NIST-CSF Boot Camp Certification Training (NCSP) With Exam Voucher

Register Online

Schedule

Class Length: 5 Days

G2R = "Guaranteed to Run" | OLL = "Online LIVE"
ILT = "Instructor-Led-Training"

This course is not currently available on the public schedule. Please contact us using the information in the footer below to inquire about future dates or to schedule a private class.

Overview

This course is targeted at IT and Cybersecurity professionals looking to become certified on how to operationalize the NIST Cybersecurity Framework (NCSP) across an enterprise and its supply chain.

Target Audience

This course assumes the student has successfully taken and passed the NCSF Foundation 2.0 course based on the NIST Cybersecurity Framework version 1.1, release April 2018. Following the course introduction, the course provides an introduction to the intersection between digital transformation and cybersecurity, which is followed by an overview of the threat landscape. Following an approach to the implementation of cybersecurity controls, the course delves into an organizational approach to cybersecurity that starts governance, management, and a supportive culture,Finally, the course provides additional guidance for the cybersecurity practitioner to determine the current state, the desired state, and a plan to close the gap – and to do this over and over again to inculcate it into organizational DNA.

Course Objectives

This course looks at the impact of digital transformation on cybersecurity risks, an understanding of the threat landscape, and an approach to the application of cybersecurity controls. It provides guidance for students on the best approach to design and build a comprehensive cybersecurity program. Executives are keenly aware of the risks but have limited knowledge on the best way to mitigate these risks. This course also enables our executives to answer the critical question – Are we secure? The class includes lectures, informative supplemental reference materials, quizzes, exercises, and formal examination. The exercises are a critical aspect of the course; do not skip them. 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.

Course Outline

1 - Digital Transformation

Explores what the Practitioner needs to know about the relationship between digital transformation and cybersecurity
Explain how to determine the impact of cybersecurity on DX.
Explain the relationships between culture and digital transformation from the perspective of a practitioner.
Explain the delivery of value to stakeholders in a DX & cybersecurity environment.
Illustrate the interdependent relationship between cybersecurity and DX.

2 - Threat Landscape

The Practitioner needs to understand what threat actors do and their capabilities.
Compare the evolving attack type impact to the threat environment.
Apply knowledge about the threat landscape to maintain a readiness to respond.
Develop a risk profile based on business impact analysis
Establish the relationship between awareness and training in the continual improvement of cybersecurity posture.
Develop and treat training & awareness as a critical aspect of deterrence
Use knowledge about the threat landscape as a predicate to the adoption and adaptation of your cybersecurity posture.

3 - The Controls

This chapter provides a sample set of controls based on an informative reference.
Understand the purpose goals & objectives for each control.
Characterize & explain the informative reference controls
Discover how to apply the controls in an organizational context.

4 - Adopt & Adapt

Adopt is a decision about governance; adapt is the set of management decisions that result from the decision to adopt.
Distinguish Adopt, Adapt, Management & Governance.
Develop an approach to adoption & adaptation.
Distinguish & demonstrate the impact of organizational culture on developing cybersecurity as a capability.
Develop an assessment approach to define current state.

5 - Adaptive Way of Working

Threat actors are agile and highly adaptive. The cybersecurity Practitioner must develop the same capabilities
Break down what constitutes an adaptive approach.
Characterize & apply the need for crossfunctional teams.
Recognize and prioritize the first steps (get started).
Demonstrate & establish cybersecurity phases.
Break down the impact of the flows.

6 - Rapid Adoption & Rapid Adaptation FastTrack

FastTrack™ is an approach to allow organizations to learn to adapt to an evolving threat landscape rapidly.
Approach: Establish what it takes to adopt CS.
Determine how that impacts management adaptation of CS.
Determine how that impacts the capability to assess.
CS Capability: Determine the gap between existing & needed capabilities.
Establish what must be developed.
Develop appropriate risk management profile.
Discover how cybersecurity impacts people, practice & technology impacts organization.
Differentiate CIS Implementation groups.
Determine appropriate implementation group & approach.
Develop appropriate phase approaches.

7 - CIIS Practice

Cybersecurity is an ongoing game of cat and mouse. Organizations must learn how to inculcate cybersecurity improvement into their DNA.
Break down & develop mechanisms for ongoing cybersecurity improvement that includes developing a learning organization.
Illustrate an improvement plan based on the NIST 7-Step Approach.
Illustrate an improvement plan based on the Improvement GPS
Demonstrate understanding of Cybersecurity Maturity Model Certification
Break down the balancing loop & how it fits into the escalation archetype
Use the Fast Track™ (improvement & implementation) cycles.