

NIST Cybersecurity Professional Foundation

This one-day course discusses how an organization can use the NIST Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment. All NCSF-CFM candidates that are successful in passing the certification exam will receive a verified digital badge that they can post to their LinkedIn profiles.

The NCSP Foundation certification exam is through APMG. Students must pass a 60 minute, 40 question closed book multiple-choice examination with a passing score of 60% in order to receive this certification.

Audience

The program is targeted at IT and Business professionals who need a basic understanding of the NIST Cybersecurity Framework and its role within an organization.

Course Outline

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.

TODAY'S DIGITAL ECONOMY

Today, half the world's population is online, a third is on a social network, 53% are mobile, and they span all ages, races, geographies, and attitudes across the planet. The culmination of this explosion in consumer connectivity is the Digital Economy.

UNDERSTANDING CYBER RISKS

Risk-based strategies go beyond compliance mandates to provide a more holistic approach for securing IT systems and information assets. This approach is based on identifying the most significant risks to the organization and then remediating the highest risks first. A risk-based approach enables the organization to adapt to changes in the threat landscape, vulnerabilities, regulatory and business environments.

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.

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.



NIST Cybersecurity Professional Foundation

IMPLEMENTATION 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.

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.

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 draw upon mission drivers, a cost/benefit analysis, and an understanding of risk to achieve the outcomes in the Target Profile.

Step 7: Implement Action Plan.

NCSF CONTROLS FACTORY 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.



NIST Cybersecurity Professional Foundation

Fees include:



- Training accredited by APMG, delivered by an accredited trainer for the NIST CSF scheme,
- Course workbook including all the slides presented during the course delivery,
- Each chapter will end with a multiple-choice quiz. The student is expected to attain a minimum of 80% passing score. The quizzes will be Blooms Level 1 & 2,
- The NIST Cybersecurity Professional Foundation exam, comprised of 40 multiple choice questions. The exam will be 60 minutes and the passing mark is 60%.