Heimdal®

NIST Cybersecurity Framework Policy Template Guide

The purpose of this document is to provide a comprehensive template for organizations seeking to assess their compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risk.

The framework's adaptable nature allows it to be implemented across various sectors and organizations, regardless of size or cybersecurity risk profile.

This template is designed to guide organizations through a detailed self-assessment of their cybersecurity practices across the NIST CSF's five core functions: Identify, Protect, Detect, Respond, and Recover.

Organization Details

- **Organization Name:**
- **Assessment Date:**
- **Assessment Team Members:**
- **Confidentiality Level of Assessment:**

Framework Adoption Overview

Description of current cybersecurity practices:

NIST CSF Core Functions Adopted:

Identify	Protect	Detect	Respond	Recover

NIST CSF Core Functions Assessment

Identify Function

The Identify function assists in developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

- Asset Management (ID.AM)

ID.AM-1: Physical and software assets are inventoried. Detail how assets are inventoried, frequency of updates, and responsible parties.
ID.AM-2: External information systems are cataloged. Describe the process for cataloging and managing external systems and services.

- Business Environment (ID.BE)

ID.BE-1: The organization's role in the supply chain is identified and communicated. Explain supply chain risk management practices.

- Governance (ID.GV)

ID.GV-1: Cybersecurity governance policies are established and communicated. List key governance policies and their dissemination methods.

- Risk Assessment (ID.RA)

ID.RA-1: Cybersecurity risk to organizational operations is assessed. Describe the risk assessment process and frequency.

- Risk Management Strategy (ID.RM)

ID.RM-1: Risk management processes are established, managed, and agreed upon by organizational stakeholders. Detail the risk management framework and stakeholder involvement.

Protect Function

The Protect function outlines appropriate safeguards to ensure delivery of critical infrastructure services.

- Access Control (PR.AC)

PR.AC-1: Access to assets and associated facilities is limited to authorized users, processes, or devices. Specify access control policies and procedures.

- Awareness and Training (PR.AT)

PR.AT-1: Personnel and partners are given cybersecurity awareness training. Outline training programs and schedules.

Detect Function

The Detect function defines the appropriate activities to identify the occurrence of a cybersecurity event.

- Anomalies and Events (DE.AE)

DE.AE-1: Anomalous activity is detected, and the potential impact of events is understood. Explain detection capabilities and event impact analysis processes.

Respond Function

The Respond function includes activities to take action regarding a detected cybersecurity incident.

- Response Planning (RS.RP)

RS.RP-1: Response processes and procedures are executed and maintained. Detail incident response plans and update mechanisms.

Recover Function

The Recover function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

- Recovery Planning (RC.RP)

RC.RP-1: Recovery processes and procedures are executed and maintained to ensure timely recovery of operations. Explain recovery strategies and backup processes.

Additional Assessment Sections

Strengths, Weaknesses, Opportunities for Improvement, and Action Plan

- **Strengths:** Detail areas where the organization excels in its cybersecurity practices.
- **Weaknesses:** Identify specific areas where improvements are needed.
- **Opportunities for Improvement:** Suggest potential enhancements in cybersecurity practices.
- **Action Plan:** Develop a prioritized list of actions to address identified gaps and weaknesses.

Conclusion

This template serves as a foundational tool for organizations to conduct a thorough self-assessment of their adherence to the NIST Cybersecurity Framework.

By meticulously evaluating each category and subcategory, organizations can gain a clear understanding of their cybersecurity posture, identify critical vulnerabilities, and implement strategic improvements.

Regular updates and reassessments are vital to adapting to evolving cybersecurity threats and ensuring the ongoing protection of critical assets.