D-CSF-SC-23

NIST Cybersecurity Framework

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 knowledgebase/skill set through hands-on product experience and/or by consuming the recommended training.
2. Pass the NIST Cybersecurity Framework exam.

Note: These details reflect certification requirements as of February 6, 2023.

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 Technologies

D-CSF-SC-23

Exam Overview

The exam covers high level framework topics as well as detailed underlying processes that support framework implementation. This includes the framework core, tiers and profiles which allow CSIRT staff to evaluate risk and prioritize feature changes based on business needs and changes in the security landscape.

Exam Topics

Topics likely to be covered on this exam include:

NIST Framework Overview (10%)

- Describe the NIST Framework architecture and purpose including the Core, Tiers, and Profiles
- Describe the topics associated with the Category layer and explain how they align to the NIST Framework functions

NIST Framework: Identify Function (18%)

- Describe what constitutes an asset and which assets need to be protected
- Describe the "who/what/why" of a continuously updated inventory
- Describe how discovery and inventory facilitates the planning efforts associated with Disaster Recovery, Incident Response, Communications, and Business Impact Analysis
- Describe the controls for the inventory classification and explain the KPIs developed around these controls

NIST Framework: Protect Function (23%)

- Describe the need for creating and documenting a baseline configuration
- Explain how the Business Impact Analysis is integral to the protect function
- Describe the role of the Business Continuity Plan and Business Impact Analysis
- Describe the maintenance and access control subcategory controls for the protect function
- Describe the awareness training, data security and protective technology subcategory controls of the protect function

NIST Framework: Detect Function (17%)

- Describe the anatomy of a breach, including what constitutes a breach, why and how it happens, and the steps to avoid a breach
- Identify the methods of detection and how detection can be implemented
- Describe the concept and benefits of continuous monitoring
- Identify and explain the subcategories associated with detection and analysis

NIST Framework: Respond Function (17%)

- Describe how to quantify the extent of a security breach
- Describe how to contain a security breach
- Understand and construct an effective Incident Response Plan
- Describe the purpose and details of an effective Communications Plan
- Describe the after action plan and review

NIST Framework: Recover Function (15%)

- Determine and describe the considerations when implementing a Disaster Recovery Plan (DRP)
- Describe how the BCP (Business Continuity Plan) supports “timely recovery to normal operations to reduce the impact from a cybersecurity incident.”
- Assess and describe the requirements and processes to return to "business as usual"
- Describe the process of understanding the impact to the business, including reputation and revenue

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

Duration

90 minutes

Recommended Training

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

Course Title	Course Number	Mode	Available
Introduction to Cybersecurity Frameworks (pre-requisite)	ES101DSY00354/ ES131DSY00354	eLearning	10/1/2022
Implementing the NIST Cybersecurity Framework	ES102DSY00786/ ES132DSY00786	eLearning	10/1/2022

Note: These exam description details reflect contents as of February 6, 2023