NCSF Practitioner

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.

Length Days: 4 / Length Hours: 32

TARGET AUDIENCE

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 OBJECTIVES

The optional certification exam is comprised of 100 multiple choice questions. Approximately 60% will be Blooms Level 1 & 2 and the remaining 40% will be Blooms Level 3 & 4. Certification is through ACQUIROS. Student must pass a 180 minute, 100 question closed book multiple choice, examination with a passing score of 70% in order to receive NCSF Practitioner Certification

- Demonstrate knowledge of essential service management concepts and awareness of essential service management techniques.
- List cost, benefits, and possible problems associated with implementing ITIL Service Support and Service Delivery processes.
- Achieve Foundation-level certification, if desired
- Be competent to apply service management essentials and participate in service delivery/support functions in your own work.

COURSE OUTLINE

1 - COURSE OVERVIEW

Reviews at a high level each chapter of the course

2 - FRAMING THE PROBLEM

Reviews the main business and technical issues that we will address through the course.

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.

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.

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.

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).

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.

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.

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.

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).

11 - WORKFORCE DEVELOPMENT

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

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.

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.

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.