Dell NIST Cybersecurity Framework 2.0

Certification Description

[Proven Professional Website]

Engage with your peers in our [Proven Professional Community]

Certification Overview

This certification benefits any professional who needs to demonstrate their ability to implement the NIST framework components to drive improved cybersecurity practices into the data center.

Certification Requirements

To successfully complete this certification, a candidate must:

1. Have a sufficient knowledge by consuming the recommended training and on the job experience.

2. Pass the Dell NIST Cybersecurity Framework exam.

Note: These details reflect certification requirements as of September 22nd, 2024.

The Proven Professional Program periodically updates Certifications to reflect technical currency and relevance. Please check the Proven Professional website regularly for the latest information.

Dell Technologies Partners: Achieving a certification validates capability; however, it does not imply authorization to deliver services. Services Competencies provide partners with the ability to deliver services under their own brand or co-deliver with Dell Technologies. Tiered partners are eligible to obtain Services Competencies upon completing the specific requirements outlined in the Services Competencies Matrix. Only partners that have met these requirements should be delivering their own services in lieu of Dell Technologies Services.

Dell Technologies
1 Dell Way
Round Rock Texas 78682

Dell NIST Cybersecurity Framework 2.0

Exam Description

Duration

90 Minutes

Exam Overview

This exam focuses on the knowledge and skills required to understand, implement, and utilize the Dell NIST Cybersecurity Framework (CSF) 2.0. Candidates will be assessed on their ability to understand the CSF 2.0, apply the CSF 2.0 Functions, implement Cybersecurity practices, manage Cybersecurity risks, and integrate CSF 2.0 into organizational processes. By passing this exam, candidates will demonstrate their competency in utilizing the CSF 2.0 to improve an organization's cybersecurity posture and resilience. This certification is suitable for cybersecurity professionals, IT managers, risk managers, and anyone responsible for implementing or overseeing cybersecurity programs.

Exam Topics

Topics likely to be covered on this exam include:

NIST CSF 2.0 Introduction (8%)

- Identify the increasing data security threats to IT systems and data.
- Define the reasons why an effective cybersecurity stance is important.
- Explain the purpose and the key changes of the NIST CSF 2.0 framework.
- Describe the NIST CSF 2.0 components.
- Identify the six NIST CSF 2.0 Core Functions.

NIST Framework: GOVERN Function (18%)

- Describe GOVERN Function and its relationship with the Enterprise Risk Management (ERM).
- Explain GOVERN Function categories and subcategories.
- Define the organizational context and risk management strategy.
- Establish clear policies and procedures to guide cybersecurity activities.
- Define clear roles and responsibilities for cybersecurity personnel.
- Identify and manage cybersecurity risks associated with suppliers and third-party vendors.

NIST Framework: IDENTITY Function (18%)

- Explain IDENTITY Function with its categories and subcategories.
- Identify and inventory all assets and categorize them based on their criticality and sensitivity.
- Assign ownership and responsibility for each asset.
- List the tools and techniques used in asset management.
- Describe risk assessment.
- Describe the controls and techniques in the Incident Response Life Cycle, Contingency Plan, and Business Continuity Plan.

Dell Technologies
1 Dell Way
Round Rock Texas 78682

NIST Framework: PROTECT Function (12%)

- Explain the PROTECT Function, its categories, and subcategories.
- Learn about the processes and controls involved in identity management, authentication, and access control.
- Understand the need for awareness and training.
- Learn about the processes and controls involved in data and platform security.
- Understand the processes and controls involved in technology infrastructure resilience.

NIST Framework: DETECT Function (7%)

- Explain the categories and subcategories of the DETECT Function.
- Describe the significance of continuous monitoring and associated security controls in the DETECT Function.
- Describe the significance of adverse event analysis and associated security controls in DETECT Function.
- Elaborate the tools and techniques that can be employed for achieving continuous monitoring and adverse event analysis.

NIST Framework: RESPOND Function (8%)

- Understand the basic concepts and categories of the RESPOND Function.
- Learn about the processes involved in managing incidents.
- Gain knowledge on analyzing incidents with a focus on controls.
- Comprehend the reporting and communication aspects of incident response.
- Understand the strategies and techniques to minimize the impact of an incident.

NIST Framework: RECOVER Function (7%)

- Explain the categories and subcategories of the RECOVER Function.
- Analyze the significance of incident recovery plan execution and associated security controls in the RECOVER Function.
- Explain the significance of incident recovery communication and associated security controls in the RECOVER Function.
- Elaborate the tools and techniques that can be employed for incident recovery plan execution.

Analyze NIST CSF Profiles (7%)

- Understand the concept of NIST CSF Organizational Profiles.
- Explore different Organizational Profiles.
- Discover how to develop and apply Organizational Profiles.
- Understand the application of NIST CSF Profiles in practical scenarios.

Applying NIST CSF Tiers (5%)

- Grasp core concepts and structure of Cybersecurity Framework (CSF) tiers.
- Choose appropriate tiers for risk governance and management.
- Apply the NIST CSF tiers in practical scenarios.

Assess Cybersecurity Risk Communication and Integration (10%)

- Explain cybersecurity risks and their impact on organizations.
- Utilize effective communication strategies to convey cybersecurity risks.
- Integrate cybersecurity risk management into broader enterprise risk management programs.
- Explain the importance of Supply Chain Risk Management (SCRM) in cybersecurity.
- Identify and manage the risks associated with emerging technologies, such as AI.
- Describe AI risk management frameworks, tools, and techniques.

The percentage after each topic above reflects the approximate distribution of the total question set across the exam.

Recommended Training

The following curriculum is recommended for candidates preparing to take this exam.

Courses	Course ID	Mode
Implementing the NIST Cybersecurity Framework 2.0	ESDTFD06684	On Demand
Implementing the NIST Cybersecurity Framework 2.0	ESDTFS06683	Virtual Classroom/ Classroom

Note: These exam description details reflect contents as of the exam publish date.