NCSF-P
NIST Cybersecurity Framework (NCSF) Practitioner Training

Duration: 2 Days

Course Overview:

The NIST Cybersecurity Framework (NCSF) Practitioner Training course is designed for individuals within an organization who are directly involved in the planning, design, creation, implementation, and or improvement of a cybersecurity program that will follow the principles of the NIST Cybersecurity Framework. Although some aspects of the course are technical, this course also includes risk management, business controls, and other topics that would be of value to staff outside of the traditional technical audience.

This course is suited for individuals working with and overseeing the technology, including CIOs, IT Directors and Managers, IT Security personnel, and IT staff.

This course includes:

- Two-day deep dive into Foundation concepts.
- Focus on designing and implementing (or improving) a cybersecurity program to minimize risks and protect critical assets based on the NIST CSF.
- Provides a detailed analysis of various technical and business controls, including the Center for Internet Security 18 Critical Security Controls, the ISO 27001: 2013 Information Security Management System, and the ISO 27002: 2013 Code of Practice.

Prerequisites:

Individuals should have already taken the NIST Cybersecurity Framework (NCSF) Foundation Training course or have significant experience with the NIST Cybersecurity Framework.

Course Outline:

Module 1: Course Introduction

Module 2: Applying NIST CSF Tiers and Profiles

- Review of the NIST CSF major components
- Tiers and Tier Selection
- Current and Target Profiles and the Framework Core

Module 3: An Exploration of Informative References

- Defining the major Informative References
- CIS Controls v8
- ISO/IEC 27001:2013
- NIST SP 800-53 Rev. 5

Module 4: Risk Management in the NIST CSF and NIST RMF

- Risk Management in the NIST Cybersecurity Framework
- Analyzing the NIST Risk Management Framework
  - Introduction and History
  - Purpose, Design, and Characteristics
  - Seven Steps
- Prepare
- Categorize System
- Select Controls
- Implement Controls
- Assess Controls
- Authorize System
- Monitor System and Controls
- Integrating the Frameworks

Module 5: Understanding and Defending Against Real World Attacks

- Major Cybersecurity Attacks and Breaches
- MITRE ATT&CK Matrices
- Defense in Depth and the NIST CSF
- Security Operations Center (SOC) activities and Security Information and Event Management (SIEM) solutions in relation to the NIST CSF

Module 6: Assessing Cybersecurity in the Subcategories

- Creating an Assessment Plan
- Assigning Roles and Responsibilities
- Tiers, Threats, Risks, Likelihoods, and Impact

Module 7: Creating a Written Information Security Programs (WISP)

- The Intersection of Business and Technical Controls
- What is a Written Information Security Program (WISP)?
- Creating a WISP Template
- Aligning Current Profile with a WISP

Module 8: A Practitioner's Deep Dive into Creating or Improving a Cybersecurity Program

- Step 1: Prioritize and Scope
  - Identifying organizational priorities
  - Aiding and influencing strategic cybersecurity implementation decisions
  - Determining scope of the implementation
  - Planning for internal adaptation based on business line/process need
  - Understanding risk tolerance
- Step 2: Orient
  - Identifying systems and applications which support organizational priorities
  - Working with compliance to determine regulatory and other obligations
  - Planning for risk responsibility
- Step 3: Create a Current Profile
  - Cybersecurity Assessment options
  - How to measure real world in relation to the Framework
  - Qualitative and quantitative metrics
  - Current Profile and Implementation Tiers
- Step 4: Conduct a Risk Assessment
  - Risk assessment options (3rd party vs internal)
  - Organizational vs. system level risk assessment
  - Risk assessment and external stakeholders

Course Outline (Cont.):

- Step 5: Create a Target Profile
  - Target Profile and Steps 1-4
  - External stakeholder considerations
  - Adding Target Profiles outside the Subcategories
- Step 6: Determine, Analyze, and Prioritize Gaps
  - Defining and determining Gaps
  - Gap analysis and required resources
  - Organizational factors in creating a prioritized action plan
- Step 7: Implement Action Plan
  - Implementation team design from Executives to Technical Practitioners
  - Assigning tasks when priorities conflict
  - Considering compliance and privacy obligations
  - Taking action
  - Reporting and reviewing

Module 9: Continuous Cybersecurity Improvement

- Creating a continuous improvement plan
- Implementing ongoing assessments