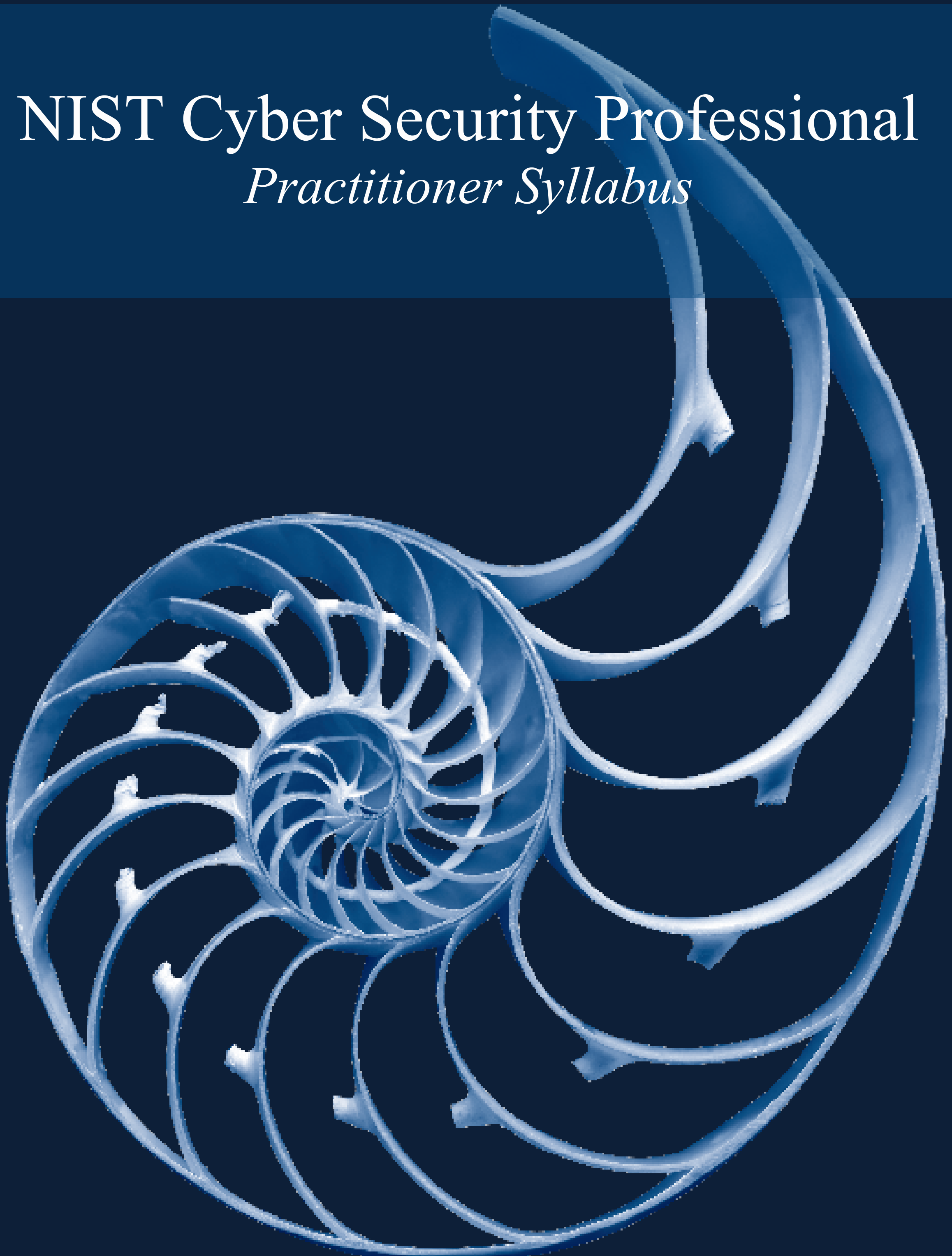
NIST Cyber Security Professional

Practitioner Syllabus



Based on NIST-CSF 1.1

itSM910 NCSF Practitioner

Syllabus

Version 1.1

April 15, 2019

Based on the NIST Cyber Security Framework 1.1

Publisher

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

Phone 401.764.0721

http://www.itsmsolutions.com.

