NIST Internal Report
NIST IR 7621r2 ipd

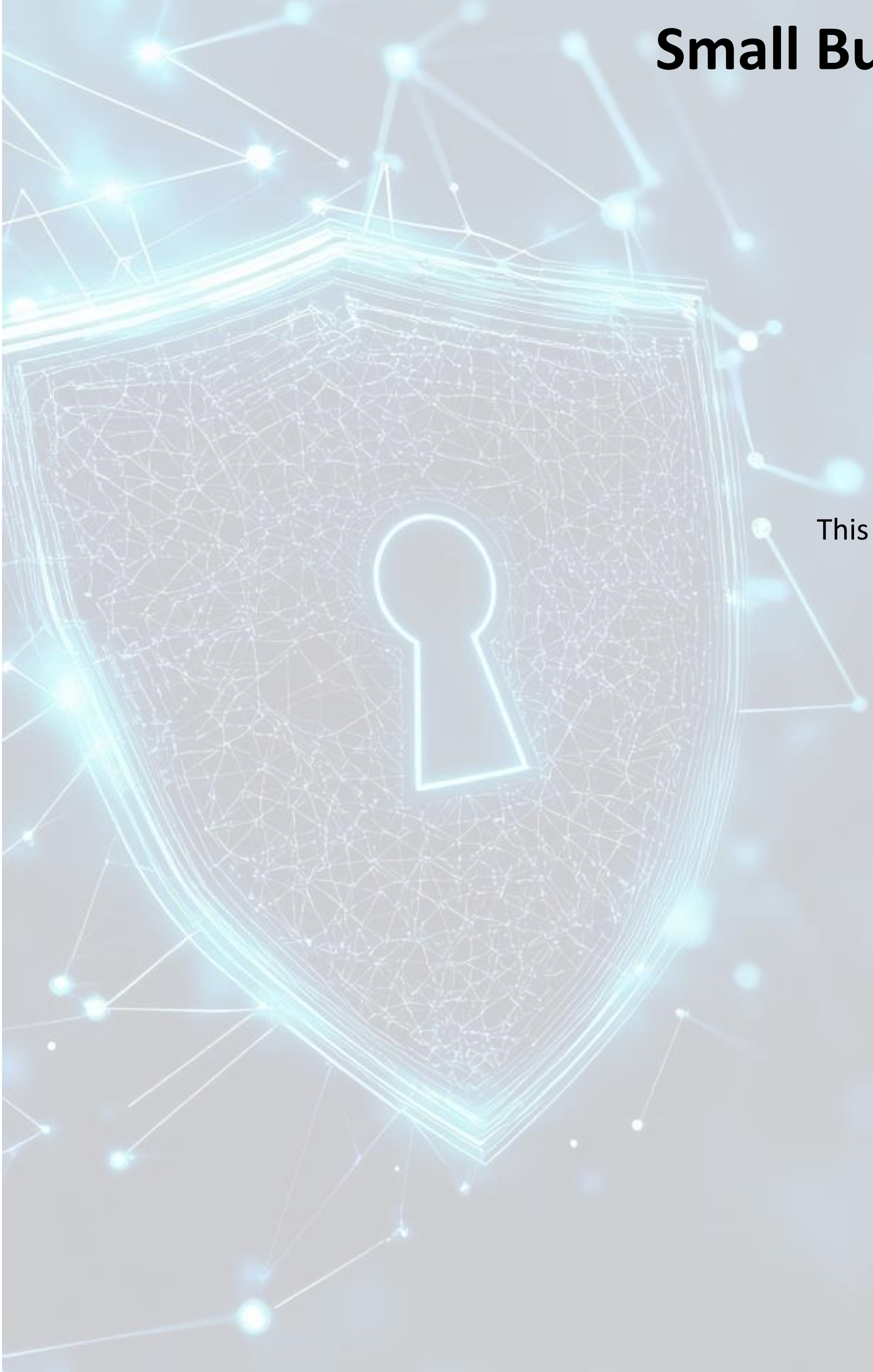
Small Business Cybersecurity:

Non-Employer Firms

Initial Public Draft

Daniel Eliot
Jeffrey A. Marron
Savann Thorn

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.7621r2.ipd



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

NIST Internal Report
NIST IR 7621r2 ipd

Small Business Cybersecurity:

Non-Employer Firms

Initial Public Draft

Daniel Eliot
Jeffrey A. Marron
Applied Cybersecurity Division
Information Technology Laboratory

Savann Thorn
National Programs Division
Hollings Manufacturing Extension Partnership

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.7621r2.ipd

May 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

How to Cite this NIST Technical Series Publication
Eliot D, Marron JA, Thorn S (2025) Small Business Cybersecurity: Non-Employer Firms. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 7621r2 ipd. https://doi.org/10.6028/NIST.IR.7621r2.ipd

Author ORCID iDs
Daniel Eliot: 0009-0006-3078-555X
Jeffrey A. Marron: 0000-0002-7871-683X
Savann Thorn: 0009-0003-1204-7682

Public Comment Period
May 1, 2025 – June 30, 2025

Submit Comments
ir7621-comments@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This report is designed to help small firms use the NIST Cybersecurity Framework (CSF) 2.0 to begin managing their cybersecurity risks. The document is tailored to the smallest of businesses—those with no employees, or “non-employer” firms. These firms are also often colloquially referred to as “solopreneurs.” The goal of the publication is to introduce fundamentals of a small business cybersecurity program in non-technical language at the earliest stage of a business to set a solid cybersecurity risk management foundation. Considerations for maturing cybersecurity risk management as the business scales are included to make the document useful for entities of varying sizes. This publication is not all-encompassing, and implementation of a cybersecurity risk management strategy will vary based on the organization’s sector, size, resources, and contractual or regulatory requirements.

Keywords

cybersecurity; Cybersecurity Framework (CSF); cybersecurity risk management; information security; small business.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL’s responsibilities include the development of management, administrative, technical, and physical standards and guidelines security and privacy of other than national security-related information in federal information systems.

Audience

According to the U.S. Small Business Administration Office of Advocacy, there are 34.8 million small businesses in the United States [3]. Of those, 81.7% have no paid employees other than the owner or owners—termed “non-employer firms.” This publication helps small firms with no employees use the NIST Cybersecurity Framework 2.0 to manage their cybersecurity risks. To make this information applicable to a broader audience, cybersecurity risk management considerations are included for businesses as they grow and hire employees—acknowledging that some non-employer firms may never hire additional employees. It is recognized that many small businesses rely upon consultants for their cybersecurity support. As such, consultants who provide cybersecurity support and services to the small business community are also a key audience for this report.

Note to Reviewers

NIST welcomes feedback and input on any aspect of this publication. NIST is also seeking responses to the following questions: Is the document's current level of specificity appropriate, too detailed, or too general? If the level of specificity is not appropriate, how can it be improved?

Acknowledgements

The authors would like to acknowledge the thorough and dedicated work the original NIST authors of NIST IR 7621, Celia Paulsen and Patricia Toth, put into creating this publication. We would also like to extend our thanks to Celia Paulsen, Patricia Toth, Stephen Quinn, Adam Sedgewick, and Karen Scarfone for providing input on this current revision.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: ir7621-comments@nist.gov.

