itSM910 NCSF Practitioner

Syllabus

Version 1.0

April 2017

Publisher

itSM Solution Publishing, LLC
31 South Talbert Blvd #295
Lexington, NC 27292

Phone (336) 243-4876
Fax (336) 499-1172

http://www.itsmsolutions.com.

Authors: Larry Wilson & David Nichols

Notice of Rights / Restricted Rights Legend

Notice of Liability

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 & 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.

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.

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

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.

Part 01 Background & Introduction

Learning Objective	Description	Learning Objective & References
01.02	**Chapter 02 – Framing the Problem**	
01.02.01	**Lesson - Today's Cybersecurity Context**	• *Why is Cybersecurity Important?* • *Key business drivers, areas of growth and security challenges of an information economy* • *What is vulnerable & what are the consequences?*
01.02.01.01	a) Understand why it is important to have a strong security program to protect key digital assets	• *Why is cybersecurity important?* • *How do we build a security organization – Controls Framework* • *What are the technical requirements?* • *Who is responsible for building the capabilities – the Workforce?*
01.02.01.02	b) Understand the innovation economy, benefits & challenges	• *What is the "innovation economy'?* • *How are we impacted by a growing dependence on technology?* • *How do we achieve the maximum potential of an innovation economy?* • *What are the main risks of an innovation economy?*
01.02.01.03	c) Understand basic cybersecurity principles and costs of a data breach	• *Understand the basic cybersecurity principles (confidentiality, integrity, availability, authentication)* • *Understand the cost of a data breach*
01.02.01.04	d) Understand critical infrastructure, vulnerabilities & consequences	• *What is critical infrastructure?* • *What is PPD-21?* • *How is critical infrastructure vulnerable to a cyber-attack?* • *Understand the Communications Sector and the Energy Sector Plans.*
01.02.01.05	e) Understand vulnerabilities and consequences of a security incident	• *How are Automotive Vehicles vulnerable?* • *How are Traffic Light Systems vulnerable?* • *How are Industrial Control Systems vulnerable?* • *How are Medical Devices vulnerable?* • What is the likelihood and impact? • *Who have been breached?*
01.02.02	**Lesson – Understanding Cyber Threats & Vulnerabilities**	• *Purpose, goals & objectives* • *Cyber Attacks, Threats and Vulnerabilities* • *The Cyber Kill Chain©* • *The Target Data Breach Example*
01.02.02.01	a) Understand how cyber threats and vulnerabilities	• *What is a Cyber-Attack?* • *What is a Cyber Threat?* • *What is a Vulnerability?*
01.02.02.02	b) Understand the Cyber Kill Chain©	• *What are the stages of the Cyber Kill Chain©?* • *What happens at each stage* • *How do threats relate to vulnerabilities?*
01.02.02.03	c) Understand the Target Data Breach	• *Understand how the hackers broke into Target* • *Understand Target's Missed Opportunities*

01.02.03	**Lesson -** Understanding Cyber Risks and Controls	• *Purpose, goals and objectives* • *Why IT needs to be controlled* • *The Risk Equation* • *Cybersecurity Vulnerabilities: Knowns and Unknowns* • *The Cyber Attack Model* • *Build a Room of Controls*
01.02.03.01	a) Understand why IT needs to be controlled	• *What are the key business objectives?* • *What are the risks with system and processing environments?* • *What are the unknown risks?*
01.02.03.02	b) Understand the risk equation, threats, vulnerabilities, asset value & controls	• *What is the Risk Equation* • *How do we calculate risk?* • *What are threats, vulnerabilities, assets, controls?*
01.02.02.03	c) Understand known and unknown risks	• *What is the risk of the unknowns?* • *What is the implication of unknown vulnerabilities?*
01.02.02.04	d) Understand the Cyber Attack Model	• *How do controls protect against a cyber-threat?* • *How to controls mitigate vulnerabilities and exposures?*
01.02.02.05	e) Understand the concept of building a room of controls	• *How do you build a room of controls?* • *What is a trusted identity?* • *How does a room of controls protect managed assets?*
01.02.03	**Lesson – Managing Risk & Implementing Program Area of Focus**	• *The NIST Risk Management Framework* • *The NIST Cybersecurity Framework* • *Cybersecurity Framework Implementation Coordination* • *The Program Areas of Focus* • *Why is Cybersecurity Important?*
01.02.03.01	a) Understand the principles & key components of the NIST Risk Management Framework	• *Why is a Risk Management Framework Important?* • *What is the NIST Risk Management Framework?*
01.02.03.02	b) Understand the principles and key components of the NIST Cybersecurity Framework	• *Why is a Cybersecurity Framework Important?* • *What is the NIST Cybersecurity Framework?* • *How is the NIST Cybersecurity Framework Implementation coordinated at all levels of an organization (Executive, Business / Process, Implementation / Operations)*
01.02.03.03	c) Understand the Program Areas of Focus	• *What are the key focus areas?* • *How will the program be implemented across all areas?*
01.02.03.04	d) Why adopt the NIST Cybersecurity Framework?	• *Improvements in Communications* • *Benefits of the Framework*
	Chapter 02 - Exercise	Blooms Level 3 & 4 • *Identify optimal technical solutions to a specified incident scenario.* • *Identify optimal business solutions to a specified incident scenario* • *Analyze the scope of exposure to employees in a specified incident scenario and propose an optimum solution to limit the organizational exposure.*