Authors: Larry Wilson & David Nichols

Notice of Rights / Restricted Rights Legend

Notice of Liability

This material is distributed "As Is," without warranty of any kind, either express or implied, respecting the content of this guide, including but not limited to implied warranties for the guide's quality, performance, merchantability, or fitness for any particular purpose. Neither the authors, nor itSM Solutions Publishing LLC, its dealers or distributors shall be liable with respect to any liability, loss or damage caused or alleged to have been caused directly or indirectly by the contents of this material.

Trademarks

Table of Contents

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.

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 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 through 4.

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 exercises will be Blooms Level 3 & 4.

The Practitioner certification exam will be comprised of 65 multiple choice questions. Approximately 60% will be Blooms Level 1 & 2 and the remaining 40% will be Blooms Level 3 & 4. The students will be given 120 minutes to complete the exam. The pass mark is 60%.

The optional Bootcamp certification exam will be comprised of 25 Blooms Level 1 & 2 and 65 Blooms Level 3 & 4 multiple choice questions for a total of 90 questions. The students will be given 150 minutes to complete the exam. The pass mark is 60%

http://www.bloomstaxonomy.org/Blooms%20Taxonomy%20questions.pdf

Body of Knowledge

This course assumes the student has successfully taken and passed the NCSF Foundation course based on the NIST Cyber Security Framework version 1.1, release April 2018.

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 – Establishes the context and rationale for the adoption and adaptation of the NIST-CSF using the Controls Factory Model.
- 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 practitioner level analysis of the controls framework based on the NIST Cybersecurity Framework version 1.1.
- 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.

Part 01 Background & Introduction

Learning Objective	**Description**	**Learning Objective & References**
01.02	**Chapter 02 – Framing the Problem**	
01.02.01	**Lesson – Cybersecurity Risks & Controls**	*Understand, analyze & apply* • How cyber-attacks occur and the three stages of an attack • Cyber Kill Chain (CKC) • Risk equation, threats, vulnerabilities, asset values & controls • Managed vs. unmanaged assets • Concept of a "room of controls (technical & business)
01.02.02	**Lesson – Cyber-Risks to Critical Infrastructure**	• What is "critical infrastructure?' • What is the impact of EO 13800?
01.02.03	**Lesson – Mitigating Cyber-Risks: Step 2 & Step 2**	• How do you mitigate cyber-risks?
01.02.04	**Lesson – Mitigating Cyber-Risk: Step 3**	• How do you mitigate cyber-risks?
01.03.05	**Lesson – Mitigating Cyber-Risks: Steps 4 & Steps 5**	• How do you mitigate cyber-risks?
	Quiz	**How measured 10 Question, Multiple choice, 80% Pass**
01.03	**Chapter 03 – The Controls Factory Model**	
01.03.01	**Lesson – Cybersecurity Controls Model**	• *Understand, analyze and apply appropriate mitigation via the Controls Factory Model* • *Understand, analyze & apply Security Controls* • *Understand technical vs. business controls* • *Understand the NCSF Controls Factory*^{TM} • *Understand how CFM converts unmanaged assets to managed assets* • *Understand the purpose, goals, objectives & key capabilities of: the Engineering, Technology & Business Offices of CFM* • Understand CFM's approach to the development of an organization wide cybersecurity program (consider the technical as well as business deliverables)
01.03.02	**Lesson – The Engineering Center**	• *Analyze threats, vulnerabilities, assets, controls* • *Component 1 – Threat & Vulnerability Area* • *Component 2 – Asset and Identity Area* • *Component 3 – Controls Framework Area*
01.03.03	**Lesson – The Technical Center**	• *Build and maintain the technical solution* • *Component 1 – Technology Program Design & Build* • *Component 2 – Technology Program Operations*

