NIST Cyber Security Professional (NCSP) 800-53 Practitioner

Course outline

Module 1: Introduction to NIST Cyber Security Professional (NCSP) 800-53

Module 1 of the NIST Cyber Security Professional (NCSP) 800-53 Practitioner course provides an introduction to the NIST 800-53 security controls and the associated security requirements. It covers the basics of the security control framework, the purpose of the security controls, and the roles and responsibilities of the NCSP 800-53 Practitioner. It also provides an overview of the security control assessment process and the associated documentation.

Lessons

- Overview of NIST Cyber Security Professional (NCSP) 800-53
- Understanding the NIST Cyber Security Professional (NCSP) 800-53 Framework
- Risk Management and NIST Cyber Security Professional (NCSP) 800-53
- Implementing NIST Cyber Security Professional (NCSP) 800-53 Controls
- Auditing and Assessing NIST Cyber Security Professional (NCSP) 800-53 Compliance
- NIST Cyber Security Professional (NCSP) 800-53 Security Operations
- NIST Cyber Security Professional (NCSP) 800-53 Incident Response
- NIST Cyber Security Professional (NCSP) 800-53 Security Monitoring
- NIST Cyber Security Professional (NCSP) 800-53 Security Awareness
- . NIST Cyber Security Professional (NCSP) 800-53 Security Training

After completing this module, students will be able to:

- Understand the purpose and scope of the NIST Cyber Security Professional (NCSP) 800-53 module.
- Identify the key components of the NIST Cyber Security Professional (NCSP) 800-53 framework.
- Develop an understanding of the security controls and their associated requirements.
- Develop the skills to assess and implement the security controls in the NIST Cyber Security Professional (NCSP) 800-53 framework.

Module 2: Understanding the NIST Cyber Security Framework

Module 2 of the NIST Cyber Security Professional (NCSP) 800-53 Practitioner course provides an in-depth look at the NIST Cyber Security Framework (CSF). It covers the core components of the CSF, including its purpose, structure, and implementation. It also provides an overview of the CSF's risk management approach and how it can be used to identify, assess, and mitigate cyber security risks.

Additionally, the module provides an introduction to the NIST 800-53 security controls and how they can be used to protect an organization's information systems.

Lessons

- Overview of the NIST Cyber Security Framework
- Understanding the NIST Cyber Security Framework Core
- Identifying and Assessing Cyber Security Risks
- Developing and Implementing Cyber Security Controls
- Monitoring and Responding to Cyber Security Events
- Improving Cyber Security Posture
- Understanding the NIST Cyber Security Framework Implementation Tiers
- Understanding the NIST Cyber Security Framework Profiles
- Understanding the NIST Cyber Security Framework Subcategories
- . Understanding the NIST Cyber Security Framework Mapping
- . Understanding the NIST Cyber Security Framework Assessment Process
- . Understanding the NIST Cyber Security Framework Reporting Requirements
- . Understanding the NIST Cyber Security Framework Compliance Requirements
- . Understanding the NIST Cyber Security Framework Risk Management Process
- . Understanding the NIST Cyber Security Framework Security Controls
- . Understanding the NIST Cyber Security Framework Security Monitoring
- . Understanding the NIST Cyber Security Framework Security Incident Response
- . Understanding the NIST Cyber Security Framework Security Awareness Training
- . Understanding the NIST Cyber Security Framework Security Auditing
- . Understanding the NIST Cyber Security Framework Security Governance

After completing this module, students will be able to:

- Identify the core components of the NIST Cyber Security Framework and their purpose.
- Explain the relationship between the NIST Cyber Security Framework and the NIST 800-53 security controls.
- Analyze the NIST Cyber Security Framework and the NIST 800-53 security controls to identify potential security gaps.
- Develop a plan to implement the NIST Cyber Security Framework and the NIST 800-53 security controls to protect an organization’s information systems.

Module 3: Risk Management and Security Controls

Module 3 of the NIST Cyber Security Professional (NCSP) 800-53 Practitioner course focuses on risk management and security controls. It covers topics such as risk assessment, security control selection, implementation, and monitoring. It also provides an overview of the NIST Risk Management Framework and the NIST Security Controls Framework. This module provides the knowledge and skills necessary to effectively manage and secure an organization's information systems.