	Quiz	**How measured 10 Question, Multiple choice, 80% Pass**
01.03	**Chapter 03 – The Controls Factory Model**	
01.03.01	**Lesson – Cybersecurity Controls Model**	• *Purpose, Goals & Objectives* • *Standard model to build and maintain security controls* • *Based on a factory model (9 functional components)* • *Includes engineering Center (3 functional components)* • *Includes technology center (3 functional components)* • *Includes business center (3 functional components)*
01.03.01.03	a) Building a Cyber Model	• *How do you build a model for applying controls to unmanaged assets?* • *How do strong controls change unmanaged assets to managed assets?*
01.03.01.04	b) Understand our Controls Factory Model (CFM)	• *What is the Controls Factory Model?* • *What are the three key centers of the Controls Factory?* • *How are unmanaged assets changed to managed assets?*
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*
01.03.02.01	a) Modelling Threats and Vulnerabilities	• *How do we conduct an in depth analysis of cyber-threats, vulnerabilities, critical assets, privileged identities, and controls framework?*
01.03.02.02	b) Modelling Assets, Business Roles / Access and Technical Roles / Access	• *How do we conduct an in depth analysis of critical assets, business roles / access and technical roles / access?*
01.03.02.03	c) House of Controls including Business and Technical Controls	• *How do we conduct an in depth analysis of House of Controls, the Controls Framework, Technical vs. Business Controls, Technical and Business Controls Mapping.?*
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*
01.03.03.01	a) Technical Program Design and Build	• *How do we implement a technical program that includes program design, build?* • *How do we design a technical solution based on the 20 Critical Security Controls?*
01.03.03.02	b) Technical Program Operations	• *How do we operate, monitor, and maintain a technology program?* • *How do we apply technical controls to our unmanaged assets?* • *How do we maintain and monitor our security controls, via a SOC?*

01.03.03.03	c) Technical Program Testing and Assurance	• *How do we test and evaluate our security controls based on the PCI Data Security Standard?* • *How do we prioritize our remediation efforts for areas that require controls enhancements?*
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*
01.03.04.01	a) Business Program Design and Build	• *How do we implement a business program that includes program design and build?* • *How do we design a technical solution based on the ISO 27002:2013 Code of Practice?*
01.03.04.02	b) Business Program Workforce Skills Assessment	• *How do we improve the cybersecurity skills of our workforce using the NICE Cybersecurity Workforce Framework (NCWF)?* • *What are the seven NCWF Workforce Categories?*
01.03.04.03	c) Business Program Cyber Risk Management	• *What is the AICPA (American Institute of Certified Public Accountants) Cyber Risk Framework?* • *What are the key elements of the AICPA Description Criteria that entities use in designing a Cybersecurity Risk Management Program?*
	Chapter 03 - Exercise	Blooms Level 3 & 4 • *Analyze a scenario and decide the priorities for technical solutions in a first year roadmap.* • *Analyze a scenario and decide the priorities business solutions in a first year roadmap.* • Decide on a communication approach for program status for an executive steering or oversight committee.
	Quiz	How measured 10 Question, Multiple choice, 80% Pass

Part 02 – The Engineering Blueprint

Learning Objective	Description	Learning Objective and References
01.04	**Chapter 04 – Cyber Threats & Vulnerabilities**	
01.04.01	**Lesson – Cyber Kill Chain® Model**	• *The anatomy of a typical cyber-attack* • *Actions of attackers* • *Actions of defenders*
01.04.01.01	a) Study the 7-step Cyber Kill Chain® from Lockheed Martin	• *What is the Lockheed Martin Cyber Attack Chain?* • *What are the seven stages of a cyber-attack?*
01.04.01.02	b) Understand attacker's goals and actions for each stage of the Cyber Kill Chain®	• *What are the attacker's goals at each stage of the Cyber Kill Chain®?* • *What are the attacker's actions at each stage of the Cyber Kill Chain®?*
01.04.01.03	c) Understand defender's goals and actions for each stage of the Cyber Kill Chain®	• *What are the defender's goals at each stage of the Cyber Kill Chain®?* • *What are the defender's actions at each stage of the Cyber Kill Chain®?*
01.04.02	**Lesson – The Cyber Threat Landscape**	• *The top cyber threats and how they are modeled* • *Standard descriptions of common cyber-attacks*
01.04.02.01	a) Understand the top cyber threats	• *Understand the Cyber Threat Landscape* • *Understand what we can learn from reviewing the top threats*
01.04.02.02	b) Understand the Cyber Threat Landscape	• *Understand the key elements of the Threat Landscape* • *Understand how the cyber threat landscape maps to the Cyber Kill Chain®.*
01.04.02.03	c) Understand the top cyber threats	• *What are the top cyber-treats according to ENISA (European Union Agency for Network and Information Security)*
01.04.02.04	d) Understand & explain the malware attack	• *How does a malware attack work?* • *What are the key steps during the attack?* • *What are the key steps after the attack?*
01.04.02.05	e) Understand & explain the web based attack	• *How does a web based attack work?* • *What are the key steps during the attack?* • *What are the key steps after the attack?*
01.04.03	**Lesson – Vulnerabilities**	• *The top technical & business vulnerabilities* • *The controls that mitigate vulnerabilities*
01.04.03.01	a) Understand vulnerabilities and weaknesses	• *Understand the vulnerabilities and weaknesses* • *Understand keys to a successful vulnerability management capability* • *Understand what we can learn from understanding vulnerabilities and remediation*