		• *Component 3 – Technology Program Test & Assurance*
01.03.04	**Lesson – The Business Center**	• *Build and maintain the business solution* • *Component 1 – Business Program Design & Build* • *Component 2 – Business Program Workforce Development* • *Component 3 – Business Program Test & Assurance*
	Quiz	How measured 10 Question, Multiple choice, 80% Pass

Part 02 – The Engineering Blueprint

Learning Objective	Description	Learning Objective and References
02.04	**Chapter 04 – Cyber Threats & Vulnerabilities**	
02.04.01	**Lesson – Cyber Kill Chain® Model**	• Understand, analyze & apply the Cyber Attack Model • 7 Stages of the Lockheed Martin Cyber Kill Chain • Mapping cybersecurity controls to the Cyber Kill Chain • Objectives & actions of attacker & defenders for each stage
02.04.02	**Lesson – The Cyber Threat Landscape**	• Understand the cyber threat landscape • Top 15 cyber threats • Typical attack models • Map attack models to the NIST-CSF
02.04.03	**Lesson – Vulnerabilities & Control Deficiencies**	• Understand vulnerabilities & control deficiencies • Top 20 technical vulnerability & applicable controls • Map 5 technical vulnerabilities to the NIST-CSF • Top 14 business vulnerabilities & applicable controls • Map to 14 business vulnerabilities to NIST-CSF
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
	Chapter 04 - Exercise	Blooms Level 3 & 4
02.05	**Chapter 05 – Digital Assets, Identities & Business Impact**	
02.05.01	**Lesson – Securing our Digital Assets**	• Understand the purpose, goals & urgency in securing the organization's digital assets
02.05.02	**Lesson – Asset Management**	• Understand & act on the need to support lifecycle of hardware, software & network configurations & identification of assets
02.05.03	**Lesson – Business Applications**	• Understand how to track relevant hardware & software assets • Control of assets • Systems interfaces • Reporting • Implementation of an ITAM solution
02.05.04	**Lesson – Security Practices**	• Understand an apply security practices for the network, application & information and systems & databases
02.05.05	**Lesson – Business Environment**	• Understand and act on the needs of specific critical sectors • Understand dependencies

		• Risks • Sector specific plans
02.05.06	**Lesson – Governance & Risk Assessment**	• Understand and apply knowledge of protecting organizational assets, conduct of employees, reputation and compliance
02.05.07	**Lesson – Risk Management & Supply Chain**	• Understand organizational priorities, constraints, risk tolerance and assumptions • Support risk decisions associated with managing supply chain risk • Processes need to identify assets and manage supply chain risks
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
	Chapter 05 - Exercise	Blooms Level 3 & 4
02.06	**Chapter 06 – NIST Cybersecurity Framework – Design & Build**	
02.06.01	**Lesson – NIST CSF: Core Function Mapping**	• Understand & apply the NIST-CSF to the • The core functions • The 23 framework categories • The 105 subcategories • Map to the 20 critical controls • Map to ISO 27002 Code of Practice
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
	Chapter 06 - Exercise	Blooms Level 3 & 4

Part 03 – The Technology Blueprint

Learning Objective	Description	Learning Objective and References
03.07	**Chapter 07 – Technology Program – Design & Build**	
03.07.01	**Lesson 07 – The Technology Program**	• Understand, analyze & apply • The technical security controls as it relates to CFM • Where technical controls reside with the cyber-attack model • 20 critical controls & sub controls and how they map to managed assets • 10 controls that protect endpoints & servers • 4 controls that protect networks • 6 controls that protect applications • Application of 20 critical controls to a technology-based cybersecurity program
03.07.02	**Lesson – CSC 01 – 05**	• Critical Security Control 1 • Critical Security Control 2 • Critical Security Control 3 • Critical Security Control 4 • Critical Security Control 5
03.07.03	**Lesson – CSC 06 – 10**	• Critical Security Control 6 • Critical Security Control 7 • Critical Security Control 8 • Critical Security Control 9 • Critical Security Control 10
03.07.04	**Lesson – CSC 11 – 15**	• Critical Security Control 11 • Critical Security Control 12 • Critical Security Control 13 • Critical Security Control 14 • Critical Security Control 15
03.07.05	**Lesson – CSC 16 – 20**	• Critical Security Control 16 • Critical Security Control 17 • Critical Security Control 18 • Critical Security Control 19 • Critical Security Control 20
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
	Chapter 07 - Exercise	Blooms Level 3 & 4
03.08	**Chapter 08** – Security Operations Center (SOC)	

