NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide

U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication
NIST SP 1300
https://doi.org/10.6028/NIST.SP.1300
February 2024

NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide Overview

Purpose

This guide provides small-to-medium sized businesses (SMB), specifically those who have modest or no cybersecurity plans in place, with considerations to kick-start their cybersecurity risk management strategy by using the NIST Cybersecurity Framework (CSF) 2.0. The guide also can assist other relatively small organizations, such as non-profits, government agencies, and schools. It is a supplement to the NIST CSF and is not intended to replace it.

What is the NIST Cybersecurity Framework?

The NIST Cybersecurity Framework is voluntary guidance that helps organizations —regardless of size, sector, or maturity— better **understand**, **assess**, **prioritize**, and **communicate** their cybersecurity efforts. The Framework is not a one-size-fits-all approach to managing cybersecurity risks. This supplement and the full CSF 2.0 can help organizations to consider and record their own risk tolerances, priorities, threats, vulnerabilities, requirements, etc.

Getting Started with the Cybersecurity Framework

The CSF organizes cybersecurity outcomes into six high-level Functions: Govern, Identify, Protect, Detect, Respond, and Recover. These Functions, when considered together, provide a comprehensive view of managing cybersecurity risk. The activities listed for each Function within this guide may offer a good starting point for your business. For specific, action-oriented examples of how to achieve the listed activities, reference the CSF 2.0 Implementation Examples. If there are activities contained within this guide that you do not understand or do not feel comfortable addressing yourself, this guide can serve as a discussion prompt with whomever you have chosen to help you reduce your cybersecurity risks, such as a managed security service provider (MSSP).

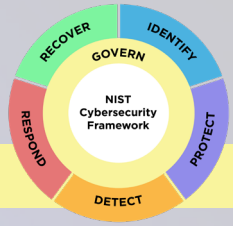
EXPLORE MORE CSF 2.0 RESOURCES

nist.gov/cyberframework

Quickly find what you need, including:

- ✓A suite of NEW Quick Start Guides
- ✓Implementation Examples
- ✓Search tools
- ✓FAQs
- ✓And much more!

GOVERN



The Govern Function helps you establish and monitor your business's cybersecurity risk management strategy, expectations, and policy.

Actions to Consider

Understand

- Understand how cybersecurity risks can disrupt achievement of your business's mission. *(GV.OC-01)*
- Understand your legal, regulatory, and contractual cybersecurity requirements. *(GV.OC-03)*
- Understand who within your business will be responsible for developing and executing the cybersecurity strategy. *(GV.RR-02)*

Assess

- Assess the potential impact of a total or partial loss of critical business assets and operations. *(GV.0C-04)*
- Assess whether cybersecurity insurance is appropriate for your business. *(GV.RM-04)*
- Assess cybersecurity risks posed by suppliers and other third parties before entering into formal relationships. *(GV.SC-06)*

Prioritize

- Prioritize managing cybersecurity risks alongside other business risks. *(GV.RM-03)*

Communicate

- Communicate leadership's support of a risk-aware, ethical, and continually improving culture. *(GV.RR-01)*
- Communicate, enforce, and maintain policies for managing cybersecurity risks. *(GV.PO-01)*

Getting Started with Cybersecurity Governance

You can use these tables to begin thinking about your cybersecurity governance strategy.

Setting Organizational Context	
Our business mission statement:	
What cybersecurity risks may prevent us from achieving this mission?	

Documenting Cybersecurity Requirements	
List your legal requirements:	
List your regulatory requirements:	
List your contractual requirements:	

Technical Deep Dive: Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

Questions to Consider

- As our business grows, how often are we reviewing our cybersecurity strategy?
- Do we need to upskill our existing staff, hire talent, or engage an external partner to help us establish and manage our cybersecurity plan?
- Do we have acceptable use policies in place for business and for employee-owned devices accessing business resources? Have employees been educated on these policies?

Related Resources

- Securing Small and Medium-Sized Supply Chains Resource Handbook
- Choosing A Vendor/Service Provider

View all NIST CSF 2.0 Resources Here

IDENTIFY

The Identify Function helps you determine the current cybersecurity risk to the business.

