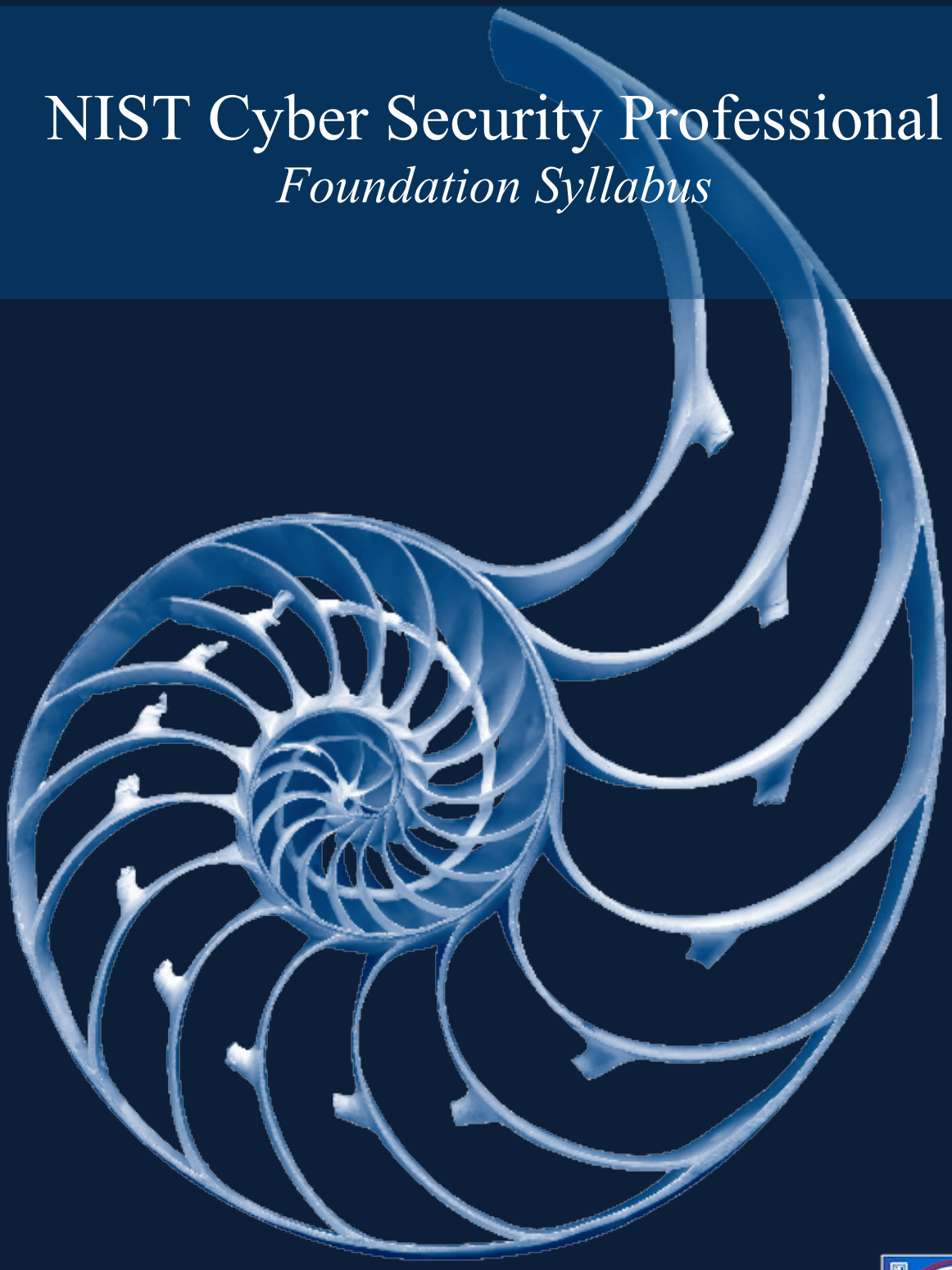
NIST Cyber Security Professional

Foundation Syllabus



Based on NIST-CSF 1.1

itSM904 NCSF Foundation

Syllabus

Version 1.1

April 15, 2019

Based on the NIST Cyber Security Framework 1.1

Contents

Acknowledgements

Publisher

itSM Solution Publishing, LLC
742 Mink Ave. #135
Murrells Inlet, SC 29576

Phone (336) 499-7016

http://www.itsmsolutions.com.

Authors: Larry Wilson & David Nichols

Course Overview

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 an 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. The course is designed for 8 contact hours and a second day of an optional security related simulation game.