03.08.01	**Lesson – Security Operations Overview**	• Review of SOC technology • Review of SOC people • Review of SOC process • Review of SOC services • Review of SOC options
03.08.02	**Lesson – SOC Technology**	• Understand the application of • Technical requirements for an ISCM capability • Analysis of SOC Technology
03.08.03	**Lesson – SOC People**	• Understand the application of • Personnel requirements for an ISCM capability • Analysis of SOC people
03.08.04	**Lesson – SOC Process/Procedures**	• Understand the application of • Process requirements for an ISCM capability • Analysis of SOC threat hunting process • Analysis of Incident management process
03.08.05	**Lesson – SOC Services**	• Understand the application of • Security Consulting and Testing Services • Managed Network Security Services • Managed Monitoring and Operations Incident Response and Forensics Services
03.08.06	**Lesson – SOC Options**	• Understand the application of • Central Log Management • DIY Security Information and Event management • Managed Security Services • Co-Managed SIEM
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
	Chapter 08 - Exercise	Blooms Level 3 & 4
03.09	**Chapter 09** – Technology Program Test & Assurance	
03.09.01	**Lesson – PCI=DSS Overview & Mapping**	• *Payment Card Industry (PCI) Data Security Standard (DSS) Version 3.2 requirements* • *Test plan for 12 DSS requirements*
03.09.02	**Lesson – Build & Maintain a Secure Network & Systems**	• Requirement 1 - Install and maintain a firewall configuration to protect cardholder data • Requirement 2 - Do not use vendor defaults for passwords and other security parameters
03.09.03	**Lesson – Protect Cardholder Data**	• Requirement 3 - Protect stored cardholder data • Requirement 4 - Encrypt transmission of cardholder data across open, public networks
03.09.04	**Lesson – Maintain a Vulnerability Management Program**	• Requirement 5 - Use and regularly update anti-virus software or programs • Requirement 6 - Develop and maintain secure systems and applications

03.09.05	**Lesson – Implement Strong Access Control Measures**	• Requirement 7 - Restrict access to cardholder data by business need-to-know • Requirement 8 - Assign a unique ID to each person with computer access • Requirement 9 - Restrict physical access to cardholder data
03.09.06	**Lesson – Regularly Monitor & Test Networks**	• Requirement 10 - Track and monitor all access to network resources and cardholder data • Requirement 11 - Regularly test security systems and processes
03.09.07	**Lesson – Maintain an Information Security Policy**	• Requirement 12 - Maintain a policy that addresses information security for employees and contractors
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
	Chapter 09 - Exercise	*Blooms Level 3 & 4*

Part 04 – The Business Blueprint

Learning Objective	Description	Learning Objective and References
04.10	**Chapter 10– Business Center Design & Build**	
04.10.01	**Lesson – Controls Factory Model – Business Center**	• Understand, analyze & apply • Objectives ISO 27001; establish an ISMS • Objectives of ISO 27002:2013; code of practice for information security controls • Relationship between ISO 27001 & ISO 2702 • ISO 27002:2014 & the 14 security control clauses • Primary deliverable & implementation checklist for each ISO control clause • Compare & contrast how controls are accomplished using the CFM and an ISMS
04.10.02	**Lesson – ISO 27002 Control Clause A.5 to A.7**	• ISO 27002 Control Clause A.5 • ISO 27002 Control Clause A.6 • ISO 27002 Control Clause A.7
04.10.03	**Lesson – ISO 27002 Control Clause A.8 to A.9**	• ISO 27002 Control Clause A.8 • ISO 27002 Control Clause A.9
04.10.04	**Lesson – ISO 27002 Control Clause A.10 to A.11**	• ISO 27002 Control Clause A.10 • ISO 27002 Control Clause A.11
04.10.05	**Lesson – ISO 27002 Control Clause A.12 to A.14**	• ISO 27002 Control Clause A.12 • ISO 27002 Control Clause A.13 • ISO 27002 Control Clause A.14
04.10.06	**Lesson – ISO 27002 Control Clause A.15 to A.18**	• ISO 27002 Control Clause A.15 • ISO 27002 Control Clause A.16 • ISO 27002 Control Clause A.17 • ISO 27002 Control Clause A.18
	Chapter 10 - Exercise	Blooms Level 3 & 4 • Replace
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
04.11	**Chapter 11** – Cyber Workforce Skills Development	
04.11.01	**Lesson – The Controls Factory Model – Cyber Workforce Development**	• Understand, analyze & apply Cybersecurity Workforce Demand • Understand NICE Workforce Categories • Understand NICE Specialty Areas
04.11.02	**Lesson the NICE Workforce Framework (NCWF)**	• Understand & discuss the following 7 Workforce Categories, 33 Specialty Areas and 52 work roles

