NCSF Practitioner Certification

Overview

This ACQUIROS accredited 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 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 Introduction

To realize the positive potential of technology and inspire confidence to achieve innovation through technology, we must collectively manage cyber-risks to an acceptable level. This includes both business risk and technology risks.

Our business goals may include organizing the company to make it more efficient and profitable, or to redefine our target market to three major areas. One of our key business goal will undoubtedly be to reduce the risk of a data breach, the loss of intellectual property, or the compromise of valuable research data. To be successful, we will need a business focused cyber-risk management program.

Our technology goals may include providing the right information, at the right time, in the right format, to the right parties and systems, at the right cost. To understand our security control requirements, we must first identify what the system is supposed to do (aka, the ideal state), and consider the risks associated with our systems, applications and processing environment. To be successful, we will need a technology focused cybersecurity program.

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 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.

Body of Knowledge

The course introduces a “Controls Factory” as a conceptual model that represents a system of controls used to protect our critical assets, by transforming our assets from an unmanaged state to a managed state. The Controls Factory Model (CFM) has three focus areas, the engineering center, the technology center and the business center. The course includes a deep dive of these three areas.

The engineering center includes threats and vulnerabilities, assets and identities, and our controls framework. We use the Lockheed Martin Cyber Kill Chain© to model threats. We examine technical and business vulnerabilities to understand potentially areas of exposure. For assets, we will study endpoints, networks, applications, systems, databases, and information assets. For identities, we look at business and technical identities, roles and permissions. We use the NIST Cybersecurity Framework as our controls framework.

The technology center includes technical controls based on the 20 Critical Security Controls, technology implementation through security product solutions and services, Information Security Continuous Monitoring (ISCM) capability through people, process and technology, and technical controls testing and assurance based on the PCI-Data Security Standard (DSS) standard. The goal is to understand how to design, build and maintain a technology focused security system.

The business center includes the key business / people oriented controls design based on ISO 27002:2013 Code of Practice, implementation (via program, policy and governance), workforce development, testing and assurance based on the AICPA Cyber-risk Management Framework. The goal is to understand how to build a security governance capability that focuses on employees / contractors, management and executives.

Finally, we discuss outcomes which include a cybersecurity (technology based) scorecard and roadmap and a cyber-risk (business based) scorecard and roadmap. These deliverables answer the questions that business and technology executives will ask – Are we secure?

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.

This course will focus on Blooms Level 1 through 4.

Each chapter will end with a multiple choice quiz. The student is expect to attain a minimum of 80% passing score. The quizzes will be Blooms Level 1 & 2.

Each chapter after the course introduction may have one or more exercises. Each exercise will provide the student to analyze a given scenario and apply the knowledge acquired in the previous and current chapters to formulate an optimal solution to the problem. The exercises will be Blooms Level 3 & 4.

Exam Options

The optional certification exam will be 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 this certification.

Credits Earned

- **24** PDU Credits