Course Outline

NIST Cybersecurity Framework (NCSF) Practitioner

Course Summary

Description

The two-day NIST Cybersecurity Practitioner 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 guidance for a continuous cybersecurity improvement plan.

Topics

- Course Introduction
- Risk Management in The NIST CSF And NIST RMF
- The Components of The NIST Cybersecurity Framework
- Defense In-Depth and The NIST Cybersecurity Framework
- Assessing Cybersecurity in The Subcategories
- Creating A Written Information Security Program
- A Practitioner's Deep Dive into Creating or Improving A Cybersecurity Program
- Continuous Cybersecurity Improvement

Audience

The 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.

Prerequisites

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

Duration

Two days

Course Outline

NIST Cybersecurity Framework (NCSF) Practitioner

Course Outline

I. Course Introduction
- A. Provides the student with information relative to the course and the conduct of the course in the classroom, virtual classroom, and course materials.

II. Risk Management In The NIST CSF And NIST RMF
- A. Risk Management in the NIST Cybersecurity Framework
- B. Analyzing the NIST Risk Management Framework
- C. Introduction and History
- D. Purpose and Use Cases
- E. Six Steps
  1. Categorize System
  2. Select Controls
  3. Implement Controls
  4. Assess Controls
  5. Authorize System
  6. Monitor Controls
- F. Integrating the Frameworks

III. Real World Attacks
- A. Major Cybersecurity Attacks and Breaches
- B. Cyber Kill Chain
- C. Mitre ATT&CK Matrix

IV. The Components Of The NIST Cybersecurity Framework
- A. Tiers and Tier selection
- B. Current and Target Profiles and the Framework Core
- C. Deep dive in Informative References
- D. Center for Internet Security 20 Critical Security Controls
- E. ISO 27001:2013 Information Security Management System (ISMS)
- F. ISO 27002:2013 Code of Practice
- G. Supply Chain Risk Management in the Enterprise

V. Defense In-Depth And The NIST Cybersecurity Framework
- A. Informative References, Subcategories, and Defense in Depth
- B. Aligning vendor Controls with Subcategories
- C. Security Operations Center (SOC) activities and Security Information and Event Management solutions in relation to the Framework

VI. Assessing Cybersecurity In The Subcategories
- A. Creating an Assessment Plan
- B. Assigning Roles and Responsibilities
- C. Tiers, Threats, Risks, Likelihoods, and Impact

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

VIII. A Practitioner's Deep Dive Into Creating Or Improving A Cybersecurity Program
- A. Step 1: Prioritize and Scope
  1. Identifying organizational priorities
  2. Aiding and influencing strategic cybersecurity implementation decisions
  3. Determining scope of the implementation
  4. Planning for internal adaptation based on business line/process need
  5. Understanding risk tolerance
- B. Step 2: Orient
  1. Identifying systems and applications which support organizational priorities
  2. Working with compliance to determine regulatory and other obligations
  3. Planning for risk responsibility

Course Outline (cont'd)

C. Step 3: Create a Current Profile
   1. Assessing – self vs. 3rd party
   2. How to measure real world in relation to the Framework
   3. Qualitative and quantitative metrics
   4. Analysis of the Current State in a sample assessment
   5. Implementation Tiers in practice
   6. Current Profile and Implementation Tiers

D. Step 4: Conduct a Risk Assessment
   1. Risk assessment options (3rd party vs internal)
   2. Organizational vs. system-level risk assessment
   3. Risk assessment and external stakeholders

E. Step 5: Create a Target Profile
   1. Target Profile and Steps 1-4
   2. Determining desired outcomes with Tiers
   3. External stakeholder considerations
   4. Adding Target Profiles outside the Subcategories

F. Step 6: Determine, Analyze, and Prioritize Gaps
   1. Defining and determining Gaps
   2. Gap analysis and required resources
   3. Organizational factors in creating a prioritized action plan

G. Step 7: Implement Action Plan
   1. Implementation team design from Executives to Technical Practitioners
   2. Assigning tasks when priorities conflict
   3. Considering compliance and privacy obligations
   4. Taking action
   5. Reporting and reviewing

IX. Continuous Cybersecurity Improvement

A. Creating a continuous improvement plan
B. Implementing ongoing assessments