01.04.03.02	b) Understand the vulnerability management lifecycle	• *Understand the six steps that comprise the vulnerability management lifecycle?*
01.04.03.03	c) Understand the top technical vulnerabilities	• *What are examples of technical vulnerabilities?*
01.04.03.04	d) Understand the top business vulnerabilities	• *What are examples of technical vulnerabilities?*
01.04.03.03	**Case Study – 2012 South Carolina Department of Revenue (DOR) Data Breach**	• *When did the 2012 State of South Carolina Department of Revenue data breach occur?* • *What was the cause of the data breach?* • *What was the timeline and impact of the breach?* • *What were the short-term findings and recommended remediation steps?* • *What were the long-term findings and recommended remediation steps?*
	Chapter 04 - Exercise	Blooms Level 3 & 4 • *Analyze a given scenario and determine the optimal approach to ensure accurate software tool configuration.* • *Determine the best approach for the identification of malware installed and its remediation.* • *Apply your knowledge of how software tools can be misconfigured formulate a plan to prevent that from happening.*
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
01.05	**Chapter 05 – Digital Assets, Identities & Business Impact**	
01.05.01	**Lesson – Securing our Digital Assets**	• *The NIST Cybersecurity Framework* • *The Identify Core Function*
01.05.01.01	a) Understand the purpose, goals & objectives for securing digital assets	• *Why do we need to protect digital assets?* • *What do we have to do to it?*
01.05.01.02	b) Understand Controls Factory Model	• *This chapter covers the Engineering Center – Assets and Identities*
01.05.01.03	c) Modeling Cyber Attacks	• *This Chapter reviews the asset and business zones*
01.05.01.02	d) Understand the NIST CSF core functions	• *What are the core NIST CSF functions?* • *What are the key categories of the Identify Core Function?*
01.05.02	**Lesson – Asset Management**	• *The Asset Management Framework Category*

01.05.02.01	a) Understand the key asset families (endpoints, networks, servers, applications, etc.)	• *What are the key asset families?* • *How are they organized into groups?* • *Who is the designated owner?* • *Who is responsible for their security?*
01.05.02.02	b) Understand the key IT diagrams (network, data flow, user access, application, etc.)	• *What are the key IT diagrams?* • *Why are they important?* • *Who is the designated owner?* • *Who is responsible for their accuracy?*
01.05.02.03	c) Understand how security technologies are implemented within a typical network architecture	• *What are the key security technologies?* • *How are they used to protect /monitor assets?* • *How are they implemented in a typical network?*
01.05.02.04	d) Understand Data Inventory and Classification	• *How is data classified?* • *What is a typical classification standard?* • *What are the key steps in Data Lifecycle Management?*
01.05.02.05	e) Understand the principles of Roles Based Access Control (RBAC)	• *What are the key business roles?* • *How are they organized to access business applications?* • *How is access to business applications managed based on the business roles (RBAC Model)?*
01.05.02.06	f) Understand the principles of Privileged Identity Management (PIM)	• *What are the key technical roles?* • *How are they organized to access IT assets?* • *How is access to the IT assets managed based on the technical roles (PIM Model)?*
01.05.03	**Lesson – Business Environment**	• *The Business Environment Framework Category*
01.05.03.01	a) Understand the Business Environment Framework Category	• *What are the five sub categories in the Business Environment Framework Category?*
01.05.03.02	b) Understand the Critical Infrastructure Sectors	• *What are the 16 critical infrastructure sectors?* • *Why is it important that these sectors are secure?*
01.05.03.03	c) Communications Sector Plan	• *What are the primary cybersecurity goals of the Communications Sector?*
01.05.03.04	d) Financial Services Sector Plan	• *What are the primary cybersecurity goals of the Financial Sector?*
01.05.03.05	e) Healthcare and Public Health Sector Plan	• *What are the primary cybersecurity goals of the Healthcare and Public Health Sector?*
		•
01.05.03	**Lesson – Governance & Risk Assessment**	• *What is IT Governance?* • *What is an IT Risk Assessment?*
01.05.03.01	a) Understand purpose, goals and objectives of IT Governance	• *What are the expected outcomes of IT governance?*
01.05.03.02	b) Understand purpose, goals and objectives of IT Risk Assessment	• *What are the expected outcomes of IT risk assessment?*
	Chapter 05 - Exercise	Blooms Level 3 & 4 • *Understand, analyze and explain the usage of a data flow diagram from an operational perspective.*

		• *Explain how a data flow diagram provides value to a business from a financial perspective.* • *Analyze a diagram in a scenario and determine what information is inaccurate or missing.*
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
01.06	**Chapter 06 – NIST Cybersecurity Framework – Design & Build**	
01.06.01	**Lesson – NIST CSF: Core, Tiers & Profiles**	• *Presidential Executive Order 13636* • *Improving Critical Infrastructure Cybersecurity* • *The Core Functions* • *The Implementation Tiers* • *The Current and Target Profiles*
01.06.01.01	a) Understand EO 13636 policy to enhance Critical Infrastructure security & resilience	• *Why was the Executive Order was issued?* • *What were the main outcomes of the Executive Order?*
01.06.01.02	b) Understand the NIST Cybersecurity Framework goals & objectives.	• *Why was the framework created?* • *Who will benefit from the framework?* • *How should the framework be used?*
01.06.01.03	c) Understand the 5 core functions and 22 Framework Categories & organization within the Core Functions	• *What are the 5 core functions?* • *What are the 22 framework categories?* • *How are the categories organized by function?*
01.06.01.04	d) Understand the implementation tiers and measure of capability.	• What is an implementation tier? • *What are the 4 implementation tiers of the NIST Cybersecurity Framework?*
01.06.01.05	e) Understand the framework profiles and implementation approach.	• *What is a framework profile?* • *What is the implementation approach for the NIST Cybersecurity Framework?*
01.06.03	**Lesson – NIST CSF: Subcategory Mapping**	• *The NIST Cybersecurity Framework* • *Mapping to security standards / best practices*
01.06.03.01	a) Understand the mapping of the 20 CSCs (technical controls) to the NIST CSF	• *How are the 20 Critical Security Controls (CSC) mapped to the NIST Cybersecurity Framework?*
01.06.03.02	b) Understand the mapping of the ISO 27002 controls (business controls) to the NIST CSF	• *How are the ISO 27002:2013 controls mapped to the NIST Cybersecurity Framework?*
01.06.03.03	c) Understand the mapping of the PCI Data Security Standards (testing standard) to the NIST CSF	• *How do the 12 Requirements of the PCI Data Security Standard map to the NIST Cybersecurity Framework?*
01.06.04	**Lesson – NIST CSF: Identify**	• *The Identify Core Function* • *The Framework Categories and Sub Categories*