Table of Contents

Executive Summary **1**

1. Introduction **2**

2. The NIST Cybersecurity Framework **8**

Govern Function (GV) 10

Identify Function (ID) 12

Protect Function (PR) 14

Detect Function (DE) 18

Respond Function (RS) 19

Recover Function (RC) 21

3. Conclusion **22**

References **23**

Appendix A. Glossary **25**

Appendix B. Acronyms **27**

Appendix C. Calculating, Documenting, Categorizing, and Prioritizing Cybersecurity Assets and Risks Worksheet **28**

Appendix D. Respond and Recover Worksheet **31**

Appendix E. Authentication Worksheet **33**

Appendix F. Change Log **34**

List of Tables

Table 1: Cybersecurity Risk Management Lifecycle **3**

Table 2: Getting Started with an Asset Inventory **4**

Table 3: The Six Functions of the CSF **8**

Table 4: Column Headings with Descriptions **9**

Table 5: Documenting Legal, Regulatory, and Contractual Cybersecurity Requirements **11**

Table 6: MFA Starter Checklist **15**

Table 7: Sample Response Contact Table **20**

Table 8: Sample Asset Categorization-Appendix **29**

Table 9: Sample Potential Events and Risks to Assets-Appendix **30**

Table 10: Sample Contact Table-Appendix **31**

Table 11: Sample Reporting Requirements Table-Appendix **32**

Table 12: Sample MFA Table-Appendix **33**

Table 13: Sample Default Manufacturer Passwords Table-Appendix **33**

List of Figures

Figure 1: Notional Architecture for Non-Employer Firm.......... 4

Figure 2: The Cybersecurity Framework Functions 8

Executive Summary

Small businesses are a substantial and critical part of the U.S. and global economy. According to the U.S. Small Business Administration Office of Advocacy [3], there are 34.8 million small businesses in the United States, comprising 99% of all U.S. businesses. Of those, 81.7% are non-employer firms with no paid employees other than the owners of the business. These businesses, though small in size, are represented in every industry and sector of the economy and contribute significantly to the Nation's innovation and industrial competitiveness.

As small businesses have become more reliant upon data and technology to operate and scale a modern business, cybersecurity has become a fundamental risk that must be addressed alongside other business risks (e.g., financial risks, natural disasters, competitors) as part of broader enterprise risk management (ERM) planning. A cybersecurity incident can be devastating to a small business and can negatively impact its ability to deliver goods and services, with effects cascading to customers, employees, business partners, and potentially the community. Establishing a strong cybersecurity culture early in the business' development, even before employees are hired, creates a foundation from which to build a resilient business in the face of ever-increasing cybersecurity risks. No business - of any size - can prevent every cybersecurity incident from occurring. But it can implement a cybersecurity plan that will enhance security while achieving business objectives.

> *"No business - of any size - can prevent every cybersecurity incident from occurring. But it can implement a cybersecurity plan that will enhance security while delivering business objectives."*

NIST IR 7621, Revision 2 Updates

One of the most significant changes to this revision is its narrowed scope. The previous versions of this publication discussed the broader topic of information security. To simplify and focus the content, this revised publication is now focused specifically on cybersecurity, which is a subset of information security. Based on community input, the audience has also been narrowed. Whereas prior versions were focused generally on "small business," which is a very broad and diverse population, this revision is tailored to a more specific population—non-employer firms [2]. Subsequent publications within this series may address other business populations. Revision 2 of this publication also reflects changes in technology and recent updates to NIST publications, including the Cybersecurity Framework (CSF) 2.0 and the NIST IR 8286 series. Another major update is that the information is presented in tabular format to enhance readability.

Relationship to the CSF 2.0 and Other NIST Publications

This publication uses the CSF 2.0 [1] and the CSF 2.0 Small Business (SMB) Quick Start Guide (QSG) as a foundation from which to address cybersecurity for a specific audience—non-employer firms. This publication goes into significantly more detail than the SMB QSG and brings in additional NIST publications as reference material to connect and demonstrate important concepts through graphics, tables, and appendices.

