NCSF Foundation

The NCSF Foundation training course outlines current cybersecurity challenges and explains how organizations who implement a NCSF program can mitigate these challenges.

Length Days: 1 / Length Hours: 8

TARGET AUDIENCE

Targeted at IT and Cybersecurity professionals looking to become certified on how to operationalize the NIST Cybersecurity Framework (NCSF) across an enterprise and its supply chain.

COURSE OBJECTIVES

This course introduces the NIST Cybersecurity Framework (NIST CSF). The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities. This course discusses how an organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk.

COURSE OUTLINE

1 - COURSE INTRODUCTION

Provides the student with information relative to the course and the conduct of the course in the classroom, virtual classroom and online self-paced. The introduction also covers the nature and scope of the examination.

2 - DOING BUSINESS IN THE DANGER ZONE

Discusses the current state of cybersecurity in the context of today's threat landscape and what organizations must do in order to ask and answer the question, "Are we secure?"

3 - RISK-BASED APPROACH

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance. With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

4 - THE NIST CYBERSECURITY FRAMEWORK FUNDAMENTALS

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities. These components are explained in the remainder of the course.

5 - CORE FUNCTIONS, CATEGORIES & SUBCATEGORIES

The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

6 - IMPLEMENTATION TIERSIMPLEMENTATION TIERS

Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

7 - DEVELOPING FRAMEWORK PROFILES

A Framework Profile ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

8 - CYBERSECURITY CONTROLS FACTORYTM MODEL

This model, developed by Larry Wilson, CSIO at UMass, President's Office, provides an approach for an organization to operationalization of the 20 Critical Security Controls within the NIST CSF within the context of the NIST CSF.

9 - CYBERSECURITY IMPROVEMENT

The NIST CSF also provides a 7-step approach for the implementation and improvement of their cybersecurity posture utilizing the NIST CSF. The 7-steps include:

Step 1: Prioritize and Scope.

The organization identifies its business/mission objectives and high-level organizational priorities.

Step 2: Orient.

The organization identifies related systems and assets, regulatory requirements, and overall risk approach and then identifies threats to, and vulnerabilities of, those systems and assets.

Step 3: Create a Current Profile.

The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

Step 4: Conduct a Risk Assessment.

The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization.

Step 5: Create a Target Profile.

The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes.

Step 6: Determine, Analyze, and Prioritize Gaps.

The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile.

Step 7: Implement Action Plan.

The organization determines which actions to take in regards to the gaps, if any, identified in the previous step.