Lessons

- Understanding the NIST Cyber Security Framework
- Risk Identification and Analysis

- Security Control Selection and Implementation
- Security Control Monitoring and Maintenance
- Security Control Documentation
- Security Control Automation
- Security Control Testing and Evaluation
- Security Control Auditing
- Security Control Reporting
- . Security Control Compliance
- . Security Control Risk Management
- . Security Control Incident Response
- . Security Control Disaster Recovery
- . Security Control Business Continuity Planning
- . Security Control Security Awareness Training

After completing this module, students will be able to:

- Understand the principles of risk management and security controls as outlined in NIST 800-53.
- Develop a risk management plan to identify, assess, and mitigate risks associated with an organization’s information systems.
- Implement security controls to protect the confidentiality, integrity, and availability of an organization’s information systems.
- Monitor and evaluate the effectiveness of security controls to ensure they are meeting the organization’s security objectives.

Module 4: Implementing NIST 800-53 Security Controls

Module 4 of the NCSP 800-53 Practitioner course focuses on the implementation of NIST 800-53 security controls. It covers topics such as the purpose of security controls, the different types of security controls, and how to implement them. It also provides guidance on how to assess the effectiveness of security controls and how to document the results. Finally, it provides an overview of the NIST 800-53 security control framework and how it can be used to ensure the security of an organization's information systems.

Lessons

- Understanding NIST 800-53 Security Controls
- Implementing NIST 800-53 Security Controls
- Assessing NIST 800-53 Security Controls
- Documenting NIST 800-53 Security Controls
- Auditing NIST 800-53 Security Controls
- Reporting on NIST 800-53 Security Controls
- Maintaining NIST 800-53 Security Controls
- Troubleshooting NIST 800-53 Security Controls
- Developing NIST 800-53 Security Control Strategies
- . Evaluating NIST 800-53 Security Controls

After completing this module, students will be able to:

- Understand the purpose and scope of NIST 800-53 security controls.
- Identify the different types of security controls and their associated requirements.
- Develop a plan to implement NIST 800-53 security controls in an organization.
- Evaluate the effectiveness of the implemented security controls and make necessary adjustments.

Module 5: Auditing and Assessing NIST 800-53 Security Controls

Module 5 of the NCSP 800-53 Practitioner course covers the fundamentals of auditing and assessing NIST 800-53 security controls. It provides an overview of the NIST 800-53 security control framework, as well as guidance on how to audit and assess the security controls. The module also covers the importance of documenting and reporting on the results of the audit and assessment.

Lessons

- Overview of NIST 800-53 Security Controls
- Understanding the NIST 800-53 Security Control Categories
- Assessing the Effectiveness of NIST 800-53 Security Controls
- Auditing NIST 800-53 Security Controls
- Developing an Audit Plan for NIST 800-53 Security Controls
- Implementing NIST 800-53 Security Controls
- Documenting NIST 800-53 Security Controls
- Reporting on NIST 800-53 Security Controls
- Troubleshooting NIST 800-53 Security Controls
- . Best Practices for NIST 800-53 Security Controls

After completing this module, students will be able to:

- Understand the purpose and scope of NIST 800-53 security controls.
- Identify the different types of security controls and their associated requirements.
- Develop an audit plan to assess the effectiveness of security controls.
- Analyze audit results and recommend corrective actions to improve security posture.

Module 6: Security Operations and Incident Response

Module 6 of the NIST Cyber Security Professional (NCSP) 800-53 Practitioner course focuses on security operations and incident response. It covers topics such as security operations, incident response planning, incident response processes, and incident response tools. It also provides guidance on how to respond to security incidents, how to investigate and analyze incidents, and how to develop and implement incident response plans.

Lessons

- Understanding the NIST Cyber Security Framework
- Developing a Security Operations and Incident Response Plan
- Implementing Security Monitoring and Detection
- Investigating and Responding to Security Incidents
- Developing and Maintaining a Security Operations and Incident Response Team

- Establishing and Maintaining Security Operations and Incident Response Processes
- Understanding the Role of Automation in Security Operations and Incident Response
- Developing and Maintaining Security Operations and Incident Response Documentation
- Understanding the Role of Third-Party Security Operations and Incident Response Services
- . Understanding the Role of Legal and Regulatory Requirements in Security Operations and Incident Response

After completing this module, students will be able to:

- Identify and respond to security incidents in accordance with NIST 800-53 security controls.
- Develop and implement security operations processes and procedures to ensure compliance with NIST 800-53 security controls.
- Utilize security operations tools and techniques to detect, investigate, and respond to security incidents.
- Analyze security incidents to determine root cause and develop remediation plans.