1. Introduction

This publication specifically addresses cybersecurity basics for non-employer firms with no paid employees other than the owners of the business, helping them to use the NIST Cybersecurity Framework 2.0 [1] to begin managing their cybersecurity risks. The actions included within this publication are ones that small businesses can take on their own with limited technical knowledge or with minimal budget to implement. To make this information applicable to a broader audience, cybersecurity risk management considerations are included for businesses as they grow and hire employees, if they decide to do so. It is recognized that many solopreneurs may never hire employees and will, instead, rely upon third-party service providers to extend their services and capabilities.

Foundational Goals of Cybersecurity

Three foundational goals of cybersecurity are to protect the confidentiality, integrity, and availability of data and technologies.[1]

- **Confidentiality** - protecting data from **unauthorized access and disclosure**.

  For example, what would be the impact if customer data, such as usernames, passwords, or credit card information were stolen? This is an example of a cybersecurity risk resulting in a potential reputational, legal, and financial risk to the company.

- **Integrity** - protecting data from **unauthorized modification**.

  For example, what if research data or a product design was changed without your knowledge?

- **Availability** - **preventing disruption in how you access** data or technologies.

  For example, what if you couldn't log in to your bank account or access customer data? Or, what if the business website is down and customers cannot make purchases or access information?

What is Cybersecurity Risk Management?

As businesses of all sizes increase their reliance on technology and digitally created, stored, processed, and communicated information, and as criminals simultaneously increase their capabilities to attack these technologies and information, cybersecurity risk has become a fundamental risk that even the smallest businesses must address alongside other business risks (e.g., environmental, legal, financial, reputational). Cybersecurity risk management (CSRM) is the management of uncertainty on or within information and technology. Table 1 provides a brief overview of the five stages of CSRM, as outlined in NIST IR 8286, *Integrating Cybersecurity and Enterprise Risk Management* [4].

[1] It is recognized that in some industries "safety" is also added to the "confidentiality, integrity, and availability" triad—especially those in industrial control systems or operational technology environments.

Table 1: Cybersecurity Risk Management Lifecycle

Cybersecurity Risk Management Lifecycle (Adapted from [4])	
Step 1: Understanding context —the environment in which the organization operates.	1. **External context** involves the expectations of outside stakeholders that affect and are affected by the organization, such as customers, regulators, legislators, and business partners. These stakeholders have objectives, perceptions, and expectations about how risk will be communicated, managed, and monitored. 2. **Internal context** relates to many of the factors within the organization and relevant cybersecurity considerations across the enterprise. This includes any internal factors that influence CSRM, such as the organization and enterprise's objectives, governance, culture, risk appetite, risk tolerances, policies, and practices.
Step 2: Identify the risks that could enhance or impede business objectives, including the risks involved in failing to pursue opportunities.	**Cybersecurity risk identification is comprised of four inputs:** 1. Identification of the organization's critical assets. 2. Determination of potential threats that might jeopardize the confidentiality, integrity, and availability of those assets. 3. Consideration of the vulnerabilities of those assets. 4. Evaluation of the potential consequences of risk scenarios.
Step 3: Analyze the risks to estimate the likelihood that the risk event will occur and the potential impact.	For a small business, you might start with a qualitative analysis, which is based on the assignment of a descriptor, such as low, medium, or high. See Appendix C for more information on this.
Step 4: Prioritize risks in order of importance to prioritize risk response.	A cybersecurity risk can have adverse effects, ranging from negligible to severe, on achieving organizational objectives. Since organizations have limited resources, it is helpful to sort the risks in order of importance to prioritize risk response. See Appendix C for more information on this.
Step 5: Plan and execute to determine the appropriate response to each risk	There are four types of actions available for responding to cybersecurity risks: accept, transfer, mitigate, and avoid. 1. **Accept** cybersecurity risk within risk tolerance levels. 2. **Transfer**--For cybersecurity risks that fall outside of tolerance levels, reduce them to an acceptable level by sharing a portion of the consequences with another party (e.g., cybersecurity insurance). While some of the financial consequences may be transferrable, there are often consequences that cannot be transferred, like loss of customer trust. 3. **Mitigate**--Apply actions that reduce the threats, vulnerabilities, and impacts of a given risk to an acceptable level. 4. **Avoid**--Apply responses to ensure that the risk does not occur. Avoiding a risk may be the best option if there is not a cost-effective method for reducing the cybersecurity risk to an acceptable level.

