https://www.nist.gov/cyberframework/getting-started/quick-start-guide

**National Institute of
Standards and Technology**
U.S. Department of Commerce

[Cybersecurity Framework](https://www.nist.gov/cyberframework) (https://www.nist.gov/cyberframework)

Quick Start Guide

This Quick Start Guide intends to provide direction and guidance to those organizations – in any sector or community – seeking to improve cybersecurity risk management via utilization of the NIST Cybersecurity Framework. Though the Cybersecurity Framework is not a one-size-fits-all approach to managing cybersecurity risk for organizations, it is ultimately aimed at reducing and better managing these risks. As such, this guide is intended for any and all organizations regardless of sector or size. Organizations will vary in how they customize practices described in this document. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize impact.

The NIST Cybersecurity Framework (https://nvlpubs.nist.gov/nistpubs /CSWP/NIST.CSWP.04162018.pdf) 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 (https://csrc.nist.gov/publications/detail/nistir/8286/final) series.

The Framework is organized by five key Functions – Identify, Protect, Detect, Respond, and 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
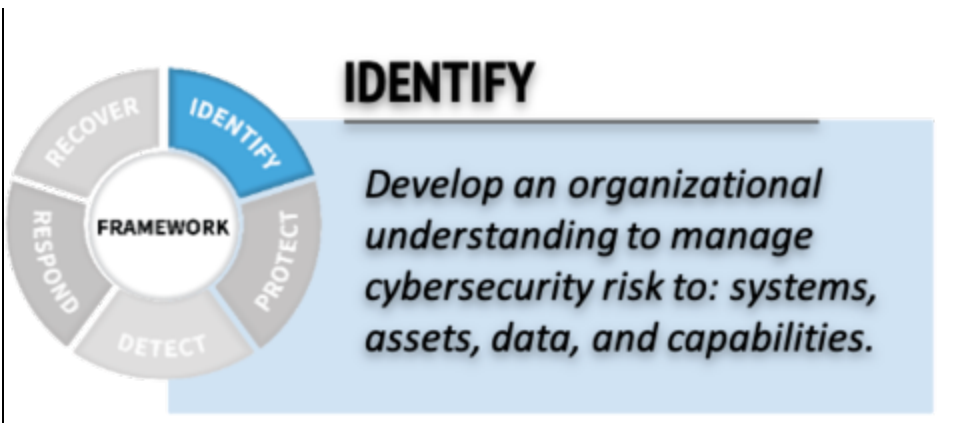
- **Identify critical enterprise processes and assets** – What are your enterprise's activities that absolutely must continue in order to be viable? For example, this could be maintaining a website to retrieve payments, protecting customer/patient information securely, or ensuring that the information 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 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.

Protect

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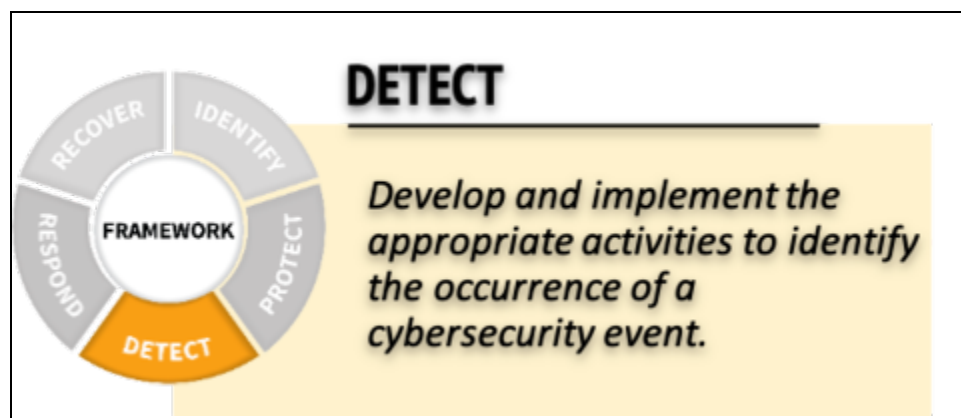
- **Test and update detection processes** – Develop and test processes and procedures for detecting unauthorized entities and actions on the networks and in the physical environment, including personnel activity. Staff should be aware of their roles and responsibilities for detection and related reporting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

- **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.
- **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.

Respond

- **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.
- **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.

Recover
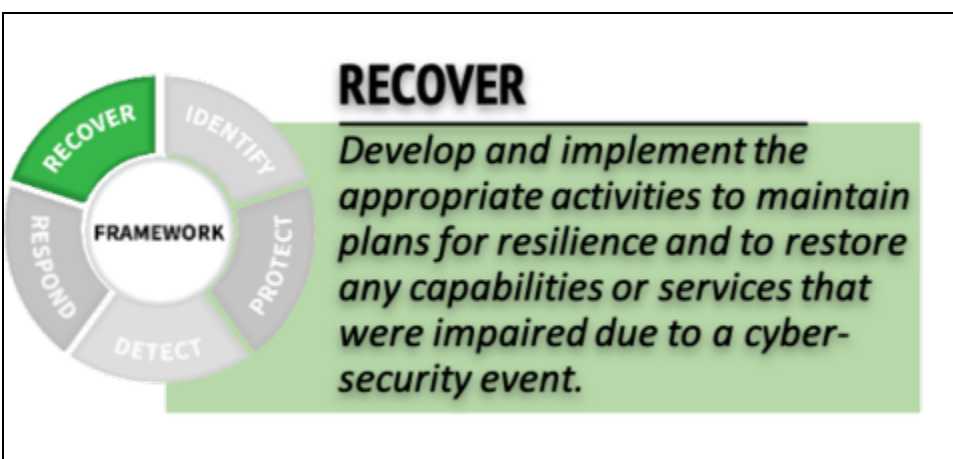
- **Communicate with internal and external stakeholders** – Part of recovery depends upon effective communication. Your recovery plans carefully account for what, how, and when information will be shared various stakeholders so that all interested parties receive the informa

need but no inappropriate information is shared.

- **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.

Download the PDF version of the quick start guide.

Quick Start Guide - English (https://doi.org/10.6028/NIST.SP.1271)
(PDF | 463 KB)

Quick Start Guide - Spanish (https://nvlpubs.nist.gov/nistpubs/SpecialPublications
/NIST.SP.1271es.pdf)
(PDF | 1.3 MB)

Quick Start Guide - Ukrainian (https://nvlpubs.nist.gov/nistpubs/SpecialPublications
/NIST.SP.1271.ukr.pdf)
(PDF | 1.1 MB)

Quick Start Guide - Portuguese (https://nvlpubs.nist.gov/nistpubs/SpecialPublications
/NIST.SP.1271pt.pdf)
(PDF | 1.3 MB)

Created January 23, 2023, Updated June 8, 2023