itSM920 NCSP 800-53 Specialist

Version 1.0 November 2020

Syllabus

Contents

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: David Moskowitz

Document Information

Program: itSM920 NCSP 800-53 Specialist
Version: 1.0

Date: 09/10/2020

Introduction

The purpose of this document is to provide the course description, target audience, and learning outcomes for the NIST Cybersecurity Professional (NCSP) Specialist courses. 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 adapting a principled approach to enterprise risk management framework to better support cybersecurity decisions within the context of the selected informative reference. It guides students on the best approach to adapt, implement, and operate (AIO) a comprehensive cybersecurity program that integrates into existing organizational capabilities and incorporates the selected Informative Reference.

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

Body of Knowledge

This course assumes the student has successfully taken and passed the NCSP Practitioner 2.0 course.

The course introduces the integration of typical enterprise capabilities with cybersecurity from the perspective of the selected cybersecurity informative reference. The overall approach places these activities into systems thinking context by introducing the Service Value Management System composed of three aspects, governance, assurance, and the Z-X Model.

With this in place, the course presents the approach to adapt, implement, operate & improve the organizational cybersecurity posture that builds on the application of the FastTrack™ presented in the NCSP Practitioner.

Course Organization

Chapter 1, Course Introduction – introduces the course and its conduct, 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, Managing Risks in the Digital Age – introduces students to enterprise risk management and the COSO Principles. Lessons in this chapter include:

- Enterprise Risk Management Framework
- COSO Overview
- Enterprise Risk Management Framework Applied

Chapter 3, Cybersecurity within a System – introduces systems thinking and the Service Value Management System (SVMS) that includes the Z-X Model. Lessons in this chapter include:

- The importance of Systems Thinking
- Governance & Culture and Strategy & Objectives
- Service Value Management System
- Z-X Model Overview

Chapter 4, Z-X Model Capabilities – probes the details of the Z-X Model and the relationship to existing organizational capabilities. Lessons in the chapter include:

- Z-X Model Plan
- Z-X Model Design
- Z-X Model Build & Deploy
- Z-X Model Operate & Improve

Chapter 5 Adapt – introduces the first part of AIO, Adapt that introduces the Goal Question Metric approach to develop appropriate metrics for the cybersecurity implementation. Lessons in this chapter include:

- Overview of AIO
- Cybersecurity Adopt & Adapt
- Adapt in the Context of the Z-X Model
- Preparations to Implement
- Project Approach w/GQM
- Metrics, Measurement & Balance

Chapter 6 Implement – covers the "I" in AIO. It presents the implementation of the selected cybersecurity informative references using the same phased approach introduced in the NCSP Practitioner (and Bootcamp) course. Lessons in this chapter include:

- Implement & COSO Principles
- Phase 0
- Phase 1

- Phase 2
- Phase 3
- Additional Controls

Chapter 7 Operate & Improve – covers the last aspect of AIO. Lessons in this chapter include:

- Operate, Improve & COSO Principles
- Deliver Value & Integrate
- Ongoing Improvement

Syllabus

Learning Outcome	Chapter	Learning Outcome	Marks	Bloom's 2 & 3	Bloom's 4 & 5
1.0	**Managing Risks in the Digital Age**	**Explores what the Specialist needs to know about enterprise digital risk**	6	3	3
1.1		Understand & apply the COSO Enterprise Risk Management Framework components and the 20 principles in the context of the adaptation of a NIST-CSF informative reference.			
1.2		Understand the application of a risk management framework			
2.0	**Cybersecurity within a System**	**Explore how cybersecurity fits into a management system.**	8	3	5
2.1		Understand & demonstrate the basics of systems thinking.			
2.2		Understand the impact and application of the COSO principles.			
2.3		Apply the COSO principles from a systems thinking context.			
2.4		Understand and determine how to apply the COSO principles in the context of the SVMS.			
3.0	**Z-X Model Capabilities**	**This chapter provides a sample set of controls based on an informative reference.**	3	3	0
3.1		Understand the Z-X Model as a generic way to organize the behaviors within a management system.			
3.2		Understand the capabilities of governance and assurance and how they apply throughout the Z-X Model.			

4.0	**Adapt**	**Explore the decisions and approaches to adapt an informative reference**	10	3	7
4.1		Understand & explain the integration of the cybersecurity strategy with the business strategy to form the business objectives necessary to achieve the desired cybersecurity posture.			
4.2		Understand, explain & evaluate the SVMS & the adaptation of the selected informative reference.			
4.3		Understand & apply the Goal, Question, Metrics approach.			
5.0	**Implement**	**Explore the integration of the selected informative reference with the service value management system.**	26	10	16
5.1		Explain and evaluate the dependencies of the informative references on existing IT capabilities.			
5.2		Evaluate & plan for cybersecurity operation & improvement			
5.3		Demonstrate working knowledge to apply GQM.			
5.4		Apply & analyze the situation described in the case study to establish a GQM template to take back to work.			
6.0	**Operate & Ongoing Improvement**	**Fast Track™ is an approach to allow organizations to learn to adapt to an evolving threat landscape rapidly.**	12	4	8
6.1		Apply & analyze organizational readiness for cybersecurity within the context of the COSO principles.			
6.1		Understand & apply the cascade from capability to practice area to process and to controls so that cybersecurity becomes part of every aspect of the SVMS.			
6.2		Evaluate changes (gaps) in the threat landscape and the associated impact of operating and improving organizational cybersecurity posture.			

Examination Design and Administration

Pre-requisites:

- itSM NCSP Practitioner or
- itSM NCSP Bootcamp

Duration:

120 minutes

Number of questions:

65

Level of knowledge:

Bloom's level:
2 – Understand
3 – Apply
4 – Analyze
5 – Evaluate
NOTE: Bloom level 4 and 5 questions may require the candidate to synthesize an answer that is not explicitly covered in the course material and exercises.

Delivery:

Open-book, open-notes
Proctored exam either paper-based in a classroom or online.

Format:

This examination consists of sixty-five (65) multiple-choice questions, each 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…?
- How would you describe…?
- How would you determine…?
- How would you justify…?
- What would you recommend…?
- Which is the best choice…?
- Which is the correct approach given…?
- Any of the questions may include an additional qualifier: Why…?

Scoring:

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