Module 7: Security Monitoring and Reporting

Module 7 of the NIST Cyber Security Professional (NCSP) 800-53 Practitioner course focuses on security monitoring and reporting. It covers topics such as the importance of monitoring and reporting, the different types of security monitoring, and the different types of security reports. It also covers the process of creating and maintaining security reports, as well as the different types of security metrics and how to use them. Finally, it covers the different types of security alerts and how to respond to them.

Lessons

- Understanding the NIST Cyber Security Framework
- Identifying Security Monitoring and Reporting Requirements
- Implementing Security Monitoring and Reporting Solutions
- Establishing Security Monitoring and Reporting Policies
- Developing Security Monitoring and Reporting Strategies
- Evaluating Security Monitoring and Reporting Performance
- Analyzing Security Monitoring and Reporting Data
- Investigating Security Monitoring and Reporting Incidents
- Responding to Security Monitoring and Reporting Events
- . Reporting Security Monitoring and Reporting Results

After completing this module, students will be able to:

- Understand the importance of security monitoring and reporting in the context of NIST Cyber Security Professional (NCSP) 800-53 Practitioner.
- Identify and implement appropriate security monitoring and reporting tools and techniques.
- Analyze and interpret security monitoring and reporting data.
- Develop and implement security monitoring and reporting policies and procedures.

Module 8: Security Automation and Orchestration

Module 8 of the NIST Cyber Security Professional (NCSP) 800-53 Practitioner course focuses on security automation and orchestration. It covers topics such as the use of automation and orchestration tools to improve security operations, the development of security automation and orchestration processes, and the implementation of security automation and orchestration solutions. The module also provides an overview of the NIST Cybersecurity Framework and its use in security automation and orchestration.

Lessons

- Introduction to Security Automation and Orchestration
- Automating Security Controls with Security Orchestration
- Understanding Security Orchestration and Automation Tools
- Automating Security Incident Response
- Automating Security Monitoring and Logging
- Automating Security Vulnerability Management
- Automating Security Compliance
- Automating Security Risk Management
- Automating Security Threat Intelligence
- . Automating Security Patch Management

After completing this module, students will be able to:

- Understand the principles of security automation and orchestration and how they can be used to improve security operations.
- Develop and implement security automation and orchestration processes to improve security operations.
- Utilize security automation and orchestration tools to automate security operations.
- Monitor and evaluate the effectiveness of security automation and orchestration processes.

Module 9: Security Governance and Compliance

Module 9 of the NIST Cyber Security Professional (NCSP) 800-53 Practitioner course covers Security Governance and Compliance. It provides an overview of the principles of security governance and compliance, including the roles and responsibilities of stakeholders, the importance of risk management, and the development of security policies and procedures. It also covers the implementation of security controls, the monitoring of compliance, and the reporting of security incidents.

Lessons

- Understanding NIST Cyber Security Framework
- Risk Management and Compliance
- Security Governance and Policies
- Security Controls and Assessments
- Security Monitoring and Auditing
- Incident Response and Reporting
- Security Awareness and Training
- Security Architecture and Design
- Security Testing and Evaluation
- . Security Operations and Maintenance

After completing this module, students will be able to:

- Understand the importance of security governance and compliance in the context of NIST Cyber Security Professional (NCSP) 800-53 Practitioner.
- Develop an understanding of the NIST 800-53 security control framework and its components.
- Identify and assess security risks and vulnerabilities associated with NIST 800-53 security controls.
- Develop and implement security policies and procedures to ensure compliance with NIST 800-53 security controls.

Module 10: Security Awareness and Training

Module 10 of the NIST Cyber Security Professional (NCSP) 800-53 Practitioner course focuses on security awareness and training. It covers topics such as the importance of security awareness, the different types of security training, and how to develop and implement an effective security awareness program. It also provides guidance on how to measure the effectiveness of security awareness and training programs.

Lessons

- Introduction to NIST Cyber Security Professional (NCSP) 800-53 Practitioner
- Understanding the NIST Cyber Security Framework
- Risk Management and Security Controls
- Security Awareness and Training
- Developing Security Awareness Programs
- Implementing Security Awareness Training
- Evaluating Security Awareness Training
- Security Awareness Best Practices
- Security Awareness Resources
- . Security Awareness Challenges and Solutions

After completing this module, students will be able to:

- Understand the importance of security awareness and training in an organization.
- Identify the key components of a security awareness and training program.
- Develop and implement a security awareness and training program.
- Evaluate the effectiveness of a security awareness and training program.