**NIST CSF Survey
User Guide**

**Overview**

**Purpose**

**What is the NIST?**

NIST is the abbreviated name of the **National Institute of Standards and Technology**. It’s one of many federal agencies under the U.S. Department of Commerce and was formed to advance measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST is an essential resource for advancing technology and improving security across industries in the United States. The government endorses NIST policies and companies often choose to follow them because they are the best security practices regardless of industry.

One of the most followed NIST guidelines is the Cybersecurity Framework which delivers fundamental protocols for various organizations and industries to ensure their infrastructure remains secure.

**What is the NIST Cybersecurity Framework?**

NIST's Cybersecurity Framework (CSF) is a voluntary set of guidelines and recommendations that combine industry standards and best practices to help organizations manage their cybersecurity risks. It was developed in 2014 and consists of a framework of policies that describe how an organization can improve its ability to detect, respond, and prevent a cyber-attack. This framework offers a complete system of methods for detecting and managing cyber risks.

The Framework Core achieves this by using straightforward language to describe sets of desired cybersecurity activities and their outcomes. The Framework is organized by five key Core Functions – **Identify**, **Protect**, **Detect**, **Respond**, **Recover**. These five terms, when considered together, provide a comprehensive view of the lifecycle for managing cybersecurity over time.

|  |  |
| --- | --- |
| **Core Function** | **Description** |
| **IDENTIFY** | Organizations manage cybersecurity risk to systems, people, assets, data, and capabilities. |
| **PROTECT** | Develop and implement appropriate safeguards to ensure the delivery of critical protective services. |
| **DETECT** | Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The detect function enables the timely discovery of cybersecurity events. |
| **RESPOND** | Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. |
| **RECOVER** | Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. |

**Categories and Subcategories**

Each of the CSF core functions is comprised of outcome categories that describe the kinds of processes and tasks organizational units should deploy at the core functional level. Subcategories are the deepest level of abstraction in the Core. There are 108 Subcategories, which are outcome-driven statements that provide considerations for creating or improving a cybersecurity program. Because the Framework is outcome driven and does not mandate how an organization must achieve those outcomes, it enables risk-based implementations that are customized to the organization's needs.

**Core Functions**

 **IDENTIFY**

The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. The Identify function contains six outcome categories which in turn comprises subcategory activities.

1. **IDENTIFY – Considerations and activities**
	1. **Identify critical organizational unit processes and assets** – What are your organizational unit’s activities that absolutely must continue in order to be viable?
	2. **Document information flows** – It’s important to not only understand what type of information your organizational unit collects and uses, but also to understand where the data is located and flows, especially where contracts and external partners are engaged.
	3. **Maintain hardware and software inventory** – It’s important to understand the computers and software in your organizational unit because these are frequently the entry points of malicious actors. This inventory could be as simple as a spreadsheet or using a more centralized tool such as **INSERT EXAMPLE TOOL HERE**.
	4. **Establish policies for cybersecurity that include roles and responsibilities** – These policies and procedures should clearly describe your organizational unit’s expectations for how cybersecurity activities will protect your data, systems, and how they support critical organizational unit processes. Cybersecurity policies should be integrated with other organizational unit risk considerations (such as financial, reputational).
	5. **Identify threats, vulnerabilities, and risk to assets** – Ensure risk management processes are established and managed to ensure internal and external threats are identified, assessed, and documented in risk registers. Ensure risk responses are identified and prioritized, executed, and results monitored.
2. **IDENTIFY – Categories**
	1. **Asset Management (ID.AM)** - all physical assets (devices and systems), software, communication workflows, external information systems, prioritized resources, and roles relating to cybersecurity documented and inventoried.
		1. Taken inventory of all physical devices and systems;
		2. Taken inventory of all software platforms and applications;
		3. Mapping of communication and data flows;
		4. Catalogued its external information systems;
		5. Prioritized resources (hardware, devices, data, time, personnel, and software) according to their classification, level of importance (criticality), and business value; and
			1. Established cybersecurity roles and responsibilities enterprise-wide and for third-party stakeholders (suppliers, customers, partners).
		* **ID.AM-1: Physical devices and systems within the organization are inventoried**
			1. Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers.
			2. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network.
			3. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments.
			4. Additionally, it includes assets that are regularly connected to the enterprise’s network infrastructure, even if they are not under control of the enterprise.
			5. Review and update the inventory of all enterprise assets bi-annually, or more frequently.
		1. **ID.AM-2: Software platforms and applications within the organization are inventoried**
			1. Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory should document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.
			2. Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise’s mission, document an exception detailing mitigating controls and residual risk acceptance.
			3. Are organizational staff, vendors or contractors allowed to install software on their devices.
			4. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.
			5. Establish and manage an updated inventory of third-party components used in development, often referred to as a “bill of materials,” as well as components slated for future use.
			6. Evaluate the list frequently to identify any changes or updates to these components, and validate that the component is still supported
		2. **ID.AM-4: External information systems are catalogued**
			1. Establish and maintain architecture diagram(s) and/or other network system documentation.
			2. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
		3. **ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value**
			1. Establish and maintain a data inventory, based on the enterprise’s data management process. Inventory sensitive data, at a minimum. Review and update inventory frequently with a priority on sensitive data.