01.06.04.01	a) Understand the 5 framework categories, detailed requirements & implementation solution for the NIST Cybersecurity Framework Identify core function	• *What is the overall goal of the Identify Core Function?* • *What are the detailed requirements of the 5 framework categories that align with the Identify Core Function?*
01.06.05	**Lesson – NIST CSF: Protect**	• *The Protect Core Function* • *The Framework Categories and Sub Categories*
01.06.05.01	a) Understand the 5 framework categories, detailed requirements & implementation solution for the NIST Cybersecurity Framework Protect core function	• *What is the overall goal of the Protect Core Function?* • *What are the detailed requirements of the 6 framework categories that align with the Protect Core Function?*
01.06.06	**Lesson – NIST CSF: Detect**	• *The Detect Core Function* • *The Framework Categories and Sub Categories*
01.06.06.01	a) Understand the 5 framework categories, detailed requirements & implementation solution for the NIST Cybersecurity Framework Detect core function	• *What is the overall goal of the Detect Core Function?* • *What are the detailed requirements of the 3 framework categories that align with the Detect Core Function?*
01.06.07	**Lesson – NIST CSF: Respond**	• *The Respond Core Function* • *The Framework Categories and Sub Categories*
01.06.07.01	a) Understand the 5 framework categories, detailed requirements & implementation solution for the NIST Cybersecurity Framework Respond core function	• *What is the overall goal of the Respond Core Function?* • *What are the detailed requirements of the 5 framework categories that align with the Respond Core Function?*
01.06.08	**Lesson – NIST CSF: Recover**	• *The Recover Core Function* • *The Framework Categories and Sub Categories*
01.06.08.01	a) Understand the 5 framework categories, detailed requirements & implementation solution for the NIST Cybersecurity Framework Recover core function	• *What is the overall goal of the Recover Core Function?* • *What are the detailed requirements of the 3 framework categories that align with the Recover Core Function?*
	Chapter 06 - Exercise	Blooms Level 3 & 4 • *In the context of the scenario involving Energy Sector determine and explain which Business*

		Environment Framework categories are the most important to consider. • *Analyze and advise the executive committee, based on a given scenario, the best approach to communicating priorities for the organizational mission.* • Based on the scenario, devise a plan to ensure that resilience requirements are included in the delivery of ALL critical services.
	Quiz	How measured 10 Question, Multiple choice, 80% Pass

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**	• *The technical security controls* • *The Center for Internet Security (CIS)* • *The 20 Critical Security Controls*
03.07.01.01	a) Understand the technology center as it relates to the controls factory.	• *What is the technology center?* • *Where does it fit under the CFM?*
03.07.01.02	b) Understand where the technology design capability fits under the technology center	• *What are the key elements of the technology design?*
03.07.01.03	c) Understand the technical controls and where they reside within the cyber-attack model	• *What are the key technology program controls*
03.07.01.04	d) Understand the 20 critical controls and sub controls and how the controls map to managed assets	• *What are the 20 Critical Controls?* • *Who is responsible for updating and maintaining the 20 critical controls?*
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*
03.07.02.01	a) Understand 5 of the 10 controls that protect endpoints and servers	• *What are Critical Security Controls 1 – 5* • *What are the control objectives?* • *How are the controls designed?* • *What are the technical requirements?*
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*
03.07.03.01	a) Understand 5 of the 10 controls that protect endpoints and servers	• *What are Critical Security Controls 6 – 10* • *What are the control objectives?* • *How are the controls designed?* • *What are the technical requirements?*
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*
03.07.04.01	a) Understand the 4 controls that protect networks	• *What are Critical Security Controls 11,12,13,15* • *What are the control objectives?* • *How are the controls designed?* • *What are the technical requirements?*
03.07.04.02	b) Understand the 1 control that protects applications	• *What is Critical Security Controls 14* • *What are the control objectives?* • *How are the controls designed?* • *What are the technical requirements?*
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*
03.07.05.01	a) Understand the 5 controls that protect applications	• *What are Critical Security Controls 1 – 5* • *What are the control objectives?* • *How are the controls designed?* • *What are the technical requirements?*
	Chapter 07 - Exercise	Blooms Leve 3 & 4 • *Summarize how specific technology maps to specific Critical Controls* • *Analyze the key benefits when using specific tools to automate a specific Critical Control.*
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
03.08	**Chapter 08** – Security Operations Center (SOC)	
03.08.01	**Lesson – Security Operations Center**	• *Review of SOC technology* • *Review of SOC people* • *Review of SOC process* • *Review of SOC services* • *Review of SOC alternatives*
03.08.01.01	a) Understand what it will take to answer the question "Are we Secure“	• *What is the goal of Information security Continuous Monitoring (ISCM)?*
03.08.01.02	b) Understand Information Security Continuous Monitoring (ISCM) definition, goals and objectives	• *What is the primary goal of Information security Continuous Monitoring (ISCM)?* • *What are the six steps of an Information security Continuous Monitoring (ISCM) program?*