Actions to Consider

Understand

- Understand what assets your business relies upon by creating and maintaining an inventory of hardware, software, systems, and services. *(ID.AM-01/02/04)*

Assess

- Assess your assets (IT and physical) for potential vulnerabilities. *(ID.RA-01)*
- Assess the effectiveness of the business's cybersecurity program to identify areas that need improvement. *(ID.IM-01)*

Prioritize

- Prioritize inventorying and classifying your business data. *(ID.AM-07)*
- Prioritize documenting internal and external cybersecurity threats and associated responses using a risk register. *(ID.RA)*

Communicate

- Communicate cybersecurity plans, policies, and best practices to all staff and relevant third parties. *(ID.IM-04)*
- Communicate to staff the importance of identifying needed improvements to cybersecurity risk management processes, procedures, and activities. *(ID.IM)*

Getting Started with Identifying Current Cybersecurity Risk to Your Business

Before you can protect your assets, you need to identify them. Then you can determine the appropriate level of protection for each asset based upon its sensitivity and criticality to your business mission. You can use this sample table to get started on your information technology (IT) asset inventory. As your business matures, you might consider using an automated asset inventory solution or a managed security service provider to help you manage all your business assets.

Software/ hardware/ system/ service	Asset's official use:	Asset administrator or owner:	Identify sensitive data the asset has access to:	Is multi-factor authentication required to access this asset?	Risk to business if we lose access to this asset

Technical Deep Dive: Integrating Cybersecurity and Enterprise Risk Management

Questions to Consider

- What are our most critical business assets (data, hardware, software, systems, facilities, services, people, etc.) we need to protect?
- What are the cybersecurity and privacy risks associated with each asset?
- What technologies or services are personnel using to accomplish their work? Are these services or technologies secure and approved for use?

Related Resources

- NIST Risk Register Template
- Take Stock. Know What Sensitive Information You Have
- Evaluating Your Operational Resilience and Cybersecurity Practices

View all NIST CSF 2.0 Resources Here

PROTECT

The Protect Function supports your ability to use safeguards to prevent or reduce cybersecurity risks.

Actions to Consider

Understand

- Understand what information employees should or do have access to. Restrict sensitive information access to only those employees who need it to do their jobs. *(PR.AA-05)*

Assess

- Assess the timeliness, quality, and frequency of your company's cybersecurity training for employees. *(PR.AT-01/02)*

Prioritize

- Prioritize requiring multi-factor authentication on all accounts that offer it and consider using password managers to help you and your staff generate and protect strong passwords. *(PR.AA-03)*
- Prioritize changing default manufacturer passwords. *(PR.AA-01)*
- Prioritize regularly updating and patching software and operating systems. Enable automatic updates to help you remember. *(PR.PS-02)*
- Prioritize regularly backing up your data and testing your backups. *(PR.DS-11)*
- Prioritize configuring your tablets and laptops to enable full-disk encryption to protect data. *(PR.DS-01)*

Communicate

- Communicate to your staff how to recognize common attacks, report attacks or suspicious activity, and perform basic cyber hygiene tasks. *(PR.AT-01/02)*

Getting Started with Protecting Your Business

Enabling multi-factor authentication (MFA) is one of the fastest, cheapest ways you can protect your data. Start with accounts that can access the most sensitive information. Use this checklist to give you a head start, but remember your own list will be longer than this:

Account	MFA Enabled (Y/N)
Banking Account(s)	
Accounting and Tax Account(s)	
Merchant Account(s)	
Google, Microsoft, and/or Apple ID Account(s)	
Email Account(s)	
Password Manager(s)	
Website Account(s)	

Technical Deep Dive: NIST Digital Identity Guidelines

Questions to Consider

- Are we restricting access and privileges only to those who need it? Are we removing access when they no longer need it?
- How are we securely sanitizing and destroying data and data storage devices when they're no longer needed?
- Do employees possess the knowledge and skills to perform their jobs with security in mind?