Course Contact time by Chapter:

Chapter 01 – Course Introduction	0:15
Chapter 02 – Today's Digital Economy	1:00
Chapter 03 – Understanding Cyber Risks	1:00
Chapter 04 – The NIST Cybersecurity Framework Fundamentals	1:00
Chapter 05 – Core Functions, Categories & Subcategories	1:30
Chapter 06 – Implementation Tiers	0:30
Chapter 07 – Developing Framework Profiles	1:00
Chapter 08 – Cybersecurity Improvement	0:30
Chapter 09 – Cybersecurity Controls Factory Mode	1:15

Blooms Taxonomy

Bloom's Taxonomy provides an important framework for teachers to use to focus on higher order thinking. By providing a hierarchy of levels, this taxonomy can assist teachers in designing performance tasks, crafting questions for conferring with students, and providing feedback on student work. This resource is divided into different levels each with **Keywords** that exemplify the **level** and **questions** that focus on that same critical thinking level. Questions for Critical Thinking can be used in the classroom to develop all levels of thinking within the cognitive domain. The results will be improved attention to detail, increased comprehension and expanded problem-solving skills.

The six levels are:

Level I Knowledge

Level II Comprehension

Level III Application

Level IV Analysis

Level V Synthesis

Level VI Evaluation

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 40 multiple choice questions. The exam will be 60 minutes and the passing mark is 60%.

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 April 16th, 2018.

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. Updated in April of 2018 it expanded its guidance to include external suppliers.

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 Description

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.

Today's Digital Economy – Today, half the world's population is online, a third are on a social network, 53% are mobile, and they span all ages, races, geographies and attitudes across the planet. The culmination of this explosion in consumer connectivity is the Digital Economy.

Understanding Cyber Risks – Risk based strategies go beyond compliance mandates to provide a more holistic approach for securing IT systems and information assets. This approach is based on identifying the most significant risks to the organization, and then remediating the highest risks first. A risk-based approach enables the organization to adapt to changes in threat landscape, vulnerabilities, regulatory and business environments.

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 an 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 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 regard to the gaps, if any, identified in the previous step.

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

NIST-CSF 1.1 Update: 12/2017: Changes to the Course

The following slides have been changed to reflect the current release of the NIST Cybersecurity Framework. The changes primarily adding in two categories and their associated subcategories. Please refer to the latest release to become familiar with the changes.

Slide changes:

- Updated for NIST-CSF 1.1
- Changed focus of introductory chapters to cybersecurity's role in enabling "digital transformation" and understanding risks to our digital assets.
- Swapped the last two chapters and simplified the chapter on the Controls Factory.

Chapter 01 – Course Introduction

Learning Objective	Description	Learning Objective & References
1.0	Introduce and orient the student to the: • Intent • Content • Scope • Methods • Quizzes • Examinations	Runtime: 0:15 Note: The course is designed to be delivered in one day with a second half day simulation game. Exam is 40 questions; 60 minutes and a pass mark is 60%.
	Quiz – Online only	

Chapter 02 – Today's Digital Economy

Learning Objective	Description	Learning Objective and References
2.0	Understand & Explain	Runtime: 1:00
2.1	What cybersecurity is and why it's important	Executive Order 13636—Improving Critical Infrastructure Cybersecurity
2.2	Cybersecurity's impact on the economy	Information Economy: http://www.businessdictionary.com/definition/information-economy.html
2.3	Basic principle of cybersecurity	Introduction to Information Security https://www.us-cert.gov/sites/default/files/publications/infosecuritybasics.pdf
2.4	Critical infrastructure, vulnerabilities & consequences	**Critical Infrastructure Sectors** https://www.dhs.gov/critical-infrastructure-sectors
2.5	What is PPD-21: Presidential Policy Directive & why it's important	**Presidential Policy Directive -- Critical Infrastructure Security and Resilience** https://www.dhs.gov/sites/.../ISC-PPD-21-Implementation-White-Paper-2015-508.pdf
2.6	The Cyber Kill Chain (CKC) & basic cybersecurity principles	Leidos Cyber https://cyber.leidos.com/solutions/cyber-kill-chain
2.7	What are threats, vulnerabilities & assets	
2.8	What is the difference between a threat & a vulnerability	Common Types of Cyber Attacks https://www.rapid7.com/fundamentals/types-of-attacks/
	Quiz – Classroom, Virtual, Online	10 question multiple choice, one right answer. 80% passing mark.

Chapter 03 – Understanding Cyber Risks

Learning Objective	Description	Learning Objective and References
3.0	Understand & explain the terms Risk Asset Vulnerability Threat	Runtime: 1:00 Threats, Vulnerabilities, Risks, Assets https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/
3.1	Determine actions to address risk & opportunities Establish context Establish criteria for risk assessment & acceptance Risk Identify action Analysis & evaluation Treatment (includes avoidance, modification, sharing & retention)	Risk Management process https://www.ausport.gov.au/__data/assets/word.../Risk_Management_process.doc ISO31000:2009
3.1	Understand how to capture, document & manage Risks Treatment plans	
	Quiz – Classroom, Virtual, Online	10 question multiple choice, one right answer. 80% passing mark.

