification
PL: Planning
PM: Program Management
PMO: Program Management Office
POA&M: Plan of Action and Milestones
PR: Protect
PS: Personnel Security
PT: PII Processing and Transparency
RA: Risk Assessment
RASCI: Responsible, Accountable, Supporting, Consulted, Informed
RC: Recover
RMF: Risk Management Framework
ROM: Read-Only Memory
RPO: Recovery Point Objective
RS: Respond
RTO: Recovery Time Objective
SA: System and Services Acquisition
SAISO: Senior Agency Information Security Officer
SAOP: Senior Agency Official for Privacy
SC: Supply Chain
SC: System and Communication Protection
SCRM: Supply Chain Risk Management
SCRM: Supply Chain Risk Manager
SDLC: Software Development Life Cycle
SEM: Security Event Management
SI: System and Information Integrity
SIEM: Security Information and Event Management
SIM: Security Information Management
SLAs: Service Level Agreements
SOC: Security Operations Center
SQL: Structured Query Language
SR: Supply Chain Risk Management
SSE: System Security Engineer
SSH: Secure Shell
SSL: Secure Sockets Layer
SSO: Single Sign-On
SSO: System Security Officer

SSP: System Security Plan
STAR: Security, Trust, Assurance, and Risk
SWOT: Strengths, Weaknesses, Opportunities, and Threats
TLS: Transport Layer Security
TT&E: Testing, Training, and Exercises
TTP: Tactics, Techniques and Procedures
UEBA: User and Entity Behaviour Analytics
UPS: Uninterruptible Power Supplies
US: United States
VPN: Virtual Private Network
WAN: Wide Area Netword
ZTNA: Zero Trust Network Access