NCSF-CFM Practitioner On-Demand

Course Overview

View Course Dates & Register Today

This course details the current cybersecurity challenges plus teaches in depth the UMass Lowell NCSF Control Factory Methodology on how to build, test, maintain and continually improve a cybersecurity program based on the NIST Cybersecurity Framework. This program is focused on candidates who need a detailed understanding of the NCSF to perform their daily roles as cybersecurity engineers, testers or operations professionals.

This course looks at cybersecurity risks and instructs students on the best approach to design and build a comprehensive technology focused cybersecurity program and business focused cyber-risk management program that will minimize risks, and at the same time, protect critical assets. Executives are keenly aware of the risks, but have limited knowledge on the best way to mitigate these risks. We will want to enable executives to answer the key question – Are we secure? **Please Note: NCSF Foundation is a Pre-requisite.**

Who Should Attend

IT and Cybersecurity professionals looking to become certified on how to operationalize the NIST Cybersecurity Framework (NCSF) across an enterprise and its supply chain.

Course Objectives

The NCSF Practitioner program teaches the knowledge to prepare for the NSCF Practitioner exam plus the skills and abilities to design, build, test, manage and improve a cybersecurity program based on the NCSF.

Course Outline

1 Background & Introduction

2 Framing the Problem

Cybersecurity Risks & Controls
Cyber-Risks to Critical Infrastructure
Mitigating Cyber-Risks: Steps 2 – 5

3 The Controls Factory Model

Cybersecurity Controls Model
The Engineering Center
The Technical Center
The Business Center

4 Cyber Threats & Vulnerabilities

Cyber Kill Chain® Model
The Cyber Threat Landscape
Vulnerabilities & Control Deficiencies

NCSF-CFM Practitioner On-Demand

5 Digital Assets, Identities & Business Impact

Securing our Digital Assets
Asset Management
Business Applications
Security Practices
Business Environment
Governance & Risk Assessment
Risk Management & Supply Chain

6 NIST Cybersecurity Framework – Design & Build

NIST CSF: Core Function Mapping

7 Technology Program – Design & Build

The Technology Program
Critical Security Control 01 – 20

8 Security Operations Center (SOC)

Security Operations Overview
SOC Technology
SOC People
SOC Process/Procedures
SOC Services
SOC Options

9 Technology Program Test & Assurance

PCI=DSS Overview & Mapping
Build & Maintain a Secure Network & Systems
Protect Cardholder Data
Maintain a Vulnerability Management Program
Implement Strong Access Control Measures
Regularly Monitor & Test Networks
Maintain an Information Security Policy

10 Business Center Design & Build

Controls Factory Model – Business Center
ISO 27002 Control Clause A.5 to A.18

11 Cyber Workforce Skills Development

The Controls Factory Model – Cyber Workforce Development
Lesson the NICE Workforce Framework (NCWF)
Securely Provision
Operate & Maintain
Oversee & Govern
Protect & Defend
Analyze
Collect & Operate
Investigate

12 Cyber Risk Program Design & Build

Controls Factory Model – Cyber Risk Program
AICPA Description Criteria Categories: 1 to 19

NCSF-CFM Practitioner On-Demand

13 Cybersecurity Program Assessment

Sample Assessment
Cybersecurity Program Summary Design

14 The Risk Management Framework

AICPA Cyber Risk Categories
FTC Compliance with the Framework