DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

NIST Cybersecurity Framework (NCSF) Boot Camp

ID OT-NCSF-FPBOOT **Price** US$ 2,995 **Duration** 3 days

Course Overview

The three-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. 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.

Who should attend

The program 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. Basic computing skills and security knowledge will be helpful.

Course Objectives

Outcomes and benefits from this class is a practical approach that students can use to build and maintain comprehensive cybersecurity and cyber-risk management programs.

Detailed 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
    - i. EO 13636

Fast Lane
Consulting & Education Services, Inc.
5565 Centerview Drive, Suite 310, Raleigh, NC 27606
Tel: (919) 674-3100 | Toll Free: (855) 778-7246
Info.US@FastLane.Net

DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

- ii. Cybersecurity Enhancement Act of 2014
- iii. EO 13800

- Uses and Benefits of the Framework
- Attributes of the Framework
- Framework Component Introduction
  - i. Framework Core
  - ii. Framework Profiles
  - iii. 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

- 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: APPLYING NIST CSF TIERS AND PROFILES

- Review of the NIST CSF Major Components
- Tiers and Tier selection
- Current and Target Profiles and the Framework Core

MODULE 3: AN EXPLORATION OF INFORMATIVE REFERENCES

- Defining the major Informative References
- CIS Controls v8
- ISO/IEC 27001:2013
- NIST SP 800-53 Rev. 5

MODULE 4: RISK MANAGEMENT IN THE NIST CSF AND NIST RMF

- Risk Management in the NIST Cybersecurity Framework
- Analyzing the NIST Risk Management Framework
  - a) Introduction and History
  - b) Purpose, Design, and Characteristics
  - c) Seven Steps
- Prepare
- Categorize System
- Select Controls
- Implement Controls
- Assess Controls
- Authorize System

Fast Lane
Consulting & Education Services, Inc.
5565 Centerview Drive, Suite 310, Raleigh, NC 27606
Tel: (919) 674-3100 | Toll Free: (855) 778-7246
Info.US@FastLane.Net

DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

- Monitor System and Controls

Integrating the Frameworks

MODULE 5: UNDERSTANDING AND DEFENDING AGAINST REAL WORLD ATTACKS

- Major Cybersecurity Attacks and Breaches
- MITRE ATT&CK Matrices
- Defense in Depth and the NIST CSF
- Security Operations Center (SOC) activities and Security Information and Event Management (SIEM) solutions in relation to the NIST CSF

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
  - 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
- 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
- Step 3: Create a Current Profile
  - a) Cybersecurity Assessment options
  - b) How to measure real world in relation to the Framework
  - c) Qualitative and quantitative metrics
  - d) Current Profile and Implementation Tiers
- 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
- Step 5: Create a Target Profile
  - a) Target Profile and Steps 1-4
  - b) External stakeholder considerations
  - c) Adding Target Profiles outside the Subcategories
- 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
- 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

Fast Lane
Consulting & Education Services, Inc.
5565 Centerview Drive, Suite 310, Raleigh, NC 27606
Tel: (919) 674-3100 | Toll Free: (855) 778-7246
Info.US@FastLane.Net

Fast Lane

DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

- e) Reporting and reviewing

MODULE 9: CONTINUOUS CYBERSECURITY IMPROVEMENT

- Creating a continuous improvement plan
- Implementing ongoing assessments

Fast Lane
Consulting & Education Services, Inc.
5565 Centerview Drive, Suite 310, Raleigh, NC 27606
Tel: (919) 674-3100 | Toll Free: (855) 778-7246
Info.US@FastLane.Net