CISSP | CEH | PKI | SECURITY

NCSF-BOOT: NIST Cybersecurity Framework Training – Bootcamp

$3,995.00

- 4 Days
- 32 PDU Credits with this class

Upcoming Dates

Feb 10 - Feb 13
Mar 16 - Mar 19
Apr 06 - Apr 09

Course Description

This 4-day certification boot camp provides a detailed plan for designing and building a cybersecurity program based on the NIST Cybersecurity Framework and its control families (20 Critical Controls, ISO 27002 etc.). The boot camp is based on the NCSF-CFM Foundation and Practitioner certification training programs. The one-day NCSF-CFM Foundation program teaches the fundamentals of the NIST Cybersecurity Framework and the UMass Lowell Controls Factory™ Model. The four-day NCSF-CFM Practitioner program teaches the advanced skills necessary to engineer, operate and manage the business risk of a NIST Cybersecurity Framework program.

The optional certification exam is through APMG. Student must pass a 180 minute, 120 question closed book multiple choice, examination. You must achieve 70 or more correct answers in order to receive this certification.
Credits Earned
• 32 PDU Credits

Course Outline

Foundation Course:

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.

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?"

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.

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.

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.

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.

Cybersecurity Improvement

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

Practitioner Course:

Module 1: Course Overview

Reviews at a high level each chapter of the course

Module 2: Framing the Problem

Reviews the main business and technical issues that we will address through the course.

Chapter 3: The Controls Factory Model

Introduces the concept of a Controls factory model and the three areas of focus, the Engineering Center, the Technology Center, and the

Business Center.

Module 4: The Threats and Vulnerabilities

Provides an overview of cyber –attacks (using the Cyber Attack Chain Model), discusses the top 15 attacks of 2015 and 2016, and the most common technical and business vulnerabilities.

Module 5: The Assets and Identities

Provides a detailed discussion of asset families, key architecture diagrams, an analysis of business and technical roles, and a discussion of governance and risk assessment.

Module 6: The Controls Framework

Provides a detailed analysis of the controls framework based on the NIST Cybersecurity Framework. Includes the five core functions (Identify, Protect, Detect, Respond and Recover).

Module 7: The Technology Controls

Provides a detailed analysis of the technical controls based on the Center for Internet Security 20 Critical Security Controls©. Includes the controls objective, controls design, controls details, and a diagram for each control.

Module 8: The Security Operations Center (SOC)

Provides a detailed analysis of Information Security Continuous Monitoring (ISCM) purpose and capabilities. Includes an analysis of people, process, technology, and services provided by a Security Operations Center.

Module 9: Technical Program Testing and Assurance

Provides a high-level analysis of technology testing capabilities based on the PCI Data Security Standard (DSS). The testing capabilities include all 12 Requirements of the standard.

Module 10: The Business Controls

Provides a high-level analysis of the business controls based on the ISO 27002:2013 Code of Practice. Includes the controls clauses, objective, and implementation overview. The business controls are in support of ISO 27001 Information Security Management System (ISMS).

Module 11: Workforce Development

Provides a review of cybersecurity workforce demands and workforce standards based on the NICE Cybersecurity Workforce Framework(NCWF).

Module 12: The Cyber Risk Program

Provides a review of the AICPA Proposed Description Criteria for Cybersecurity Risk Management. Covers the 9 Description Criteria Categories and the 31 Description Criteria.

Module 13: Cybersecurity Program Assessment

Provides a detailed review of the key steps organizations can use for conducting a Cybersecurity Program Assessment. Assessment results include a technical scorecard (based on the 20 critical controls), an executive report, a gap analysis and an implementation roadmap.

Module 14: Cyber-risk Program Assessment

Provides a review of the Cyber Risk Management Program based on the five Core Functions of the NIST Cybersecurity Framework. This chapter includes a resource guide by the Conference of State Bank Supervisors (CSBS), “Cybersecurity 101 – A Resource Guide for Bank Executives”. Results include a sample business scorecard, executive report, gap analysis and an implementation roadmap.

Audience

The class is designed for IT and Business professionals who will play an active role in the design and management of an NCSF program.

Prerequisites

There are no prerequisites for this course, although basic Security knowledge will be helpful.

What You Will Learn

After completing this course, students will understand:

- Risk-based Approach
- The NIST Cybersecurity Framework Fundamentals
- Core Functions, Categories & Subcategories
- Developing Framework Profiles
- Cybersecurity Controls FactoryTM Model
- Cybersecurity Improvement
- Framing the Problem
- The Controls Factory Model
- The Threats and Vulnerabilities
- The Assets and Identities
- The Controls Framework
- The Technology Controls
- The Security Operations Center (SOC)
- Technical Program Testing and Assurance
- The Business Controls
- Workforce Development
- The Cyber Risk Program
- Cybersecurity Program Assessment
- Cyber-risk Program Assessment