Understanding Your Business Assets

As a non-employer firm, you might not have a tremendous amount of assets. Still, it is important to document those assets you do rely upon, evaluate how important they are to your business, identify potential risks to those assets, and take steps to protect them. At this stage you might consider using the simple table below to get started:

Table 2: Getting Started with an Asset Inventory

Document the assets you rely upon to run your business	Document possible risks to that asset	What would the impact be if that asset were unable to operate? (e.g., significant, moderate, negligible)	Steps taken to limit exposure to compromise.

Figure 1 shows a graphic depicting sample architecture for a fictional small, non-employer firm.

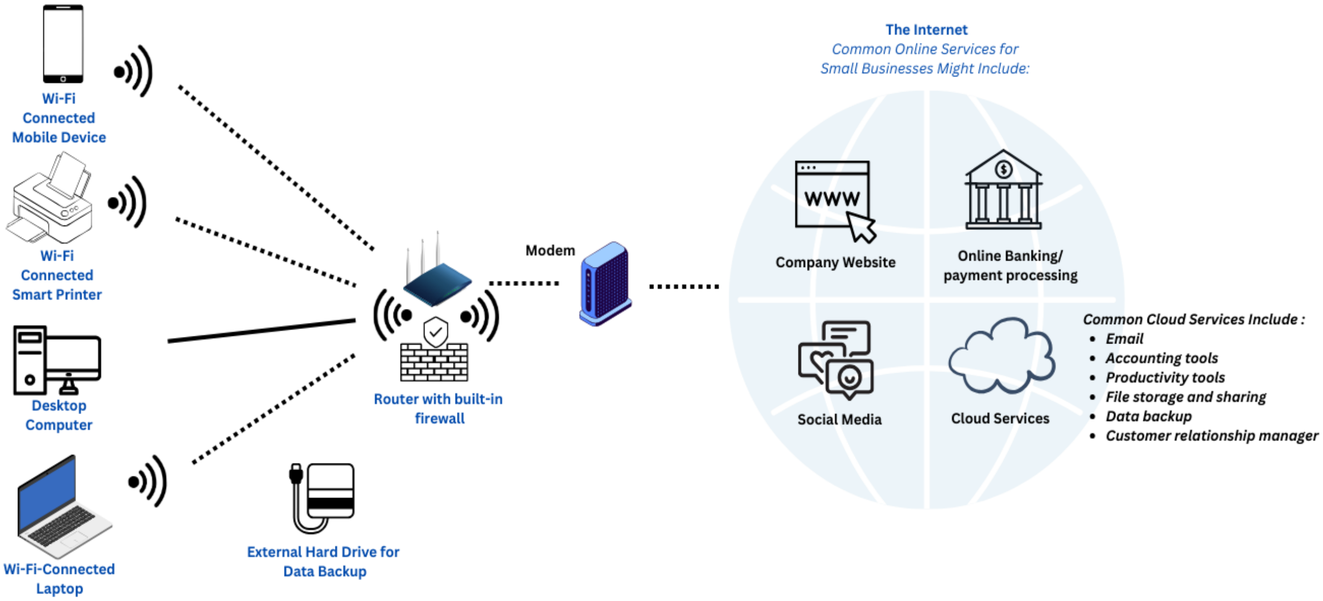

Wi-Fi Connected Mobile Device
Wi-Fi Connected Smart Printer
Desktop Computer
Wi-Fi-Connected Laptop
External Hard Drive for Data Backup
Router with built-in firewall
Modem
The Internet
Common Online Services for Small Businesses Might Include:
WWW
Company Website
Online Banking/ payment processing
Social Media
Cloud Services
Common Cloud Services Include :
Email
Accounting tools
Productivity tools
File storage and sharing
Data backup
Customer relationship manager

