NCSP Foundation Certification

Overview

This APMG accredited one day or four hour video training program 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. The NCSP Foundation training course outlines current cybersecurity challenges and explains how organizations who implement a NCSP program can mitigate these challenges.

Body of Knowledge

This course is based on the Framework for Improving Critical Infrastructure Cybersecurity, version 1.1. It was published by the National Institute of Standards & Technology on February 12, 2014.

Course Introduction

This course introduces the NIST Cybersecurity Framework (NIST CSF). The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: Framework Core, Framework Implementation Tiers, and Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities.

This course discusses how an organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The class will include lectures, informative supplemental reference materials, quizzes, and tests. Outcomes and benefits from this class is a fundamental understanding of cybersecurity and the NIST CSF.

Course Outline:

The course is organized as follows:

Course Introduction – provides the student with information relative to the course and the conduct of the course in the classroom, virtual classroom and online self-paced. The introduction also covers the nature and scope of the examination.

Doing Business in the Danger Zone – discusses the current state of cybersecurity in the context of today's threat landscape and what organizations must do in order to ask and answer the question, "Are we secure?"

Risk-based Approach – Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance.

The NIST Cybersecurity Framework Fundamentals – The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities.

Cybersecurity Controls Factory™ Model – This model, developed by Larry Wilson, CSIO at UMass, President's Office, provides an approach for an organization to operationalization of the 20 Critical Security Controls within the NIST CSF within the context of the NIST CSF

Cybersecurity Improvement – The NIST CSF also provides a 7-step approach for the implementation and improvement of their cybersecurity posture utilizing the NIST CSF.

Prerequisites

There are no prerequisites to attend the NCSP Foundation class.

Target Audience

- Candidates looking to pursue a career in Cybersecurity
- IT & Cybersecurity Engineers, Operations and Business Risk professionals
- IT & Cybersecurity Specialists including Developers, Pen Testers, Auditors etc.
- Business Professionals – Lawyers, Accountants, HR, Sales, Marketing etc.

Exam FAQ's

Exam information can be found **here**

Credits Earned

- **8** PDU and CEU Credits