itSM920 NCSP® 800-53 Specialist

Version 1.0 January, 2021

Datasheet

Introduction

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 certification 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.

The class includes lectures, informative supplemental reference materials, workshops, and a formal examination. . 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.

About the Body of Knowledge

The NIST 800-53, Revision 5 publication provides a comprehensive overview of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.

The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines. Finally, the consolidated control catalog addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms provided by the controls) and from an assurance perspective (i.e., the measure of confidence in the security or privacy capability provided by the controls). Addressing functionality and assurance helps to ensure that information technology products and the systems that rely on those products are sufficiently trustworthy.

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

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 2.0.

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

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

Delivery:

Open-book, open-notes
Paper-based, proctored classroom
Online, proctored

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).