03.08.01.03	c) ISCM Technical Solution: Security Information and Event Management (SIEM)	• *What is a SIEM?* • *What are the SIEM basics?* • *What are the key SIEM capabilities?*
03.08.01.04	d) ISCM Operations: Security Operations Center	• *What is a SOC?* • *A SOC is where information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.*
03.08.01.05	e) SOC inputs and outputs. Security Events, Attacks and Incidents.	• *Reported issues, managed and unmanaged assets, threat & vulnerability intelligence* • *What are Security Events, Attacks and Incidents?*
03.08.01.06	f) SOC core functions and building blocks	• *What are the six steps of an Information security Continuous Monitoring (ISCM) program?*
03.08.02	**Lesson – SOC Technology**	• *Technical requirements for an ISCM capability* • *Analysis of SOC Technology*

03.08.02.01	a) Understand SOC technology solutions and how they map to cyber attacks	• *What are functional capabilities of SIEM technology?*
		  • *Monitoring Security Devices*
		  • *Monitoring Servers & Mainframes*
		  • *Monitoring Networks & Virtual Activity*
		  • *Monitoring Data Activity*
		  • *Monitoring Application Activity*
		  • *Monitoring Configuration Information*
		  • *Monitoring Vulnerabilities and Threats*
		  • *Monitoring User Activity*

03.08.03	**Lesson – SOC People**	• *Personnel requirements for an ISCM capability* • *Analysis of SOC people*
03.08.03.01	a) Understand SOC personnel, resources, roles, responsibilities, skills and duties	• *What are the key roles of a SOC?* • *What are the responsibilities for each role?* • *What are SOC Analyst Levels and Functions?* • *What are skills / roles for SOC Tier 1 (Analyst), Tier 2 (Incident Responder), Tier 3 (Subject Matter Expert), Tier 4 (SOC Manager)?*
03.08.04	**Lesson – SOC Process**	• *Process requirements for an ISCM capability* • *Analysis of SOC threat hunting process* • *Analysis of Incident management process*
03.08.04.01	a) Understand threat hunting approach for uncovering a threat actor's TTPs	• *What is cyber threat hunting?* • *What are the levels of maturity for a threat hunting program?*
03.08.04.02	b) Understand incident management requirements	• *What is Information Security Incident Management?* • *What are the main steps in managing incidents?*
03.08.05	**Lesson – SOC Services**	
03.08.05.01	a) Understand SOC services	• *Security Consulting and Testing Services* • *Managed Network Security Services* • *Managed Monitoring and Operations*

		• *Incident Response and Forensics Services*
03.08.05.02	b) Understand Security Consulting and Testing Services	• *What is a Cyber Risk Assessment?* • *What is Penetration Testing?* • *What is Vulnerability Management?* • *What is Web Application Testing?* • *What is a Compliance Audit?*
03.08.05.03	c) Understand Managed Network Security Services	• *What is Managed Firewall Service?* • *What is Managed IDS/IPS Service?* • *What is Managed Malware Service?* • *What is Managed Proxy Service?* • *What is Managed Authentication Service?* • *What is DDoS Protection?* • *What is Threat Monitoring and Analysis?*
03.08.05.04	d) Understand Managed Monitoring and Operations Services	• *What is Log management?* • *What is Managed SIEM?* • *What is Threat Detection* • *What is Device Health Monitoring & Management?*
03.08.05.05	e) Understand Incident Response and Forensics Services	• *What are IR Services* • *What are Computer Forensic Services?*
03.08.06	**Lesson – SOC Alternatives**	• *Central Log Management* • *DIY Security Information and Event management* • *Managed Security Services* • *Co-Managed SIEM*
03.08.06.01	a) Understand Central Log Management	• *What is the purpose of Log Management?* • *What are the Log Sources?* • *What is Log Collection and Storage?* • *What are Log management Challenges?* • *What are Log management Benefits & Weaknesses?*
03.08.06.02	b) Understand DIY Security Information and Event management	• *What is the purpose of SIEM Technology?* • *What are SIEM Operations?* • *What are SIEM Challenges?* • *What are SIEM Benefits & Weaknesses?*
03.08.06.03	c) Understand Managed Security Services	• *What is the purpose of MSSP?* • *What are MSSP Services?* • *What are MSSP Advantages & Weaknesses?*
03.08.06.04	d) Understand Co-managed SIEM	• *What is the purpose of co-managed Services?* • *What are Co-Managed Services?* • *What are Co-managed Services Benefits & Weaknesses?*
	Chapter 08 - Exercise	Blooms Level 3 & 4 • *Summarize the key benefits of an ISCM and include why organizations fail to implement continuous monitoring programs.*

		• *In a given scenario, analyze and explain your rationale for the implementation of an ISCM program.*
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
03.09	**Chapter 09** – Technology Program Test & Assurance	
03.09.01	**Lesson – Controls Factory - Testing & Assurance**	• *Payment Card Industry (PCI) Data Security Standard (DSS) Version 3.2 requirements* • *Test plan for 12 DSS requirements*
03.09.01.01	a) Understand high level 6 high level function and the 12 requirements of the PCI data security standard	• *What are the 6 High Level PCI DSS functions?* • *What are the 12 PCI DSS requirements?*
03.09.01.02	b) Understand how the 12 PCI-DSS map to the NIST CSF	• *How do the 12 PCI DSS Requirements map to the NIST Cybersecurity Framework?*
03.09.02	Lesson – Goal 1	• *Build and Maintain a Secure Network and Systems*
03.09.02.01	a) Install and maintain a firewall configuration to protect cardholder data	• *Requirement 1: Install and maintain a firewall configuration to protect cardholder data*
03.09.02.02	b) Do not use vendor defaults for passwords and other security parameters	• *Requirement 2: Do not use vendor defaults for passwords and other security parameters*
03.09.03	Lesson – Goal 2	• *Protect Cardholder Data*
03.09.03.01	a) Protect stored cardholder data	• *Requirement 3: Protect stored cardholder data*
03.09.03.02	b) Encrypt transmission of cardholder data across open, public networks	• *Requirement 4: Encrypt transmission of cardholder data across open, public networks*
03.09.04	Lesson – Goal 3	• *Maintain a Vulnerability Management Program*
03.09.04.01	a) Use and regularly update anti-virus software or programs	• *Requirement 5: Use and regularly update anti-virus software or program*
03.09.04.02	b) Develop and maintain secure systems and applications	• *Requirement 6: Develop and maintain secure systems and applications*
03.09.05	Lesson – Goal 4	• *Implement and Maintain Strong Access Control Measures*
03.09.05.01	a) Restrict access to cardholder data by business need-to-know	• *Requirement 7: Restrict access to cardholder data by business need-to-know*
03.09.05.02	b) Assign a unique ID to each person with computer access	• *Requirement 8: Assign a unique ID to each person with computer access*
03.09.05.03	c) Restrict physical access to cardholder data	• *Requirement 9: Restrict physical access to cardholder data*

