NCSF-CFM Foundation 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 Foundation training course outlines current cybersecurity challenges and explains how organizations who implement a NCSF program can mitigate these challenges.

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 introduces the NIST Cybersecurity Framework (NIST CSF). 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. These components are explained below.

- The *Framework Core* is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

- Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.
- A *Framework Profile* ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

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.

In addition this course will introduce the cybersecurity Controls Factory™ Model (CFM) developed by Larry Wilson, CISO, UMass President's Office. The CFM provides an organization with an approach to the operationalization of the NIST Cybersecurity Framework based on a modular engineering-based approach. The Controls Factory™ Model has three main areas of focus (called centers).

The Engineering Center (E-Center) utilizes a systems engineering approach that focuses on designing, building and managing complex systems over their life cycles. The systems engineering process begins by discovering the real threats and vulnerabilities that affect critical IT resources and information assets, identify the most likely or highest impact risks, failures that can occur– systems engineering involves finding elegant solutions to these problems. The basis of E-Center solutions is the NIST Cybersecurity Framework.

The Technology Center (T-Center) operationalizes a set of technical controls to identify, protect and detect potential security threats to vulnerable assets. This includes designing, building, managing, monitoring and testing technical solutions through a set of security products and services. A central capability of the technology program is the Security Operations Center where advanced technology

solutions and skilled cybersecurity resources provide a central place for detecting, diagnosing, and remediating online attacks. The basis of T-Center Solutions is the Center for Internet Security (CIS) 20 Critical Security Controls.

The Business Center (B-Center) is where central management of the organization's security policy, program, people and practices occur. The B-Center is based on ISO 27001 Information Security Management System (ISMS) and ISO 27002 Code of Practice for Information Security Management. A definition of Cyber- Workforce skills are established based on the NICE Cybersecurity Workforce Framework (NCWF, which provides employers, employees, educators, students, and training providers with a common language to define cybersecurity work as well as a common set of tasks and skills required to perform cybersecurity work. The AICPA (American Institute of Certified Public Accountants) Description Criteria is used for reviewing the effectiveness of an entity's Cybersecurity Risk Management Program.

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

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.

Body of Knowledge

This course is based on the Framework for Improving Critical Infrastructure Cybersecurity, version 1.0. It was published by the National Institute of Standards & Technology on February 12, 2014.

The **NIST Cybersecurity Framework** (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber-attacks. It "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes." Version 1.0 was published by the US National Institute of Standards and Technology in 2014, originally aimed at operators of critical infrastructure. Is being used by a wide range of businesses and organizations, and helps shift organizations to be proactive about risk management.

A security framework adoption study reported that 70% of the surveyed organizations see NIST's framework as a popular best practice for computer security, but many note that it requires significant investment.

It includes guidance on relevant protections for privacy and civil liberties.

The NIST CSF is designed with the intent that individual businesses and other organizations use an assessment of the business risks they face to guide their use of the framework in a cost-effective way.

The framework is divided into three parts, "Core", "Profile" and "Tiers". The "Framework Core" contains an array of activities, outcomes and references which detail approaches to aspects of cyber security. The "Framework Implementation Tiers" are used by an organization to clarify for itself and its partners how it views cybersecurity risk and the degree of sophistication of its management approach. Finally, a "Framework Profile" is a list of outcomes that an organization has chosen from the categories and subcategories, based on its business needs and individual risk assessments.

An organization typically starts by using the framework to develop a "Current Profile", which describes its current cybersecurity activities and what outcomes it is achieving. It can then develop a "Target Profile", or adopt a baseline profile that has been tailored to better match its critical infrastructure sector or type of organization. It can then take steps to close the gaps between its current profile and its target profile.

NIST CSF also includes references to informative references and can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity. To address that need, the organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices. The Informative References are part of the Body of Knowledge.

Information regarding Informative References may be found at the following locations:

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): http://www.counciloncybersecurity.org
- ANSI/ISA-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*: http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (including updates as of January 15, 2014). http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Course Organization:

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.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

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. These components are explained in the remainder of the course.

Core Functions, Categories & Subcategories – The *Framework Core* is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

Implementation Tiers – Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

Developing Framework Profiles – A *Framework Profile* ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and

Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

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. The 7-steps include:

Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities.

Step 2: Orient. The organization identifies related systems and assets, regulatory requirements, and overall risk approach and then identifies threats to, and vulnerabilities of, those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

Step 4: Conduct a Risk Assessment. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile.

Step 7: Implement Action Plan. The organization determines which actions to take in regards to the gaps, if any, identified in the previous step.

This course will focus on Blooms Level 1 & 2.

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

The certification exam will be comprised of 100 multiple choice questions. The exam will be 90 minutes and the passing mark is 70%.

Exam Options

The optional certification exam will be comprised of 100 Blooms level 1 & 2 multiple choice questions.

Certification is through ACQUIROS. Student must pass a 90 minute, 100 question closed book multiple choice, examination with a passing score of 70% in order to receive this certification.

Credits Earned

- **8** PDU Credits with the one day class
- **16** PDU Credits with the class is combined with a NCSF Simulation class