Chapter 04 – The NIST Cybersecurity Framework Fundamentals

Learning Objective	Description	Learning Objective and References
4.0	Understand the NIST Cybersecurity Framework (NIST CSF) • Genesis • Framework core functions • Framework categories & subcategories • Framework implementation tiers • Framework profiles	Runtime: 1:00 Framework for Improving Critical Infrastructure Cybersecurity 1.0
4.1	Understand & explain the NIST CSF objectives • Assess existing cybersecurity program or build one from scratch • Establish cybersecurity goals that align with the business environment	Framework for Improving Critical Infrastructure Cybersecurity 1.0

	• Prioritize opportunities for improvement • Establish a plan for improving or maintaining cybersecurity • Study the critical controls & referenced standards	
	Quiz – Classroom, Virtual, Online	10 question multiple choice, one right answer. 80% passing mark.

Chapter 05 – Core Functions, Categories & Subcategories

Learning Objective	**Description**	**Learning Objective and References**
5.0	Understand & explain the Core Functions • Organize basic cybersecurity activities at their highest level • The 5 Core Functions	Runtime: 1:30 Framework for Improving Critical Infrastructure Cybersecurity 2.0
5.1	Understand & Explain the Framework Categories • Subdivides function in to groups of cyber security outcomes • Tie to programmatic needs & particular activities	Framework for Improving Critical Infrastructure Cybersecurity 2.0, Appendix A
5.2	Understand & Explain the Framework Subcategories • Divide a category into specific outcomes • Technical activities • Management activities	Framework for Improving Critical Infrastructure Cybersecurity 2.0, Appendix A
5.3	Understand & Explain the Informative References • Specific sections of standards, guidelines and practices • Common among critical infrastructure sectors • Illustrate a method to achieve the outcomes associated with each subcategory	Framework for Improving Critical Infrastructure Cybersecurity 2.0, Appendix A
	Quiz – Classroom, Virtual, Online	10 question multiple choice, one right answer. 80% passing mark.

Chapter 06 – Implementation Tiers

Learning Objective	Description	Learning Objective and References
6.0	Understand in general terms NIST CSF Implementation Tiers & their use	Runtime: 0:30 Framework for Improving Critical Infrastructure Cybersecurity 2.0, Appendix A
6.1	Understand the four NIST CSF Implementation Tiers • Tier 1 – Partial • Tier 2 – Risk Informed • Tier 3 – Repeatable • Tier 4 – Adaptive	Framework for Improving Critical Infrastructure Cybersecurity 2.0, Appendix A
6.2	Understand the three risk categories • Risk Management Process • Integrated Risk Management Program • External participation	Framework for Improving Critical Infrastructure Cybersecurity 2.0, Appendix A
	Quiz – Classroom, Virtual, Online	10 question multiple choice, one right answer. 80% passing mark.

Chapter 07 – Developing Framework Profiles

Learning Objective	Description	Learning Objective and References
7.0	Understand in general terms NIST CSF Profiles & their use • Current profile • Target profile	Runtime: 1:00 Framework for Improving Critical Infrastructure Cybersecurity 2.0, Appendix A
7.1	Understand how to determine biggest gaps • Use of current & target profiles across subcategories • How it is used to help identify & prioritize focus areas	Framework for Improving Critical Infrastructure Cybersecurity 2.0, Appendix A
7.2	Understand & demonstrate how to determine profiles through a risk assessment • Prioritize & scope • Orient • Create a current profile • Conduct a risk assessment • Create a target profile	Framework for Improving Critical Infrastructure Cybersecurity 2.0, Appendix A

	• Determine, analyze & prioritize gaps • Implementation action plan.	
	Quiz – Classroom, Virtual, Online	10 question multiple choice, one right answer. 80% passing mark.

Chapter 08 – Cybersecurity Improvement

Learning Objective	Description	Learning Objective and References
9.0	Understand key considerations for beginning a security program	Runtime: 0:30 Framework for Improving Critical Infrastructure Cybersecurity 3.0, Appendix A
9.1	Learn how to integrate cybersecurity into an Information Security Management System (ISMS)	Framework for Improving Critical Infrastructure Cybersecurity 3.0, Appendix A
9.2	Understand how to adopt the NIST Risk Management Framework	Framework for Improving Critical Infrastructure Cybersecurity 3.0, Appendix A
9.3	Learn how to develop organizational capability to continually improve cybersecurity capabilities	Framework for Improving Critical Infrastructure Cybersecurity 3.0, Appendix A
9.4	Understand the expected framework adoption	Framework for Improving Critical Infrastructure Cybersecurity 3.0, Appendix A
9.5	Understand differences between a rules-based approach and a risk based approach	Framework for Improving Critical Infrastructure Cybersecurity 3.0, Appendix A
9.6	Know the differences between risk assessment & compliance assessment	Framework for Improving Critical Infrastructure Cybersecurity 3.0, Appendix A
9.7	Understand the 7-step process organizations use to create a new cybersecurity program or improve an existing program	Framework for Improving Critical Infrastructure Cybersecurity 3.0, Appendix A
	Quiz – Classroom, Virtual, Online	10 question multiple choice, one right answer. 80% passing mark.

