ISC2

NCSF-BOOT: NIST Cybersecurity Framework Boot Camp Training

$3,995.00

- 4 Days

Upcoming Dates

Course Description

The four-day NIST Cybersecurity Bootcamp course is a combination of the NIST Cybersecurity Framework (NCSF) Foundation and Practitioner Training courses. The bootcamp provides a deep dive into the components of the NIST CSF and NIST Risk Management Framework (RMF) and how they align to risk management. The course will follow the principles of the NIST Cybersecurity Framework to design and implement (or improve) a cybersecurity program to protect critical assets. The bootcamp details defense in depth, creation of a Written Information Security Program, and implementing ongoing assessments for a continuous improvement plan.

Course Outline

The Foundation course is organized as follows:

Module 1) Course Introduction

Module 2) The Basics of Cybersecurity

- What is cybersecurity?
- Types of attackers
- Vulnerabilities
- Exploits
- Threats
- Controls
- Frameworks
- Risk-Based Cybersecurity

Module 3) A Holistic Study of the NIST Cybersecurity Framework

- History

  o EO 13636

  o Cybersecurity Enhancement Act of 2014

  o EO 13800

- Uses and Benefits of the Framework
- Attributes of the Framework
- Framework Component Introduction

o Framework Core

o Framework Profiles

o Framework Implementation Tiers

Module 4) Cybersecurity Activities: The Framework Core

- Purpose of the Core
- Core Functions, Categories, and Subcategories
- Informative References

Module 5) Risk Management Considerations: Framework Implementation Tiers

- Purpose of the Tiers
- The Four Tiers
- Components of the Tiers
- Compare and contrast the NIST Cybersecurity Framework with the NIST Risk Management Framework

Module 6) Current and Desired Outcomes: Framework Profiles

- Purpose of the Profiles
- The Two Profiles
- Interrelationships between the Framework Components

Module 7) A Primer on the Seven Step Framework Implementation Process

- Prioritize and Scope
- Orient
- Create a Current Profile
- Conduct a Risk Assessment
- Create a Target Profile
- Determine, Analyze, and Prioritize Gaps
- Implement Action Plan

The Practitioner course is organized as follows:

Module 1) Course Introduction

Module 2) Risk Management in the NIST CSF and NIST RMF

- Risk Management in the NIST Cybersecurity Framework
- Analyzing the NIST Risk Management Framework

i. Introduction and History

ii. Purpose and Use Cases

iii. Six Steps

1. Categorize System
2. Select Controls
3. Implement Controls
4. Assess Controls
5. Authorize System
6. Monitor Controls

- Integrating the Frameworks

Module 3) Real World Attacks

- Major Cybersecurity Attacks and Breaches

- Cyber Kill Chain
- Mitre ATT&CK Matrix

Module 4) Review of the Components of the NIST Cybersecurity Framework

- Tiers and Tier selection
- Current and Target Profiles and the Framework Core
- Deep dive in Informative References

 i. Center for Internet Security 20 Critical Security Controls

 ii. ISO 27001:2013 Information Security Management System (ISMS)

 iii. ISO 27002:2013 Code of Practice

- Supply Chain Risk Management in the Enterprise

Module 5) Defense in Depth and the NIST Cybersecurity Framework

- Informative References, Subcategories, and Defense in Depth
- Aligning vendor Controls with Subcategories
- Security Operations Center (SOC) activities and Security Information and Event Management solutions in relation to the Framework

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 Program

- 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

 1) Step 1: Prioritize and Scope

- a) Identifying organizational priorities
- b) Aiding and influencing strategic cybersecurity implementation decisions
- c) Determining scope of the implementation
- d) Planning for internal adaptation based on business line/process need
- e) Understanding risk tolerance

 2) Step 2: Orient

- a) Identifying systems and applications which support organizational priorities
- b) Working with compliance to determine regulatory and other obligations
- c) Planning for risk responsibility

 3) Step 3: Create a Current Profile

- a) Assessing – self vs. 3rd party
- b) How to measure real world in relation to the Framework

  1. i) Qualitative and quantitative metrics
  2. ii) Analysis of the Current State in a sample assessment
  3. iii) Implementation Tiers in practice

- c) Current Profile and Implementation Tiers

4) Step 4: Conduct a Risk Assessment

- a) Risk assessment options (3rd party vs internal)
- b) Organizational vs. system level risk assessment
- c) Risk assessment and external stakeholders

5) Step 5: Create a Target Profile

- a) Target Profile and Steps 1-4
- b) Determining desired outcomes with Tiers
- c) External stakeholder considerations
- d) Adding Target Profiles outside the Subcategories

6) Step 6: Determine, Analyze, and Prioritize Gaps

- a) Defining and determining Gaps
- b) Gap analysis and required resources
- c) Organizational factors in creating a prioritized action plan

7) Step 7: Implement Action Plan

- a) Implementation team design from Executives to Technical Practitioners
- b) Assigning tasks when priorities conflict
- c) Considering compliance and privacy obligations
- d) Taking action
- e) Reporting and reviewing

Module 9) Continuous Cybersecurity Improvement

- Creating a continuous improvement plan
- Implementing ongoing assessments

Audience

This course is suited for individuals working with and overseeing the cybersecurity of an organization, including CIOs, CISOs, IT Security workforce, and IT Directors/Managers/Personnel.

Prerequisites

There are no prerequisites for this course. Basic computing skills and security knowledge will be helpful.

What You Will Learn