03.09.06	Lesson – Goal 5	• *Regularly Monitor and Test Networks*
03.09.06.01	a) Track and monitor all access to network resources and cardholder data	• *Requirement 10: Track and monitor all access to network resources and cardholder data*
03.09.06.02	b) Regularly test security systems and processes	• *Requirement 11: Regularly test security systems and processes*
03.09.07	Lesson – Goal 6	• *Maintain an Information Security Policy*
03.09.07.01	a) Requirement 12 - Maintain a policy that addresses information security for employees and contractors	• *Requirement 12: Maintain a policy that addresses information security for employees and contractors*
	Chapter 09 - Exercise	Blooms Level 3 & 4 • *For a given scenario, assess and explain when an organization might fail to implement a vulnerability management program.* • Detail what characteristics make up an optimal vulnerability assessment program.
	Quiz	How measured 10 Question, Multiple choice, 80% Pass

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**	• *Key elements of the Business Program* • *Building an Information Security Management System (ISMS)*
04.10.01.01	a) Understand objectives of ISO 27001 which establishes an ISMS	• *What is an Information Security Management System (ISMS)?*
04.10.01.02	b) Understand objectives of ISO 27002:2013 code of practice for information security controls	• *What are the primary objectives of ISO 27002?* • *What are the key control clauses?*
04.10.01.03	c) Understand the relationship between ISO 27001 and ISO 27002	• *How does ISO 27002 Code of Practice relate to the ISO 27001 Information Security Management System?*
04.10.01.04	d) Understand the structure of the ISO 27002:2013 and the 14 security control clauses	• *What are the 14 Control Clauses for ISO 27002?*
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*
04.10.02.01	a) Understand the purpose, goals and objectives for each ISO control clause	• *What are the goals and objectives for ISO 27002 Control Clause A.5 to A.7?*
04.10.02.02	b) Understand high level implementation requirements for each ISO control clause	• *What are the high-level implementation requirements for ISO 27002 Control Clause A.5 to 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*
04.10.03.01	a) Understand the purpose, goals and objectives for each ISO control clause	• *What are the goals and objectives for ISO 27002 Control Clause A.8 to A.9?*
04.10.03.02	b) Understand high level implementation requirements for each ISO control clause	• *What are the high-level implementation requirements for ISO 27002 Control Clause A.8 to 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*

04.10.04.01	a) Understand the purpose, goals and objectives for each ISO control clause	• *What are the goals and objectives for ISO 27002 Control Clause A.10 to A.11?*
04.10.04.02	b) Understand high level implementation requirements for each ISO control clause	• *What are the high-level implementation requirements for ISO 27002 Control Clause A.10 to 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*
04.10.05.01	a) Understand the purpose, goals and objectives for each ISO control clause	• *What are the goals and objectives for ISO 27002 Control Clause A.12 to A.14?*
04.10.05.02	b) Understand high level implementation requirements for each ISO control clause	• *What are the high-level implementation requirements for ISO 27002 Control Clause A.12 to 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*
04.10.06.01	a) Understand the purpose, goals and objectives for each ISO control clause	*What are the goals and objectives for ISO 27002 Control Clause A.15 to A.18?*
04.10.06.02	b) Understand high level implementation requirements for each ISO control clause	*What are the high-level implementation requirements for ISO 27002 Control Clause A.15 to A.18?*
	Chapter 10 - Exercise	Blooms Level 3 & 4 • *Compare and contrast how controls are accomplished using the Controls Factor Model and an ISMS*
	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**	• *Review Cybersecurity Workforce Demand* • *Review NICE Workforce Categories* • *Review NICE Specialty Areas*
04.11.01.01	a) Understand workforce demands for cybersecurity skills	• *What are the key workforce demands?*
04.11.01.02	b) Understand the NICE Cybersecurity Workforce Framework (NCWF)	• *What is the NICE Cybersecurity Workforce Framework (NCWF)?*

