NIST Special Publication 1271
https://doi.org/10.6028/NIST.SP.1271
August 2021

Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide

Amy Mahn[1], Jeffrey Marron[1], Stephen Quinn[2], Daniel Topper[3]

[1] NIST Applied Cybersecurity Division, Information Technology Laboratory
[2] NIST Computer Security Division, Information Technology Laboratory
[3] Huntington Ingalls Industries

What is the NIST Cybersecurity Framework, and how can my organization use it?

The NIST Cybersecurity Framework[4] can help an organization begin or improve their cybersecurity program. Built off of practices that are known to be effective, it can help organizations improve their cybersecurity posture. It fosters communication among both internal and external stakeholders about cybersecurity, and for larger organizations, helps to better integrate and align cybersecurity risk management with broader enterprise risk management processes as described in the NISTIR 8286[5] series.

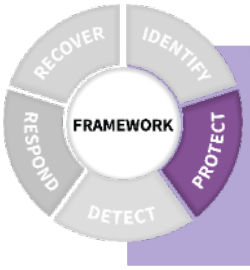
The Framework is organized by five key Functions – Identify, Protect, Detect, Respond, Recover. These five widely understood terms, when considered together, provide a comprehensive view of the lifecycle for managing cybersecurity risk over time. The activities listed under each Function may offer a good starting point for your organization:

IDENTIFY

Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.

- **Identify critical enterprise processes and assets** – What are your enterprise's activities that absolutely must continue in order to be viable? For example, this could be maintaining a website to retrieve payments, protecting customer/patient information securely, or ensuring that the information your enterprise collects remains accessible and accurate.
- **Document information flows** – It's important to not only understand what type of information your enterprise collects and uses, but also to understand where the data is located and and how it is used, especially where contracts and external partners are engaged.
- **Maintain hardware and software inventory** – It's important to have an understanding of the computers and software in your enterprise because these are frequently the entry points of malicious actors. This inventory could be as simple as a spreadsheet.
- **Establish policies for cybersecurity that include roles and responsibilities** – These policies and procedures should clearly describe your expectations for how cybersecurity activities will protect your information and systems, and how they support critical enterprise processes. Cybersecurity policies should be integrated with other enterprise risk considerations (e.g., financial, reputational).
- **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.

[4] https://www.nist.gov/cyberframework
[5] https://csrc.nist.gov/publications/detail/nistir/8286/final



PROTECT

Develop and implement the appropriate safeguards to ensure delivery of services.

- **Manage access to assets and information** – Create unique accounts for each employee and ensure that users only have access to information, computers, and applications that are needed for their jobs. Authenticate users (e.g., passwords, multi-factor techniques) before they are granted access to information, computers, and applications. Tightly manage and track physical access to devices.

- **Protect sensitive data** – If your enterprise stores or transmits sensitive data, make sure that this data is protected by encryption both while it's stored on computers as well as when it's transmitted to other parties. Consider utilizing integrity checking to ensure only approved changes to the data have been made. Securely delete and/or destroy data when it's no longer needed or required for compliance purposes.

- **Conduct regular backups** – Many operating systems have built-in backup capabilities; software and cloud solutions are also available that can automate the backup process. A good practice is to keep one frequently backed up set of data offline to protect it against ransomware.
- **Protect your devices** – Consider installing host-based firewalls and other protections such as endpoint security products. Apply uniform configurations to devices and control changes to device configurations. Disable device services or features that are not necessary to support mission functions. Ensure that there is a policy and that devices are disposed of securely.
- **Manage device vulnerabilities** – Regularly update both the operating system and applications that are installed on your computers and other devices to protect them from attack. If possible, enable automatic updates. Consider using software tools to scan devices for additional vulnerabilities; remediate vulnerabilities with high likelihood and/or impact.
- **Train users** – Regularly train and retrain all users to be sure that they are aware of enterprise cybersecurity policies and procedures and their specific roles and responsibilities as a condition of employment.

DETECT

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

- **Test and update detection processes –** Develop and test processes and procedures for detecting unauthorized entities and actions on the networks and in the physical environment, including personnel activity. Staff should be aware of their roles and responsibilities for detection and related reporting both within your organization and to external governance and legal authorities.

- **Know the expected data flows for your enterprise** – If you know what and how data is expected to be used for your enterprise, you are much more likely to notice when the unexpected happens – and unexpected is never a good thing when it comes to cybersecurity. Unexpected data flows might include customer information being exported from an internal database and exiting the network. If you have contracted work to a cloud or managed service provider, discuss with them how they track data flows and report, including unexpected events.

- **Maintain and monitor logs** – Logs are crucial in order to identify anomalies in your enterprise's computers and applications. These logs record events such as changes to systems or accounts as well as the initiation of communication channels. Consider using software tools that can aggregate these logs and look for patterns or anomalies from expected network behavior.

RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

- **Ensure response plans are tested** – It's even more important to test response plans to make sure each person knows their responsibilities in executing the plan. The better prepared your organization is, the more effective the response is likely to be. This includes knowing any legal reporting requirements or required information sharing.

- **Ensure response plans are updated** – Testing the plan (and execution during an incident) inevitably will reveal needed improvements. Be sure to update response plans with lessons learned.

RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.

- **Communicate with internal and external stakeholders** – Part of recovery depends upon effective communication. Your recovery plans need to carefully account for what, how, and when information will be shared with various stakeholders so that all interested parties receive the information they need but no inappropriate information is shared.

- **Understand the impact of cybersecurity events –** If a cybersecurity event is detected, your enterprise should work quickly and thoroughly to understand the breadth and depth of the impact. Seek help. Communicating information on the event with appropriate stakeholders will help keep you in good stead in terms of partners, oversight bodies, and others (potentially including investors) and improve policies and processes.

- **Coordinate with internal and external stakeholders** – It's important to make sure that your enterprise's response plans and updates include all key stakeholders and external service providers. They can contribute to improvements in planning and execution.

- **Ensure recovery plans are updated** – As with response plans, testing execution will improve employee and partner awareness and highlight areas for improvement. Be sure to update Recovery plans with lessons learned.

- **Manage public relations and company reputation** – One of the key aspects of recovery is managing the enterprise's reputation. When developing a recovery plan, consider how you will manage public relations so that your information sharing is accurate, complete, and timely – and not reactionary.