NCSP Practitioner Certification

Overview

This APMG accredited four day or thirteen-hour video training training program is targeted at IT and Cybersecurity professionals looking to become certified on how to operationalize the NIST Cybersecurity Framework (NCSF) across an enterprise and its supply chain. The NCSP 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.

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 looks at cybersecurity risks and instructs students on the best approach to design and build a comprehensive cybersecurity and risk management program based on the NIST Cybersecurity Framework.

The class will include lectures, informative supplemental reference materials, quizzes, exercises and tests. 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 Organization:

The course is organized as follows:

- Chapter 1: Course Overview - Reviews at a high level each chapter of the course
- Chapter 2: Framing the Problem – Reviews the main business and technical issues that we will address through the course.
- Chapter 3: The Controls Factory Model – Introduces the concept of a Controls factory model and the three areas of focus, the Engineering Center, the Technology Center, and the Business Center.
- Chapter 4: The Threats and Vulnerabilities – Provides an overview of cyber –attacks (using the Cyber Attack Chain Model), discusses the top 15 attacks of 2015 and 2016, and the most common technical and business vulnerabilities.
- Chapter 5: The Assets and Identities – Provides a detailed discussion of asset families, key architecture diagrams, an analysis of business and technical roles, and a discussion of governance and risk assessment.

- Chapter 6: The Controls Framework – Provides a detailed analysis of the controls framework based on the NIST Cybersecurity Framework. Includes the five core functions (Identify, Protect, Detect, Respond and Recover).

- Chapter 7: The Technology Controls - Provides a detailed analysis of the technical controls based on the Center for Internet Security 20 Critical Security Controls©. Includes the controls objective, controls design, controls details, and a diagram for each control.

- Chapter 8: The Security Operations Center (SOC) - Provides a detailed analysis of Information Security Continuous Monitoring (ISCM) purpose and capabilities. Includes an analysis of people, process, technology, and services provided by a Security Operations Center.

- Chapter 9: Technical Program Testing and Assurance – Provides a high-level analysis of technology testing capabilities based on the PCI Data Security Standard (DSS). The testing capabilities include all 12 Requirements of the standard.

- Chapter 10: The Business Controls - Provides a high-level analysis of the business controls based on the ISO 27002:2013 Code of Practice. Includes the controls clauses, objective, and implementation overview. The business controls are in support of ISO 27001 Information Security Management System (ISMS).

- Chapter 11: Workforce Development – Provides a review of cybersecurity workforce demands and workforce standards based on the NICE Cybersecurity Workforce Framework (NCWF).

- Chapter 12: The Cyber Risk Program – Provides a review of the AICPA Proposed Description Criteria for Cybersecurity Risk Management. Covers the 9 Description Criteria Categories and the 31 Description Criteria.

- Chapter 13: Cybersecurity Program Assessment – Provides a detailed review of the key steps organizations can use for conducting a Cybersecurity Program Assessment. Assessment results include a technical scorecard (based on the 20 critical controls), an executive report, a gap analysis and an implementation roadmap.

- Chapter 14: Cyber-risk Program Assessment – Provides a review of the Cyber Risk Management Program based on the five Core Functions of the NIST Cybersecurity Framework. This chapter includes a resource guide by the Conference of State Bank Supervisors (CSBS), “Cybersecurity 101 – A Resource Guide for Bank Executives”. Results include a sample business scorecard, executive report, gap analysis and an implementation roadmap.

Prerequisites

Candidates must have completed the NCSP Foundation class and passes the NCSP Foundation exam.

Target Audience

- Candidates looking to pursue a career in Cybersecurity
- IT, Cybersecurity and Digital Transformation Design & Implementation Engineers
- IT, Cybersecurity and Digital Transformation Technical Operations & Business Analysts
- IT, Cybersecurity and Digital Transformation Specialists including Pen Testers, Ethical Hackers, Software & – Application Developers, Auditors, and Investigators

Exam FAQ's

Exam information can be found **here**

Credits Earned

- **24** PDU & 24 CEU Credits