Related Resources

- Cybersecurity Training Resources
- Multi-Factor Authentication
- Protecting Your Business from Phishing

View all NIST CSF 2.0 Resources Here

DETECT

The Detect Function provides outcomes that help you find and analyze possible cybersecurity attacks and compromises.

Actions to Consider

Understand

- Understand how to identify common indicators of a cybersecurity incident. *(DE.CM)*

Assess

- Assess your computing technologies and external services for deviations from expected or typical behavior. *(DE.CM-06/09)*
- Assess your physical environment for signs of tampering or suspicious activity. *(DE.CM-02)*

Prioritize

- Prioritize installing and maintaining antivirus and anti-malware software on all business devices—including servers, desktops and laptops. *(DE.CM-09)*
- Prioritize engaging a service provider to monitor computers and networks for suspicious activity if you don't have the resources to do it internally. *(DE.CM)*

Communicate

- Communicate with your authorized incident responder, such as an MSSP, about the relevant details from the incident to help them analyze and mitigate it. *(DE.AE-06/07)*

Getting Started with Detecting Incidents

Some common indicators of a cybersecurity incident are:

- Loss of usual access to data, applications, or services
- Unusually sluggish network
- Antivirus software alerts when it detects that a host is infected with malware
- Multiple failed login attempts
- An email administrator sees many bounced emails with suspicious content
- A network administrator notices an unusual deviation from typical network traffic flows

Technical Deep Dive: NIST Computer Security Incident Handling Guide

Questions to Consider

- Do devices that are used for our business, whether business-owned or employee-owned, have antivirus software installed?
- Do employees know how to detect possible cybersecurity attacks and how to report them?
- How is our business monitoring its logs and alerts to detect potential cyber incidents?

Related Resources

- Ransomware Protection and Response
- Detecting a Potential Intrusion
- Cybersecurity Training Resources

View all NIST CSF 2.0 Resources Here

RESPOND

The Respond Function supports your ability to take action regarding a detected cybersecurity incident.

Actions to Consider

Understand

- Understand what your incident response plan is and who has authority and responsibility for implementing various aspects of the plan. *(RS.MA-01)*

Assess

- Assess your ability to respond to a cybersecurity incident. *(RS.MA-01)*
- Assess the incident to determine its severity, what happened, and its root cause. *(RS.AN-03, RS.MA-03)*

Prioritize

- Prioritize taking steps to contain and eradicate the incident to prevent further damage. *(RS.MI)*

Communicate

- Communicate a confirmed cybersecurity incident with all internal and external stakeholders (e.g., customers, business partners, law enforcement agencies, regulatory bodies) as required by laws, regulations, contracts, or policies. *(RS.CO-02/03)*

Getting Started with an Incident Response Plan

Before an incident occurs, you want to be ready with a basic response plan. This will be customized based on the business but should include:

- ✓ **A business champion**: Someone who is responsible for developing and maintaining your incident response plan.
- ✓ **Who to call:** List all the individuals who may be part of your incident response efforts. Include their contact information, responsibilities, and authority.
- ✓ **What/when/how to report:** List your business's communications/reporting responsibilities as required by laws, regulations, contracts, or policies.

Technical Deep Dive: NIST Computer Security Incident Handling Guide

Contact	Phone
Business Leader:	
Technical Contact:	
State Police:	
Legal:	
Bank:	
Insurance:	

Questions to Consider

- Do we have a cybersecurity incident response plan? If so, have we practiced it to see if it is feasible?
- Do we know who the key internal and external stakeholders and decision-makers are who will assist if we have a confirmed cybersecurity incident?

Related Resources

- Incident Response Plan Basics
- FBI's Internet Crime Complaint Center
- Data Breach Response: A Guide for Business
- Best Practices for Victim Response and Reporting of Cyber Incidents

View all NIST CSF 2.0 Resources Here

RECOVER

The Recover Function involves activities to restore assets and operations that were impacted by a cybersecurity incident.