Chapter 09 – NCSF Controls Factory™ Model

Learning Objective	Description	Learning Objective and References
8.0	Understand the NCSF Controls Factory Model (CFM)	Runtime: 1:15 See Course Overview
8.1	Learn how the CFM converts assets from • Unmanaged • Managed	See Course Overview
8.2	Understand the purpose, goals, objectives & key capabilities • Engineering center • Technology center • Business center	See Course Overview
8.3	Describe how the NCSF CFM operationalized • NIST-CSF • 20 Critical Controls	Center for Internet Security (CIS) https://www.cisecurity.org/
	Quiz – Classroom, Virtual, Online	10 question multiple choice, one right answer. 80% passing mark.

Quizzes & Examination

Quizzes

Each chapter, except for the Course Introduction chapter will have an end of chapter quiz. The quizzes, found in the course's Checkpoint booklet, will be 10 question, multiple choice, single right answer. A passing mark is 80%. Failure to achieve a passing mark indicates additional study is require. The online course will require a retake of the quiz until a passing mark is achieved.

The Checkpoint booklet will also contain the correct answers along with the question/answer rationale.

Sample Paper

A sample paper is provided for the student to practice a live test paper. Its 40 questions and the student should seek to complete the exam in under an hour. The passing mark is 60%.

Certification Examination

The NCSF Foundation Certification Exam tests the student's knowledge and comprehension of the NIST-CSF, its categories, subcategories, tiers and adoption.

The examination test at a Blooms Level

1. Knowledge
2. Comprehension

The format of the exam is multiple choice, single correct answer. There are 40 questions. The duration of the exam is 60 minutes. The passing mark is 60%.

Prerequisites: It is recommended that the student have a working knowledge of IT (1-2 years).

Appendices

Documents & Links

A Kill Chain Analysis of the 2013 Target Data Breach

The Website: http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf

The NIST cybersecurity Framework.

The website: https://www.nist.gov/cyberframework

The Cyber Kill Chain Framework (Leidos Cyber)

The Website: https://cyber.leidos.com/gaining-the-advantage-applying-cyber-kill-chain-methodology-to-network-defense?

Seven Ways to Apply the Kill Chain (Leidos Cyber)

The Website: https://cyber.leidos.com/seven-ways-to-apply-the-cyber-kill-chain-with-a-threat-intelligence-platform-white-paper

ENISA Threat Landscape 2016

The Website: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

ISO31000:2009 https://www.iso.org/iso-31000-risk-management.html

State of South Carolina: Office of the Inspector General

The Website:
http://oig.sc.gov/Documents/State%20Government%20Information%20Security%20Initiative%20Current%20Situation%20and%20A%20Way%20Forward%20Interim%20Report.pdf

The NIST cybersecurity Framework.

The website: https://www.nist.gov/cyberframework

The NIST cybersecurity Framework.

The website: https://www.nist.gov/cyberframework

The Center for Internet Security 20 Critical Controls.

The website: https://www.cisecurity.org/critical-controls.cfm

SQRRL Threat Hunting Reference Guide

The Website: https://sqrrl.com/threat-hunting-reference-guide/

Building a World-Class Security Operations Center: A Roadmap, Alissa Torres, May 2015

The Website: https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907

NIST 800-61 Computer Security Incident Handling Guide

The Website: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

The Payment Card Industry Data Security Standard.

The Website: https://www.pcisecuritystandards.org/

The ISO 27002:2013 Code of Practice

The website: https://www.iso.org/standard/54533.html

The NICE Cybersecurity Workforce Framework (NCWF)

The Website: http://csrc.nist.gov/nice/framework/

The AICPA Proposed Decision Criteria for Cyber Risk Management

The Website: http://www.aicpa.org/Press/PressReleases/2016/Pages/AICPA-Proposes-Criteria-for-Cybersecurity-Risk-Management.aspx

The Website:
https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/cybersecurity_illustrative_management_description.pdf

The Center for Internet Security 20 Critical Controls.

The website: https://www.cisecurity.org/critical-controls.cfm

Cybersecurity 101 - A Resource Guide for Bank Executives

The Website:
https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf