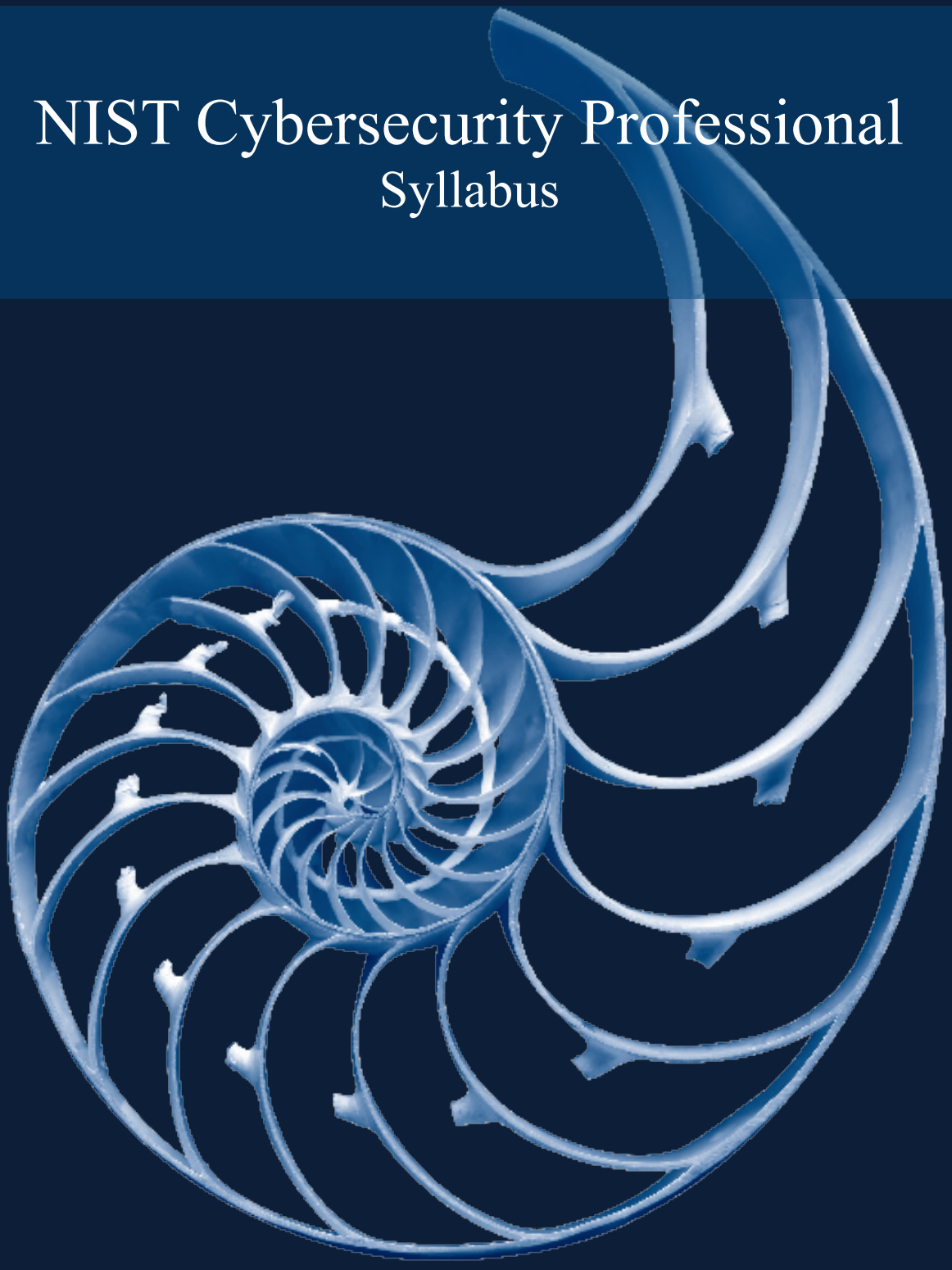
NIST Cybersecurity Professional
Syllabus



Based on Framework for Improving Critical Infrastructure Cybersecurity - Version 1.1

itSM912 NCSP Practitioner

Version 2.02, January 2020

Syllabus

Contents

Acknowledgments 4
Introduction 5
Body of Knowledge 5
Course Organization 7
Syllabus 9
Examination Design and Administration 13
Duration: 13
Number of questions: 13
Level of knowledge: 13
Delivery: 13
Format: 13
Scoring: 13
Examination Design and Administration as Part of the NCSP Bootcamp 14
Duration: 14
Number of questions: 14
Level of knowledge: 14
Delivery: 14
Format: 14
Scoring: 14

Acknowledgments

Publisher

itSM Solution Publishing, LLC
742 Mink Ave., #135
Murrells Inlet, SC 29576
Phone (401) 764-0721

http://www.itsmsolutions.com.

Authors: David Moskowitz, David M. Nichols
Subject Matter Expert & Chief Examiner: Ted Ritter, CISSP

Document Information

Program: itSM912 NCSP Practitioner
Version: 2.02

Date: 01/17/2020

Introduction

The purpose of this document is to provide the course description, target audience, and learning outcomes for the NIST Cybersecurity Professional (NCSP) Practitioner course. The learning outcomes include the number of exam marks allocated to each chapter. It does not include sample questions or the certification exam process.

To realize the positive potential of technology and inspire confidence to achieve innovation through technology, we must collectively manage cyber-risks, both business and technical, to acceptable levels.

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 goals must be to reduce the risk of a data breach, the loss of intellectual property, the compromise of valuable research data, or the protection of employee and customer information. To be successful, we require a business focused cyber-risk management program that includes a complete understanding of business activities and the potential risk to the organization if a bad actor compromises one or more of these activities.

Technology goals start with the identified business activities. What technology underpins enables, supports, or delivers each business activity? To understand security control requirements, we must first identify how the system supports the business activity and the impact on the business if a bad actor compromises the system. It is essential to consider the risks associated with our systems, applications, and processing environment.

This course looks at the impact of digital transformation on cybersecurity risks, an understanding of the threat landscape, and an approach to the application of cybersecurity controls. It provides guidance for students on the best approach to design and build a comprehensive cybersecurity program. Executives are keenly aware of the risks but have limited knowledge on the best way to mitigate these risks. This course also enables our executives to answer the critical question – Are we secure?

The class includes lectures, informative supplemental reference materials, quizzes, exercises, and formal examination. The exercises are a critical aspect of the course; do not skip them. Outcomes and benefits from this class is a practical approach that students can use to build and maintain comprehensive cybersecurity and cyber-risk management programs.

Body of Knowledge

This course assumes the student has successfully taken and passed the NCSF Foundation 2.0 course based on the NIST Cybersecurity Framework version 1.1, release April 2018.

Following the course introduction, the course provides an introduction to the intersection between digital transformation and cybersecurity, which is followed by an overview of the threat landscape.

With this in place, the course uses the Center for Internet Security Controls as an example of a cybersecurity “informative reference” (mentioned in the NIST Cybersecurity Framework. Each organization that sends candidates to the course should select one or more informative references that match the need of the organization (e.g., HIPAA, PCI-DSS, or NIST 800-171).

Following an approach to the implementation of cybersecurity controls, the course delves into an organizational approach to cybersecurity that starts governance, management, and a supportive culture,

including an understanding of how things occur within the organization concerning three specific areas: work, communication, and improvement.

Finally, the course provides additional guidance for the cybersecurity practitioner to determine the current state, the desired state, and a plan to close the gap – and to do this over and over again to inculcate it into organizational DNA.

Course Organization

The course is organized as follows:

Chapter 1: Course Introduction introduces the course and its conduct, which is followed by a lesson that sets the stage for the rest of the material. Lessons in this chapter include:

- Course Organization
- Setting the Stage

Chapter 2: Digital Transformation introduces students to digital transformation from the perspective of the cybersecurity practitioner. Lessons in this chapter include:

- DX as a Practitioner
- DX in the Context of Cybersecurity
- Cybersecurity as a DX Catalyst

Chapter 3: Threat Landscape introduces the agile and rapidly evolving nature of the threat landscape. It also provides an analysis of well-known breaches as a learning opportunity. Lessons in this chapter include:

- Threat Actors: Agile & Creative
- Attacks
- Challenges
- Organizational Response to Threat Landscape
- Absolute Prevention Not Possible

Chapter 4: The Controls provides an overall approach to control selection for the organization. It presents a natural order to control implementation divided into three areas. Lessons in the chapter include:

- Initiation & Basic
- Foundation
- Organizational & Recovery

Chapter 5: Adopt & Adapt presents an overview of the necessary governance, management and cultural changes for a successful cybersecurity program. Lessons in this chapter include:

- The Context of Adopt & Adapt
- Cybersecurity & Culture
- Where We Are?

Chapter 6: Adaptive Way of Working introduces and approach an adaptive way of working. The overall goal is to work for shorter durations to resolve small increments of work. Lessons in this chapter include:

- Introduction to Adaptive Way to Work
- How to Get Started

Chapter 7: Rapid Adoption & Rapid Adaptation FastTrack™ applies the information in the previous chapters to a FastTrack™ to the adoption and adaption of the implementation of a cybersecurity profile. Lessons in this chapter include:

- Rapid Adoption
- Rapid Adaptation

Chapter 8: CIIS as a Practice provides the student with the understanding that cybersecurity isn't a "1-and-done>" operation. It requires continual improvement and implementation. It includes an overview of the Cybersecurity Maturity Model (CMMC) that is applicable for the Department of Defense (DoD) non-classified suppliers and is likely to see wider acceptance (beyond the DoD) . Lessons in this chapter include:

- Ongoing Practice of Cybersecurity
- NIST 7-step Improvement
- Cybersecurity Maturity Model Certification (CMMC)
- Integrate Cybersecurity

Syllabus

Learning Outcome	Chapter	Learning Outcome	Marks	Bloom's 1 & 2	Bloom's 3 & 4
1.0	**Digital Transformation**	**Explores what the Practitioner needs to know about the relationship between digital transformation and cybersecurity.**	3	3	0
1.1		Explain how to determine the impact of cybersecurity on DX.			
1.2		Explain the relationships between culture and digital transformation from the perspective of a practitioner.			
1.3		Explain the delivery of value to stakeholders in a DX & cybersecurity environment.			
g1.4		Illustrate the interdependent relationship between cybersecurity and DX.			
2.0	**Threat Landscape**	**The Practitioner needs to understand what threat actors do and their capabilities.**	8	4	4
2.1		Compare the evolving attack type impact to the threat environment.			
2.2		Apply knowledge about the threat landscape to maintain a readiness to respond.			
2.3		Develop a risk profile based on business impact analysis			
2.4		Establish the relationship between awareness and training in the continual improvement of cybersecurity posture.			
2.5		Develop and treat training & awareness as a critical aspect of deterrence			
2.6		Use knowledge about the threat landscape as a predicate to the adoption and adaptation of your cybersecurity posture.			
3.0	**The Controls**	**This chapter provides a sample set of controls based on an informative reference.**	10	6	4
3.1		Understand the purpose goals & objectives for each control.			
3.1a		Characterize & explain the informative reference controls			
3.2		Discover how to apply the controls in an organizational context.			

4.0	**Adopt & Adapt**	**Adopt is a decision about governance; adapt is the set of management decisions that result from the decision to adopt.**	10	3	7
4.1		Distinguish Adopt, Adapt, Management & Governance.			
4.2		Develop an approach to adoption & adaptation.			
4.3		Distinguish & demonstrate the impact of organizational culture on developing cybersecurity as a capability.			
4.4		Develop an assessment approach to define current state.			
5.0	**Adaptive Way of Working**	**Threat actors are agile and highly adaptive. The cybersecurity Practitioner must develop the same capabilities**	10	3	7
5.1		Break down what constitutes an adaptive approach.			
5.2		Characterize & apply the need for cross-functional teams.			
5.3		Recognize and prioritize the first steps (get started).			
5.4		Demonstrate & establish cybersecurity phases.			
5.5		Break down the impact of the flows.			

