NIST Cybersecurity Professional Practitioner

This three-day 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 our 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 our executives to answer the key question – Are we secure?

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.

The NCSP Practitioner certification exam is through APMG. Students must pass a 120-minute, 65 question closed book multiple-choice examination with a passing score of 60% in order to receive this certification.

Audience

The 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 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

COURSE OVERVIEW

Reviews at a high level of each chapter of the course.

FRAMING THE PROBLEM

Establishes the context and rationale for the adoption and adaptation of the NIST-CSF using the Controls Factory Model.

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.

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.

DIGITAL ASSETS, IDENTITIES AND BUSINESS IMPACT

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.

THE NIST CYBERSECURITY FRAMEWORK

Provides a practitioner level analysis of the control's framework based on the NIST Cybersecurity Framework.

TECHNOLOGY PROGRAM DESIGN AND BUILD

NIST Cybersecurity Professional Practitioner

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.

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.

TECHNOLOGY 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.

BUSINESS PROGRAM DESIGN AND BUILD

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).

CYBER WORKFORCE SKILLS DEVELOPMENT

Provides a review of cybersecurity workforce demands and workforce standards based on the NICE Cybersecurity Workforce Framework (NCWF).

CYBER-RISK MANAGEMENT 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.

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.

CYBER RISK PROGRAM ASSESSMENT

Provides a review of the Cyber Risk Management Program based on the five Core Functions of the NIST Cybersecurity Framework.

Fees include:

- Training accredited by APMG, delivered by an accredited trainer for the NIST CSF scheme,
- Course workbook including all the slides presented during the course delivery,
- Each chapter will end with a multiple-choice quiz. The student is expected to attain a minimum of 80% passing score. Exercises are available for chapters 4 through 12. Each exercise will provide the student an opportunity to analyze a given scenario and apply the knowledge acquired in the previous training and current content to formulate an optimal solution to the problem,
- The NIST Cybersecurity Professional Practitioner exam, comprised of 65 multiple choice questions. The exam will be 120 minutes and the passing mark is 60%.