Actions to Consider

Understand

- Understand who within and outside your business has recovery responsibilities. *(RC.RP-01)*

Assess

- Assess what happened by preparing an after-action report—on your own or in consultation with a vendor/partner—that documents the incident, the response and recovery actions taken, and lessons learned. *(RC.RP-06)*
- Assess the integrity of your backed-up data and assets before using them for restoration. *(RC.RP-03)*

Prioritize

- Prioritize your recovery actions based on organizational needs, resources, and assets impacted. *(RC.RP-02)*

Communicate

- Communicate regularly and securely with internal and external stakeholders. *(RC.CO)*
- Communicate and document completion of the incident and resumption of normal activities. *(RC.RP-06)*

Getting Started with a Recovery Playbook

A playbook typically includes the following critical elements:

- ✓ A set of formal recovery processes
- ✓ Documentation of the criticality of organizational resources (e.g., people, facilities, technical components, external services)
- ✓ Documentation of systems that process and store organizational information, particularly key assets. This will help inform the order of restoration priority
- ✓ A list of personnel who will be responsible for defining and implementing recovery plans
- ✓ A comprehensive recovery communications plan

Technical Deep Dive: NIST Guide for Cybersecurity Event Recovery

Questions to Consider

- What are our lessons learned? How can we minimize the chances of a cybersecurity incident happening in the future?
- What are our legal, regulatory, and contractual obligations for communicating to internal and external stakeholders about a cybersecurity incident?
- How do we ensure that the recovery steps we are taking are not introducing new vulnerabilities to our business?

Related Resources

- Cybersecurity Training Resources
- Creating an IT Disaster Recovery Plan
- Backup and Recover Resources

View all NIST CSF 2.0 Resources Here

Profiles and Additional Resources

Using Organizational Profiles to Implement the Cybersecurity Framework

A *CSF Organizational Profile* describes an organization's current and/or target cybersecurity posture in terms of the CSF Core's cybersecurity outcomes. Every Organizational Profile includes one or both of the following:

1. A **Current Profile** specifies the desired outcomes an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved.
2. A **Target Profile** specifies the outcomes an organization has selected and prioritized for achieving its cybersecurity risk management objectives.
   - You can also use a **Community Profile** as the basis for your Target Profile. A Community Profile is a baseline of targeted outcomes for a particular sector, technology, threat type, or other use case.
   - You can also choose to use the **CSF Tiers** to inform your Profile creation. Tiers characterize the current or targeted rigor of an organization's practices by CSF Function or Category. See the *Quick-Start Guide for Using the CSF Tiers* for more information on Tiers and their use.

View the *Quick-Start Guide for Creating and Using Organizational Profiles* for more detailed information on how to get started creating Current and Target Profiles for your organization.

Additional Resources

The NIST Cybersecurity Framework Reference Tool allows users to explore the full CSF 2.0 Core in human and machine-readable versions (in JSON and Excel), while also maintaining resources with information to help you achieve your desired outcomes, such as:

- Mapping: Informative references are mappings indicating relationships between the CSF 2.0 and various standards, guidelines, regulations, and other content. They help inform how an organization may achieve the Core's outcomes.
- Implementation examples provide illustrations of concise, action-oriented steps to guide organizations in achieving the CSF outcomes. The examples are not a comprehensive list of all actions that could be taken by an organization, nor are they a baseline of required actions; they are a set of helpful examples to get organizations thinking about concrete steps.

NIST Cybersecurity and Privacy Reference Tool (CPRT) provides a simple way to access reference data from various NIST cybersecurity and privacy standards, guidelines, and Frameworks–downloadable in common formats (XLSX and JSON).

NIST SP 800-53 provides a catalog of security and privacy controls you can choose from. The controls are flexible, customizable, and implemented as part of an organization-wide process to manage risk. View and export from the Cybersecurity and Privacy Reference Tool (CPRT).

The Workforce Framework for Cybersecurity (NICE Framework) helps employers achieve the outcomes in the CSF 2.0 by assisting them to identify critical gaps in cybersecurity staffing and capabilities; determine and communicate position responsibilities and job descriptions; and provide staff training and career pathways.