6.0	**Rapid Adoption & Rapid Adaptation FastTrack™**	**FastTrack™ is an approach to allow organizations to learn to adapt to an evolving threat landscape rapidly.**	12	3	9
6.1		Approach			
6.1a		Establish what it takes to adopt CS.			
6.1b		Determine how that impacts management adaptation of CS.			
6.1c		Determine how that impacts the capability to assess.			
6.2		CS Capability			
6.2a		Determine the gap between existing & needed capabilities.			
6.2b		Establish what must be developed.			
6.2c		Develop appropriate risk management profile.			
6.3		Discover how cybersecurity impacts people, practice & technology impacts organization.			
6.4		Differentiate CIS Implementation groups.			
6.5		Determine appropriate implementation group & approach.			
6.6		Develop appropriate phase approaches.			
7.0	**CIIS Practice**	**Cybersecurity is an ongoing game of cat and mouse. Organizations must learn how to inculcate cybersecurity improvement into their DNA.**	12	3	9
7.1		Break down & develop mechanisms for ongoing cybersecurity improvement that includes developing a learning organization.			
7.2		Illustrate an improvement plan based on the NIST 7-Step Approach.			
7.3		Illustrate an improvement plan based on the Improvement GPS.			
7.4		Demonstrate understanding of Cybersecurity Maturity Model Certification			
7.5		Break down the balancing loop & how it fits into the escalation archetype.			
7.6		Use the Fast Track™ (improvement & implementation) cycles.			

Examination Design and Administration

Duration:

120 minutes

Number of questions:

65

Level of knowledge:

Bloom's level:
3 – Analysis
4 -- Application

Delivery:

Paper-based, proctored classroom
Online, proctored
Recommended pre-requisites: itSM NCSP Foundation

Format:

This is a closed book exam with sixty-five (65) multiple-choice questions with a single correct answer from 4-choices (A, B, C, D).

Questions may appear in any of the following forms (sample, not an exhaustive list).

- Which of the following is true, correct, most correct?
- Which of the following statements is NOT correct?
- Which of the following statements addresses X?
- How would you show Y?
- What is…?
- What is missing from…?
- _____ is a correct way to…?
- How would you describe…?
- How would you explain…?
- What is the main idea of…?
- Which is the best choice…?
- Which is correct…?
- Which is the correct approach given…?
- Any of the questions may be combined with: Why…?

Scoring:

Each correct answer is worth 1 point. Passing is 60% (39 correct out of 65).

Examination Design and Administration as Part of the NCSP Bootcamp

Duration:

135 minutes

Number of questions:

90

Level of knowledge:

Bloom's level:
1 – Knowledge
2 -- Comprehension
3 – Analysis
4 -- Application

Delivery:

Paper-based, proctored classroom
Online, proctored
Recommended pre-requisites: itSM NCSP Foundation

Format:

This is a closed book exam with sixty-five (65) multiple-choice questions with a single correct answer from 4-choices (A, B, C, D).

Questions may appear in any of the following forms (sample, not an exhaustive list).

- Which of the following is true, correct, most correct?
- Which of the following statements is NOT correct?
- Which of the following statements addresses X?
- How would you show Y?
- What is…?
- What is missing from…?
- _____ is a correct way to…?
- How would you describe…?
- How would you explain…?
- What is the main idea of…?
- Which is the best choice…?
- Which is correct…?
- Which is the correct approach given…?
- Any of the questions may be combined with: Why…?

25 multiple choice Bloom's Level 1 & 2 questions
65 Multiple choice Bloom's Level 3 & 4

Scoring:

Each correct answer is worth 1 point. Passing is 60% (54 correct out of 90).