Figure 1: Notional Architecture for Non-Employer Firm

The firm might have a stationary desktop computer in the office (whether that is at home or somewhere else), a Wi-Fi enabled printer, and a laptop and phone that serve as mobile devices for connecting to the internet to access the business' necessary data and systems—whether that's the company website, online banking, social media, or a host of cloud services that the business depends upon to extend their capabilities and operate more efficiently. The firm might also have an external hard drive that is used as one of their methods of backing up data. Though the number of assets in this diagram is limited, and will vary depending upon the type of business, there are still quite a few opportunities for cyber criminals to compromise the business—such as taking advantage of the default manufacturer's password in the router; sending a phishing link to the business owner via text, social media, or email; or taking over the company website by leveraging a vulnerability in outdated software.

All businesses have cybersecurity risk. Unfortunately, in one respect, small businesses often have more to lose than larger organizations simply because a risk event—whether criminal, natural disaster, or business resource loss—can be extremely costly. With fewer resources, the impact of one of these risks is felt more substantially within a small business. The overall impact of a cybersecurity incident could include one or more of the following:

- Inability to operate;
- Regulatory fines and penalties or legal fees;
- Decreased productivity;
- Loss of business-critical information;
- Adverse impact to reputation, including loss of trust from customers, employees, or business partners;
- Damage to your credit and inability to get loans from banks;
- Loss of business income.

When striving for business success and growth, strong cybersecurity enables that goal. A few ways that implementing fundamental cybersecurity practices can enhance the competitiveness of your business include:

- Protecting intellectual property;
- Enhancing the business' ability to comply with legal, regulatory, and contractual requirements;
- Positioning the business as a reliable participant in a larger supply chain;
- Gaining the confidence of customers, business partners, and employees—demonstrated by taking their cybersecurity seriously;
- Making the business more resilient in the face of cybersecurity risks so that if an incident or breach occurs, the impact is minimized.

Often, the biggest concern for most small businesses is the efficient use, or prioritization, of limited resources. However, it is possible—and necessary—to implement a program that balances security with the needs and capabilities of the business.

Based on your needs and capabilities, these are some best practices that have been shown to significantly reduce cybersecurity risks, such as:

- ✓ Enabling phishing-resistant **multi-factor authentication** on all accounts that offer it,
- ✓ Using **strong and unique passphrases.** A passphrase is similar to a password but is generally longer—in the form of a sequence of words or other text. Length has been found to be a primary factor in characterizing password strength [11].
- ✓ Learning how to **recognize phishing attempts**,
- ✓ Having **regular data backups**, and
- ✓ Maintaining **updated software** on all devices and applications.

These will be expanded upon later in this document.

Cybersecurity for your business requires continuous improvement. Many business leaders often strive for continuous improvement in the business—growing revenues, gaining more market share, expanding the product offering, operating more efficiently, etc. Cybersecurity risk management also requires continuous improvement. As the business grows or changes, as technologies and threats change, and as legal and regulatory requirements change, leaders must revisit and update the business' cybersecurity risk management strategy to account for any important changes that might impact their approach.

Recognize when you need help. No one is an expert in every business and technical area. Many small businesses outsource some of their tax, intellectual property, or contractual work to accountants or lawyers. These are complex topics that require specialized training. Cybersecurity is the same. It is common for businesses of all sizes to outsource their cybersecurity needs to companies that specialize in these services. Here are a few tips which can help you find a provider that is right for your business:

- **Ask for recommendations**. You can ask others in your industry who they use and trust. You can also ask your local Manufacturing Extension Partnership, APEX Accelerator, or local SBA resource partner for recommendations.
- **Do your research**. Have a clear list of outcomes you want to achieve—this document can help you get started with that. Read online reviews to see what the experience of other customers has been. Check for complaints with the Better Business Bureau. Request quotes from multiple vendors. Understand what experience they have working with your industry and their ability to help you meet your specific legal, regulatory, or contractual requirements.
- **Recognize you are still responsible**. You can outsource some of your cybersecurity needs, but you do not transfer your liability for protecting your information. You are ultimately responsible for protecting your systems and data.

