



NIST Cybersecurity Framework (NCSF) Boot Camp Training

COURSE OVERVIEW

The three-day NIST Cybersecurity Bootcamp course is a combination of the NIST Cybersecurity Framework (NCSF) Foundation and Practitioner Training courses. The boot camp 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 boot camp details defense in-depth, creation of a Written Information Security Program, and implementing ongoing assessments for a continuous improvement plan. 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.

COURSE OUTLINE

THE FOUNDATION COURSE IS ORGANIZED AS FOLLOWS:

Module 1: Course Introduction

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

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
 - EO 13636
 - Cybersecurity Enhancement Act of 2014
 - EO 13800
- Uses and Benefits of the Framework
- Attributes of the Framework



- Framework Component Introduction
 - Framework Core
 - Framework Profiles
 - 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

Modules 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

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

Module 2: The Components of the NIST Cybersecurity Framework

- Review of the NIST CSF Major Components
- Tiers and Tier selection
- Current and Target Profiles and the Framework Core
- Informative References
 - Center for Internet Security Controls v8
 - ISO/IEC 27001:2013
 - ISO/IEC 27002:2013
 - NIST SP 800-53 Rev. 5
- Supply Chain Risk Management in the Enterprise



Module 3: Risk Management in the NIST CSF and NIST RMF

- Risk Management in the NIST Cybersecurity Framework
- Analyzing the NIST Risk Management Framework
 - Introduction and History
 - Purpose and Use Cases
 - Six Steps
 - Categorize System
 - Select Controls
 - Implement Controls
 - Assess Controls
 - Authorize System
 - Monitor Controls
 - Integrating the Frameworks

Module 4: Real-World Attacks

- Major Cybersecurity Attacks and Breaches
- Cyber Kill Chain
- MITRE ATTACK Matrices

Module 5: Defense In-Depth and the NIST Cybersecurity Framework

- Defense in Depth and the NIST CSF
- Zero Trust
- 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 Security in the Subcategories

- Creating an Assessment Plan
- Assigning Roles and Responsibilities
- Tiers, Threats, Risks, Likelihoods, and Impact

Module 7: Creating a Written Information Security Programs (WISP)

- 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

- Step 1: Prioritize and Scope
 - Identifying organizational priorities
 - Aiding and influencing strategic cybersecurity implementation decisions
 - Determining scope of the implementation
 - Planning for internal adaptation based on business line/process need
 - Understanding risk tolerance
- Step 2: Orient
 - Identifying systems and applications which support organizational priorities
 - Working with compliance to determine regulatory and other obligations
 - Planning for risk responsibility



- Step 3: Create a Current Profile
 - Cybersecurity Assessment options
 - How to measure real world in relation to the Framework
 - Qualitative and quantitative metrics
 - Current Profile and Implementation Tiers
- Step 4: Conduct a Risk Assessment
 - Risk assessment options (3rd party vs internal)
 - Organizational vs. system-level risk assessment
 - Risk assessment and external stakeholders
- Step 5: Create a Target Profile
 - Target Profile and Steps 1-4
 - External stakeholder considerations
 - Adding Target Profiles outside the Subcategories
- Step 6: Determine, Analyze, and Prioritize Gaps
 - Defining and determining Gaps
 - Gap analysis and required resources
 - Organizational factors in creating a prioritized action plan
- Step 7: Implement Action Plan
 - Implementation team design from Executives to Technical Practitioners
 - Assigning tasks when priorities conflict
 - Considering compliance and privacy obligations
 - Taking action
 - Reporting and reviewing

Module 9: Continuous Cybersecurity Improvement

- Creating a continuous improvement plan
- Implementing ongoing assessments

WHY TRAIN WITH SUNSET LEARNING INSTITUTE?

Sunset Learning Institute (SLI) has been an innovative leader in developing and delivering authorized technical training since 1996. Our goal is to help our customers optimize their technology Investments by providing convenient, high quality technical training that our customers can rely on. We empower students to master their desired technologies for their unique environments.

What sets SLI apart is not only our immense selection of trainings options, but our convenient and consistent delivery system. No matter how complex your environment is or where you are located, SLI is sure to have a training solution that you can count on!

Premiere World Class Instruction Team

- All SLI instructors have a four-year technical degree, instructor level certifications and field consulting work experience
- Sunset Learning has won numerous Instructor Excellence and Instructor Quality Distinction awards since 2012

Enhanced Learning Experience

- The goal of our instructors during class is ensure students understand the material, guide them through our labs and encourage questions and interactive discussions.

Convenient and Reliable Training Experience

- You have the option to attend classes live with the instructor, at any of our established training facilities, or from the convenience of your home or office
- All Sunset Learning Institute classes are guaranteed to run – you can count on us to deliver the training you need when you need it!

Outstanding Customer Service

- You will work with a dedicated account manager to suggest the optimal learning path for you and/or your team
- An enthusiastic student services team is available to answer any questions and ensure a quality training experience

Interested in Private Group Training?

[Contact Us](#)