		- Understand Workforce Categories and Specialty Areas
04.11.03	**Lesson – Securely Provision**	- Securely Provision Workforce Category & 7 Specialty Areas
04.11.04	**Lesson – Operate & Maintain**	- Operate and Maintain Workforce Category & 6 Specialty Areas
04.11.05	**Lesson – Oversee & Govern**	- Oversee and Govern Workforce Category & 6 Specialty Areas
04.11.06	**Lesson – Protect & Defend**	- Protect and Defend Workforce Category & 4 Specialty Areas
04.11.07	**Lesson – Analyze**	- Analyze Workforce Category & 5 Specialty Areas
04.11.08	**Lesson – Collect & Operate**	- Collect and Operate Workforce Category & 3 Specialty Areas
04.11.09	**Lesson – Investigate**	- Investigate Workforce Category and two Specialty Areas
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
	Chapter 11 - Exercise	Blooms Level 3 & 4
04.12	**Chapter 12** – Cyber Risk Program Design & Build	
04.12.01	**Lesson – Controls Factory Model – Cyber Risk Program**	- The Proposed AICPA Description Criteria Categories - The Proposed AICPA Description Criteria - What is the proposed AICPA Description Criteria for a Cybersecurity Risk Management Program? - What are the nine key objectives of the AICPA Description Criteria for a Cybersecurity Risk Management Program? - What are the 31 detailed criteria the AICPA Description Criteria for a Cybersecurity Risk Management Program?
04.12.02	**Lesson – AICPA Description Criteria Categories: 1 to 8** - *Nature of Operations* - *Nature of Information at Risk* - *Cybersecurity Risk Management Program Objectives* - *Inherent Risk Related to the Use of Technology*	- AICPA Description Criteria Categories: - Nature of Operations - Nature of Information at Risk - Cybersecurity Risk Management Program Objectives - Inherent Risk Related to the Use of Technology - What are the description criteria, points of focus of the AICPA Description Criteria Categories: - Nature of Operations - Nature of Information at Risk - Cybersecurity Risk Management Program Objectives - Inherent Risk Related to the Use of Technology
04.12.03	**Lesson – AICPA Description Criteria Categories: 9 to 19** - *Cybersecurity Risk Governance Structure*	- AICPA Description Criteria Categories: - Cybersecurity Risk Governance Structure - Cybersecurity Risk Management Process

	• *Cybersecurity Risk Management Process* • *Cybersecurity Communications and the Quality of Cybersecurity Information* • *Monitoring of the Cybersecurity Risk Management Program*	• Cybersecurity Communications and the Quality of Cybersecurity Information • Monitoring of the Cybersecurity Risk Management Program • What are the description criteria, points of focus of the AICPA Description Criteria Categories: • Cybersecurity Risk Governance Structure • Cybersecurity Risk Management Process • Cybersecurity Communications and the Quality of Cybersecurity Information • Monitoring of the Cybersecurity Risk Management Program
	Chapter 12 - Exercise	Blooms Level 3 & 4
	Quiz	How measured 10 Question, Multiple choice, 80% Pass

