Justice Guardian - Navigating Cybersecurity:
Identify Core Function, NIST Cyber Security Framework for Command Staff

What Is It?
The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides high-level cybersecurity objectives, structured around six Core Functions (Govern, Identify, Protect, Detect, Respond, and Recover) that aid agencies in understanding, assessing, prioritizing, and communicating their efforts. The Identify function is foundational to the framework helps organizations understand their assets, systems, data, and capabilities, as well as their cybersecurity environment, threats, vulnerabilities, and risks.

Why Does It Matter?
The Identify function is essential for establishing an effective cybersecurity program. Without a clear understanding of what needs to be protected and why, organizations cannot make informed decisions about how to protect it. The Identify function helps organizations align their cybersecurity activities with their business objectives, mission, values, and comply with relevant regulations and standards. The Identify function also supports the other four functions of the framework. By identifying their assets and risks, organizations can better protect them from unauthorized access, use, or modification.

What To Do
The Identify function consists of six categories: 1) Asset Management 2) Business Environment 3) Governance 4) Risk Assessment 5) Risk Management Strategy 6) Supply Chain Risk Management. The framework does not prescribe a specific way to implement the Identify function. Rather, it allows organizations to customize their approach based on their needs, goals, and resources. However, some general steps that leadership should take to initiate and execute the Identify function are:

- Establish a cross-functional team that includes representatives from different organizational units, such as IT, legal, finance, human resources, and operations.
- Define the scope and boundaries of the cybersecurity program, and identify the critical assets, systems, data, and capabilities that need to be protected.
- Conduct a comprehensive and ongoing risk assessment to identify the cybersecurity threats, vulnerabilities, and impacts that could affect the organization.
- Develop and document a risk management strategy that defines the organization’s risk appetite, tolerance, and thresholds, and guides the selection and implementation of cybersecurity controls.

Considerations
The Identify function is not a one-time activity, but a continuous process that requires regular review and update, especially when there are changes in the organization’s assets, environment, threats, or risks. The Identify function should be aligned and integrated with the organization’s overall risk management and strategic planning processes, and should support the organization’s mission, vision, and values. The Identify function should involve the participation and collaboration of all relevant stakeholders, both internal and external, and should foster a culture of cybersecurity awareness and responsibility.

Further Reading & Resources
- NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

---

1 This Justice Guardian builds on the information provided in "Justice Guardian - Navigating Cybersecurity: Determining a Framework," which should be read first.
2 https://www.nist.gov/cyberframework
3 The Govern Core Function is new to version 2.0 and moves multiple subcategories to new Core Functions. This document follows the draft version of 2.0, as of January 2024, and will be updated when the final version is released.
Technical Insight

The Identify function of the NIST Cybersecurity Framework helps organizations to understand and manage their cybersecurity risks. Technical implementers of the Identify function are responsible for collecting, analyzing, and reporting data on the organization’s assets, vulnerabilities, threats, and controls.

Technical Details

Technical implementers of the Identify function have several responsibilities that are crucial to the execution of the Identify function of CSF. The foundational tasks involve the identification and inventory of the organization’s physical and logical assets, such as devices, systems, networks, data, and users. Implementers must assess the current state of the organization's cybersecurity posture, such as the level of protection, detection, and response capabilities, as well as identify and prioritize the organization's cybersecurity risks, such as the likelihood and impact of potential threats and vulnerabilities. Establishing and documenting the organization’s risk management strategy, such as the risk appetite, tolerance, and mitigation plans is also a key step in the implementation of the Identify function.

What To Do

Technical implementers of the Identify function should take the following steps to commence implementation:

- Review the Identify function and its subcategories in the NIST cybersecurity framework and select the relevant ones for the organization.
- Use existing or develop new tools and methods to collect and analyze data on the organization's assets, vulnerabilities, threats, and controls.
- Communicate and collaborate with other stakeholders, such as senior management, business units, and external partners, to share information and align on the organization's risk management strategy.

Technical Considerations

Technical implementers should use diligence to help ensure the data collected and analyzed for the Identify function is accurate, complete, and up-to-date, and the tools and methods used should be secure, reliable, and scalable. Ideally, these tools are already in operation and are integrated with the organization’s existing systems and processes. The Identify function should be aligned with the other core functions of the NIST cybersecurity framework, such as Protect, Detect, Respond, and Recover, and should support the organization’s overall cybersecurity goals and objectives.

Additional Help

Technical implementers of the Identify function may find the following resources helpful:

- The NIST Cybersecurity Framework Implementation Tiers, which provide guidance on how to apply the framework based on the organization's current and desired level of cybersecurity maturity.
- The NIST Cybersecurity Framework Profiles, which provide examples of how to customize the framework based on the organization's specific needs and priorities.
- The NIST Cybersecurity Framework Online Informative References, which provide links to various standards, guidelines, and best practices that support the implementation of the framework.

Further Reading & Resources

- NIST Special Publication 1271, Getting Started with NIST Cybersecurity Framework: A Quick Start Guide
- NIST CSF 2.0 Implementation Examples

---

4 This page builds on the information provided in the “for Command Staff” page.