itSM921 NCSP 800-171 Specialist

Syllabus

Version 1.0 March 2021

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 and 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 redefine the major target markets. Key business goals must also reduce the risk of a data breach, the loss of intellectual property, and the compromise of valuable research data, while protecting employee and customer information. Success requires a business-focused cyber risk management program that includes a complete understanding of business activities and the potential organizational risk when 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 of a bad actor on the business. 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 the enterprise risk management (ERM) framework to better support cybersecurity decisions, establishing the context for the selected informative reference (IR). It guides students on the best approach to adapting, implementing, and operating (AIO) a comprehensive cybersecurity program that can be integrated into the existing organizational capabilities and incorporates the selected IR.

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

Body of knowledge

This course assumes that 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 selected cybersecurity IR perspective. The overall approach places these activities into a systems-thinking context by introducing the service value management system (SVMS), including governance, assurance, and the Z-X model.

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

Course organization

Chapter 1, Course introduction, introduces the course and its aims, followed by a lesson that prepares students for the rest of the material. Lessons include:

- Course organization
- Setting the stage.

Chapter 2, Managing risks in the digital age, introduces students to ERM and the COSO principles. Lessons include:

- Enterprise risk management framework
- COSO overview
- Enterprise risk management framework applied.

Chapter 3, Cybersecurity within a system, introduces systems thinking and the SVMS (which includes the Z-X model). Lessons include:

- The importance of systems thinking
- Governance and culture
- Strategy and set objectives
- The service value management system
- The Z-X model overview.

Chapter 4, Z-X model capabilities, probes the details of the Z-X model and its relationship to existing organizational capabilities. Lessons include:

- Plan
- Design
- Build and deploy
- Operate
- Improve.

Chapter 5, Adapt, covers the first part of AIO, which introduces the goal, question, metrics (GQM) approach to develop appropriate metrics for the cybersecurity implementation. Lessons include:

- Overview of AIO (adapt, implement, and operate)
- Cybersecurity adopt and adapt
- Adapt in the context of the Z-X model
- Preparation to implement
- Project approach
- Goal, question, metrics (GQM) overview
- Metrics, measurement, and balance.

Chapter 6, Implement, covers the second part of AIO. It presents the implementation of the selected cybersecurity IRs using the phased approach introduced in the NCSP Practitioner (and Bootcamp) course. Lessons include:

- CMMC Overview

- FastTrack & CMMC
- Phase 0 controls
- Phase 1 controls
- Phase 2 controls
- Phase 3 controls
- FastTrack™/CMMC & You.

Chapter 7, Operate and ongoing improvement, covers the third part of AIO. Lessons include:

- Operate, improve, and the COSO principles
- Deliver value and integrate
- Ongoing improvement.

Syllabus

Chapter	Learning outcome*		Total marks	Marks according to	
				Bloom's levels 2 and 3	Bloom's levels 4 and 5
Managing risks in the digital age	1.0	**Explores what the specialist needs to know about risk management for the digital business**	6	3	3
	1.1	Understand and apply the COSO ERM framework components and the 20 principles in the context of the adaptation of a NIST-CSF IR			
	1.2	Understand the application of a risk management framework			
Cybersecurity within a system	2.0	**Explores how cybersecurity fits into a management system**	8	3	5
	2.1	Understand and 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			
Z-X model capabilities	3.0	**Provides a sample set of controls based on an IR**	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			
Adapt	4.0	**Explores the decisions and approaches to adapt an IR**	10	3	7
	4.1	Understand and explain how to integrate cybersecurity strategy with the business strategy to form the objectives necessary to achieve the desired cybersecurity posture			
	4.2	Understand, explain, and evaluate the SVMS and the adaptation of the selected IR			
	4.3	Understand and apply the goal, question, metrics (GQM) approach			

* The numbers reflect the learning objective levels.

Implement	5.0	**Explores the integration of the selected IR with the SVMS and potential assessment guided by the CMMC**	26	10	16
	5.1	Explain the purpose, goals, and objectives of the Cybersecurity Model Certification (CMMC)		5	0
	5.2	Explain and apply the relationship between the FastTrack™ approach to the adaptation, implementation, operation, and improvement of cybersecurity controls and the CMMC.		5	2
	5.3	Explain and evaluate the dependencies of the informative references on existing IT capabilities.			8
	5.4	Demonstrate working knowledge to apply GQM			4
	5.5	Apply and analyze the situation described in the case study to establish a GQM template to take back to work			2
Operate and ongoing improvement	6.0	**FastTrack™ is an approach to allow organizations to learn to adapt to an evolving threat landscape rapidly**	12	4	8
	6.1	Apply and analyze organizational readiness for cybersecurity within the context of the COSO principles			
	6.2	Understand and apply the cascade from capability to practice area to process to controls so that cybersecurity becomes part of every aspect of the SVMS			
	6.3	Evaluate changes (gaps) in the threat landscape and the associated impact of operating and improving the organizational cybersecurity posture			

Examination design and administration

The key elements of the examination and its administration are as follows:

- Prerequisites: 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
- Delivery:
    - Open book, open notes
    - Proctored exam, either paper-based in a classroom or online
- Format: 65 multiple-choice questions, each with a single correct answer from four choices (A, B, C, or D).
- Questions: These may appear in any of the following formats (not an exhaustive list):
    - Which of the following is true, correct, or 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).

[†] Note that Bloom's level 4 and 5 questions may require the candidate to synthesize an answer that is not explicitly covered in the course material and exercises.