04.11.01.03	c) Understand the capabilities of the interactive NCWF Website "Cyber Seek"	• *What are the capabilities of Cyber Seek?* • *What is the tool used for?* • *What is the Cybersecurity Career Pathway?* • *Which Cybersecurity Careers map to the NICE Specialty Areas?*
04.11.02	**Lesson the NICE Workforce Framework (NCWF)**	• *Review the NICE Workforce Framework (NCWF)* • *Review Workforce Categories and Specialty Areas*
04.11.02.01	a) Understand the 7 NICE Workforce Categories and 33 Specialty Areas	• *What are the 7 NICE Workforce Categories?* • *What are the 33 NICE Specialty Areas?* • *What are the 52 Work Roles?*
04.11.03	**Lesson – Securely Provision**	• *Review Securely Provision Workforce Category*
	a) Understand the Securely Provision Workforce Category and seven Specialty Areas	• *What are the seven Specialty Areas under the Securely Provision Workforce Category?* • *What are the Work Roles under the Securely Provision Workforce Category?*
04.11.04	**Lesson – Operate & Maintain**	• *Review Operate and Maintain Workforce Category*
04.11.03.01	a) Understand the Operate and Maintain Workforce Category and six Specialty Areas	• *What are the six Specialty Areas under the Operate and Maintain Workforce Category?* • *What are the Work Roles under the Operate and Maintain Workforce Category?*
04.11.05	**Lesson – Oversee & Govern**	• *Review Oversee and Govern Workforce Category*
04.11.05.01	a) Understand the Oversee and Govern Workforce Category and six Specialty Areas	• *What are the six Specialty Areas under the Oversee and Govern Workforce Category?* • *What are the Work Roles under the Oversee and Govern Workforce Category?*
04.11.06	**Lesson – Protect & Defend**	• *Review Protect and Defend Workforce Category*
04.11.06.01	a) Understand the Protect and Defend Workforce Category and four Specialty Areas	• *What are the four Specialty Areas under the Protect and Defend Workforce Category?* • *What are the Work Roles under the Protect and Defend Workforce Category?*
04.11.07	**Lesson – Analyze**	• *Review Analyze Workforce Category*
04.11.07.01	a) Understand the Analyze Workforce Category and five Specialty Areas	• *What are the five Specialty Areas under the Analyze Workforce Category?* • *What are the Work Roles under the Analyze Workforce Category?*
04.11.08	**Lesson – Collect & Operate**	• *Review Collect and Operate Workforce Category*
04.11.08.01	a) Understand the Collect and Operate Workforce Category and three Specialty Areas	• *What are the three Specialty Areas under the Collect and Operate Workforce Category?* • *What are the Work Roles under the Collect and Operate Workforce Category?*

04.11.09	**Lesson – Investigate**	• *Review Investigate Workforce Category*
04.11.09.01	a) Understand the Investigate Workforce Category and two Specialty Areas	• *What are the two Specialty Areas under the Investigate Workforce Category?* • *What are the Work Roles under the Investigate Workforce Category?*
	Chapter 11 - Exercise	Blooms Level 3 & 4 • *Explain why the various tactics, the techniques and procedures used in Threat Hunting are important.* • *When conducting a malware analysis which technique is the best and why it's superior to the others available.*
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
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*
04.12.01.01	a) Understand objectives of AICPA Proposed Description Criteria for a Cybersecurity Risk Management Program	• *What is the proposed AICPA Description Criteria for a Cybersecurity Risk Management Program?*
04.12.01.02	b) Understand the objectives of the nine AICPA Description Criteria Categories	• *What are the nine key objectives of the AICPA Description Criteria for a Cybersecurity Risk Management Program?*
04.12.01.03	c) Understand the 31 AICPA Description Criteria	• *What are the 31 detailed criteria the AICPA Description Criteria for a Cybersecurity Risk Management Program?*
04.12.02	**Lesson – Description Criteria Categories:** • *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*
04.12.02.01	a) Understand at a high level the Description Criteria and Points of Focus of the AICPA Cyber Risk Management Framework	• *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 – 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*	• *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*
04.12.03.01	a) Understand at a high level the Description Criteria and Points of Focus of the AICPA Cyber Risk Management Framework	• *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*
04.12.04	**Lesson – Description Criteria Categories:** • *Cybersecurity Control Activities*	• *AICPA Description Criteria Categories:* • *Cybersecurity Control Activities*
04.12.04.01	a) Understand at a high level the Description Criteria and Points of Focus of the AICPA Cyber Risk Management Framework	• *What are the description criteria, points of focus of the AICPA Description Criteria Categories:* • *Cybersecurity Control Activities*
	Chapter 12 - Exercise	Blooms Level 3 & 4 • *When considering risk management, what are the decisions the executive committee must make and why are they important to the implementation of the program.* • *As an executive, what would be the questions you should be asking and why is each one important?*
	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?*
05.13.01.02	b) Understand Step 1: Establish Project Scope	• *Establish Team Leaders* • *Define Organizational Goal and Scope* • *Define Business Goals and Scope* • *Define Technical Goals and Scope*
05.13.01.03	c) Understand Step 2: Document Current State	• *Assess Business Practices, Risks and Controls* • *Assess Applications, Risks and Controls* • *Assess Infrastructure, Risks and Controls* • *Create a Current State Profile*
05.13.01.04	d) Understand Step 3: Create a Remediation Plan	• *Create a Target State Profile* • *Determine, analyze and prioritize gaps* • *Create a business case* • *Implement action plan*
05.13.01.05	e) Understand Step 4: Create a Communications 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*
05.13.02,01	a) Understand how to conduct a cybersecurity program assessment based on the 20 critical security controls	• *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*
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?*
05.13.03.02	b) Understand how to establish a current state profile / scorecard, target state profile / scorecard, and an implementation roadmap	• *How do you document and deliver a report that contains a current state profile, target state profile and cybersecurity scorecard?*

