****

**DVMS Cyber Resilience Professional Foundation Certification Training** - **Version:** 4.0

**Course Overview**

This course introduces learners to the fundamentals of adopting the NIST Cybersecurity Framework (CSF) and prepares them for the Cyber Resilience Professional Foundation certification. Participants will understand the core concepts of cybersecurity risk, the structure of the NIST-CSF, and how to adopt and adapt the framework to enhance enterprise resilience and improve performance. The program combines lecture material, instructor commentary, and references to the *Fundamentals of Adopting the NIST Cybersecurity Framework (2nd Edition)* textbook.

**Learning Objectives**

By the end of the course, participants will be able to:

* Explain fundamental cybersecurity and risk management concepts.
* Understand the structure, components, and relationships within the NIST-CSF.
* Apply concepts of organizational culture, privacy, and resiliency to cybersecurity programs.
* Describe how to adopt and adapt the NIST-CSF within a digital enterprise.
* Recognize how the DVMS (Digital Value Management System) overlay extends and integrates with the NIST-CSF to drive digital business performance and resilience.

**Course Modules and Content Outline**

**Module 1: Imperative & Origin**

* Explain the concept of risk.
* Differentiate between threats and vulnerabilities.
* Understand cybersecurity risk.
* Review the NIST-CSF timeline and its origins.
* Identify the benefits of adopting the NIST-CSF.

**Module 2: Framework Structure**

* Explain the structure of the NIST-CSF Core.
* Understand profiles and tiers and their relationships.
* Learn to use the NIST-CSF Online Reference tool.

**Module 3: Framework Core**

* Describe the structure and outcomes of the CSF Core.
* Understand category-level objectives within the framework.

**Module 4: CSF Profiles & CSF Tiers**

* Explain the use of CSF Profiles.
* Describe CSF Tiers and their applications.

**Module 5: COSO Enterprise Risk Management (ERM)**

* Understand COSO’s 20 principles in the context of the NIST-CSF.
* Discuss how culture influences organizational risk.

**Module 6: NIST CSF & NIST Privacy Framework**

* Describe the role of a privacy framework.
* Understand how the NIST Privacy Framework integrates with the CSF.

**Module 7: NIST-CSF and Resiliency**

* Define organizational resiliency in the context of NIST-CSF.

**Module 8: Adopt and Adapt the NIST-CSF**

* Describe the strategic importance of adopting the NIST-CSF.
* Explain leadership’s role in commitment and culture curation.
* Define organizational commitment to adoption.

**Module 9: Adopt the NIST-CSF**

* Define “Informative References” (IRs).
* Describe how to adapt IR controls to suit organizational needs.
* Understand how adaptation enhances organizational resiliency.

**Module 10: Beyond the Framework – DVMS Overlay**

* Explain DVMS overlay concepts.
* Understand the DVMS Z-X Model and its seven capabilities.
* Learn to identify performance gaps using the DVMS overlay.
* Explore the DVMS FastTrack™ approach.

**Examination Details**

| **Parameter** | **Details** |
| --- | --- |
| **Duration** | 60 minutes |
| **Format** | 40 multiple-choice questions (4 options each) |
| **Delivery** | Paper-based or online, proctored |
| **Bloom’s Levels** | Level 1 – Knowledge; Level 2 – Comprehension |
| **Scoring** | 1 point per question; 60% to pass (24/40) |
| **Closed Book** | Yes |