Cybersecurity Risk Management in Relation to Privacy Risk Management

Privacy is beyond the scope of this publication. However, it is important to note that though they are distinct disciplines, cybersecurity and privacy can have overlapping and complementary objectives. As documented in the NIST Privacy Framework, “While managing cybersecurity risk contributes to managing privacy risk, it is not sufficient, as privacy risks can also arise by means unrelated to cybersecurity incidents” [5]. For example, a business might use a customer’s personal information in ways that violates an individual’s privacy without that data having been breached or compromised through a security incident. This type of issue can occur under a variety of scenarios, such as when data is stored for extended periods, beyond the need for which the information was initially collected [6]. To better understand privacy risk management, view Getting Started with the NIST Privacy Framework: A Guide for Small and Medium-Sized Businesses.

2. The NIST Cybersecurity Framework

The Cybersecurity Framework (CSF) is a flexible, technology-neutral framework that helps organizations—regardless of size, sector, or maturity— better understand, assess, prioritize, and communicate their cybersecurity efforts. It is important to note that the Framework is not a one-size-fits-all approach to managing cybersecurity risks—because every organization has unique needs, resources, and missions that must be taken into account individually.

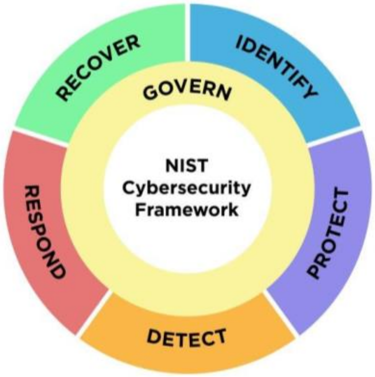


Figure 2: The Cybersecurity Framework Functions

The CSF is comprised of three primary components:

1. **The CSF Core** provides high-level cybersecurity outcomes organized into Functions (see Table 3 below), Categories, and Subcategories, that can help any organization manage its cybersecurity risks. These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. The six CSF Functions, when considered together, provide a comprehensive and strategic view of managing cybersecurity risk.
2. **CSF Organizational Profiles** are a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.
3. **CSF Tiers** can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices.

Table 3: The Six Functions of the CSF

Govern	The Govern Function helps you establish and monitor your business' cybersecurity risk management strategy, expectations, and policy.
Identify	The Identify Function helps you determine the current cybersecurity risk to your business.
Protect	The Protect Function supports your ability to use safeguards to prevent or reduce cybersecurity risks.
Detect	The Detect Function provides outcomes that help you find and analyze possible cybersecurity attacks and compromises.
Respond	The Respond Function supports your ability to take action regarding a detected cybersecurity incident.
Recover	The Recover Function involves activities to help you restore assets and operations that were impacted by a cybersecurity incident.

Learn more about the Cybersecurity Framework:
nist.gov/cyberframework

Organization of this Publication

This document is organized according to the six Functions of the CSF 2.0. The activities listed for each Function within this guide offer a good starting point for creating a basic cybersecurity risk management strategy for a small non-employer business.

The tables on the following pages are organized into the following column headings:

Table 4: Column Headings with Descriptions

Actions to Consider	Rationale	Getting Started	Considerations as Your Business Grows
This column explains **what** action a business might consider taking to reduce their cybersecurity risks. The activities are not all encompassing. They are considerations to help establish a cybersecurity risk management strategy and create a strong foundation upon which to build. Citations included in this column (e.g., “GV.RR-01”) are mappings back to the full CSF 2.0 Core Function (e.g., GV), Category (e.g., RR), and Subcategory (e.g., 01).	This column explains **why** the action is an important step to take to reduce or manage cybersecurity risks.	This column provides tips for **how** a business can get started with the specified action.	This column highlights options for **what’s next** as a business adds employees or grows in other ways.