	to assist an organization in improving its overall maturity of the cybersecurity program	• *How do you evaluate and report on the overall maturity of a cybersecurity program?*
	Chapter 13 - Exercise	Blooms Level 3 & 4 • *Based on a scenario, conduct a detailed cybersecurity program assessment and set up a scorecard for the 20 Critical Controls.*
	Quiz	How measured 10 Question, Multiple choice, 80% Pass
05.14	**Chapter 14** – The Cyber Risk Program Assessment	
05.14.01	**Lesson – Cybersecurity 101: A Resource Guide for Bank Executives**	• *Develop Cyber Risk Management Program and Scorecard*
05.14.01.01	a) Cybersecurity 101 - Purpose Goals and Objectives	• *What are purpose, goals and objectives of a cyber-risk management program?*
05.14.01.02	b) The NIST Cybersecurity Framework Core Functions	• *What are the objectives of the five core functions of the NIST Cybersecurity Framework?*
05.14.01.03	c) Conducting a Cyber Risk Assessment	• *What are the three main steps for conducting a Risk Assessment?* • *Classification of information* • *Identify threats and vulnerabilities* • *Cyber-risk management process*
05.14.01.04	d) Key risk areas of NIST CSF Core Function: Identify	• *What are the key areas of a risk assessment for the Identify Core Function?*
05.14.01.05	e) Key risk areas of NIST CSF Core Function: Protect	• *What are the key areas of a risk assessment for the Protect Core Function?*
05.14.01.06	f) Key risk areas of NIST CSF Core Function: Detect	• *What are the key areas of a risk assessment for the Detect Core Function?*
05.14.01.07	g) Key risk areas of NIST CSF Core Function: Respond	• *What are the key areas of a risk assessment for the Respond Core Function?*
05.14.01.08	h) Key risk areas of NIST CSF Core Function: Recover	• *What are the key areas of a risk assessment for the Recover Core Function?*
05.14.01.09	i) Summary of Requirements for a Risk Assessment based on the NIST Cybersecurity Framework	• *What is the summary of requirements for Identify, Protect, Detect, Respond and Recover core functions?*
05.14.02	**Lesson – Sample Risk Assessment**	• *Conduct sample cyber-risk assessment*
05.14.02.01	a) Understand how to conduct a cybersecurity program assessment based on the NIST Cybersecurity Framework	• *What is the process used to establish a risk score based on the core functions on the NIST Cybersecurity Framework?*
05.14.02.02	b) Step 1: Identify Core Function	• *Threat Likelihood and Vulnerability Impact for key risk areas relative to the Identify Core Function*

05.14.02.03	c) Step 2: Protect Core Function	• *Threat Likelihood and Vulnerability Impact for key risk areas relative to the Protect Core Function*
05.14.02.04	d) Step 3: Detect Core Function	• *Threat Likelihood and Vulnerability Impact for key risk areas relative to the Detect Core Function*
05.14.02.05	e) Step 4: Respond Core Function	• *Threat Likelihood and Vulnerability Impact for key risk areas relative to the Respond Core Function*
05.14.02.06	f) Step 5: Recover Core Function	• *Threat Likelihood and Vulnerability Impact for key risk areas relative to the Recover Core Function*
05.14.02.06	g) Step 5: Recover Core Function	• *Current risk profile based on NIST Cybersecurity Framework Key Risk Areas*
	Lesson – Sample Cyber Risk Assessment	• *Asset Management Framework Category* • *Access Control Framework Category* • *Continuous Monitoring Framework Category* • *Communications Framework Category* • *Improvements Framework Category*
	a) Sample Asset Management Framework Category Risk Assessment: Score = ***	• *ID.AM-1: Inventory of physical devices and systems* • *ID.AM-2: Inventory of software platforms & applications* • *ID.AM-3: Communications and Data Flow Diagrams* *ID.AM-4: Resources prioritized based on classification* • *ID.AM-5: Workforce Roles and responsibilities*
	b) Sample Access Control Framework Category Risk Assessment: Score = ***	• *PR.AC-1: Identities and Credentials are managed* • *PR.AC-2: Physical access is managed* • *PR.AC-3: Remote access is managed* • *PR.AC-4: Access permissions are managed* • *PR.AC-5: Network Integrity is protected*
	c) Sample Continuous Monitoring Framework Category Risk Assessment: Score = ***	• *DE.CM-1: The network is monitored to detect potential cyber-security events.* • *DE.CM-2: The physical environment is monitored to detect potential cyber-security events.* • *DE.CM-3: Personnel activity is monitored to detect potential cyber-security events.* • *DE.CM-4: Malicious code is detected.* • *DE.CM-5: Unauthorized mobile code is detected.* • *DE.CM-6: External service providers are monitored* • *DE.CM-7: Unauthorized resources are monitored.* • *DE.CM-8: Vulnerability assessments are performed.*
	d) Sample Communications Framework Category Risk Assessment: Score = ***	• *RS.CO-1: Personnel know their roles and order of operations when a response is needed.* • *RS.CO-2: Events are reported consistent with established criteria.* • *RS.CO-3: Detection/response information, such as breach reporting requirements, is shared* • *RS.CO-4: Coordination with stakeholders*

		• *RS.CO-5: Voluntary coordination occurs with external stakeholders*
	e) Sample Improvements Framework Category Risk Assessment: Score = ***	• *RC.IM-1: Plans are updated with lessons learned* • *RC.IM-2: Recovery strategy is updated*
05.14.03	**Lesson – Sample Summary Design**	• *Develop sample executive cyber-risk management report*
05.14.03.01	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 cyber-risk management assessment?*
05.14.03.02	b) Understand how to establish a current state profile / scorecard, target state profile / scorecard, and an implementation roadmap to assist an organization in improving its overall maturity of the cyber risk program	• *How do you document and deliver a report that contains a current state profile, implementation roadmap and cyber-risk scorecard?* • *How do you evaluate and report on the overall maturity of a cyber-risk management program?*
	Chapter 14 - Exercise	Blooms Level 3 & 4 • *Based on a scenario, conduct a detailed cybersecurity program assessment and set up a scorecard for the NIST Cybersecurity Framework.*
	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