Part 05 – The Program Deliverables

Learning Objective	Description	Learning Objective and References
05.13	**Chapter 13 – Cybersecurity Program Assessment**	
05.13.01	**Lesson – Cybersecurity Program Assessment**	- Develop Cybersecurity Assessment Program and Scorecard
05.13.01.01	a) Understand the four steps that organizations should take in conducting a cybersecurity program assessment	- What are the four steps of a typical cybersecurity assessment program? - Establish Team Leaders - Define Organizational Goal and Scope - Define Business Goals and Scope - Define Technical Goals and Scope - Assess Business Practices, Risks and Controls - Assess Applications, Risks and Controls - Assess Infrastructure, Risks and Controls - Create a Current State Profile - Create a Target State Profile - Determine, analyze and prioritize gaps - Create a business case - Implement action plan - Executive communication plan - Senior Management / Department Lead communication plan - Mid-level Management communications plan - Technical / Operational lead communication plan
05.13.02	**Lesson – Sample Assessment**	- Conduct sample cybersecurity assessment - What is the process used to conduct a cybersecurity program assessment based on the 20 critical controls?
05.13.03	**Lesson – Cybersecurity Program Summary Design**	- Develop sample executive cybersecurity report - How do you design and communicate an executive presentation that outlines the key results of a cybersecurity assessment?
05.13.03.01	a) Understand how to develop and deliver an executive presentation that outlines the key findings that are discovered by conducting the cybersecurity program assessment	- How do you design and communicate an executive presentation that outlines the key results of a cybersecurity assessment? - How do you document and deliver a report that contains a current state profile, target state profile and cybersecurity scorecard? - How do you evaluate and report on the overall maturity of a cybersecurity program?
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
05.14	**Chapter 14** – The Cyber Risk Program Assessment	

05.14.01	**Lesson – The Risk Management Framework**	• Understand, analyze & apply the 6 steps for completing a risk assessment as defined by NIST in special publication NIST S) 800-37 • Understand, analyze & apply the three inputs to the RISK Management Framework including the Security plan, Security Assessment Report and the Plan of Action and Milestone (POA&M)
05.14.02	**Lesson – AICPA Cyber Risk Categories**	• Understand, analyze & apply how to conduct a cyber risk assessment program based on the AICPA Description Criteria. • Learn, analyze & apply the f steps in developing a cybersecurity program roadmap.
05.14.03	**Lesson – FTC Compliance with the Framework**	• Understand how the Federal Trade Commission (FTC) views compliance with the framework • Understand the Deloitte top 10 Board Recommendations regarding cybersecurity.
	Quiz	How measured 10 Question, Multiple choice, 80% Pass

Appendix A

Documents & Links

Chapter 2: Framing the Problem

A Kill Chain Analysis of the 2013 Target Data Breach

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

Chapter 3: The Controls Factory Model

The NIST cybersecurity Framework.

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

Chapter 4: Threats and Vulnerabilities

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

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

Chapter 5: Digital Assets, Identities and Business Impact

The NIST cybersecurity Framework.

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

Chapter 6: The NIST Cybersecurity Framework

The NIST cybersecurity Framework.

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

Chapter 7: Technology Program Design and Build

The Center for Internet Security 20 Critical Controls.

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

Chapter 8: Security Operations Center (SOC)

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

Chapter 9: Technology Program Testing and Assurance

The Payment Card Industry Data Security Standard.

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

Chapter 10: Business Program Design and Build

The ISO 27002:2013 Code of Practice

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

Chapter 11: Cyber Workforce Skills Development

The NICE Cybersecurity Workforce Framework (NCWF)

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

Chapter 12: Cyber-Risk Management Program

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

Description of XYZ Manufacturing's Cybersecurity Risk Management Program

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

Chapter 13: Cybersecurity Program Assessment

The Center for Internet Security 20 Critical Controls.

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

Chapter 14: Cyber Risk Program Assessment

The NIST cybersecurity Framework.

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

Cybersecurity 101 - A Resource Guide for Bank Executives

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