Appendices are included to provide sample worksheets, planning documents, and additional background text. Though this publication is primarily based off the CSF 2.0, it also leverages insights and resources from various NIST publications and frameworks to inform the content.

Govern Function (GV)

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

Actions to Consider	Rationale	Getting Started	Considerations as Your Business Grows
Document and track your legal, regulatory, and contractual cybersecurity requirements. GV.OC-03	Your business may be required to meet specific legal or regulatory requirements[2] depending on which sector it operates in. Also, if you've signed contracts with other businesses, you may have contractual requirements for cybersecurity or privacy risk management.	Create a spreadsheet to document and track your requirements. You can use the table on the next page as a starting point to help you document and track compliance with them.	As your business grows, you'll likely enter into more contractual agreements. Regulations might also change as time goes on. There are regulatory compliance tools on the market that can help you. You might also want to select a third-party vendor who has experience working within your regulatory environment to assist you.
Determine whether cybersecurity insurance is appropriate for your business. GV.RM-04	Cyber liability insurance may help you recover from a security incident. In some cases, cyber liability insurance companies may also provide cybersecurity expertise and help you identify actions you need to take to protect your business.	Speak to others in your industry and to your trusted insurance agent to understand if cybersecurity insurance is appropriate for your business. You should also understand if business contracts or agreements require cybersecurity insurance.	As your business grows, be sure to account for any increased complexity (e.g., expanded mission, new business processes, or assets). Ensure that your insurance provider is updated about any changes to your business that could affect risk or that may require policy updates.
Assess cybersecurity risks posed by suppliers and other third parties before entering into formal relationships. GV.SC-06	Many businesses enter into contracts with third parties to support their critical business processes and achieve their mission. These engagements with other companies can introduce additional cybersecurity risk.	Contracts, including purchase orders, can be a primary vehicle a small business has for addressing risk with third parties. Consider whether you need legal support to help you. There are some university-based legal clinics that can help write and review contracts at no cost.	As your business grows, the number of suppliers and third parties will likely grow. Ensure that you have a process in place to manage these contractual arrangements and the risks these relationships may introduce to your business.

[2] Examples of sources of regulatory requirements include Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS).

Additional Govern Function Resources

- CSF 2.0 Cybersecurity Supply Chain Risk Management Quick Start Guide
- Empowering SMBs: A Resource Guide for Developing a Resilient Supply Chain Risk Management Plan

Get Started. Document and track your legal, regulatory, and contractual cybersecurity requirements. Completing a table like the one below will help you to begin documenting and tracking your cybersecurity requirements. You will likely need to modify the table to meet your own needs, but this provides a starting point.

Table 5: Documenting Legal, Regulatory, and Contractual Cybersecurity Requirements

Requirement Body	Individual Requirement to Meet	Status	Deadline	Documentation	Evaluation	Action(s) Needed	Next Review Date
(E.g., HIPAA, PCI DSS)	*(E.g., conducting risk assessments to identify potential vulnerabilities*	*(E.g., in compliance, in progress, out-of-compliance*			*(e.g., self-attest, audit)*		

Identify Function (ID)

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

Actions to Consider	Rationale	Getting Started	Considerations as Your Business Grows
Understand what assets your business relies upon by **creating, categorizing, and maintaining an inventory** of hardware, software, data, and services (including cloud services). ID.AM-01/02/04/05/06/07	By inventorying and categorizing data and systems, you will be better prepared to make informed decisions on what protective measures to take to reduce your cybersecurity risks.	(See Appendix C)	As your business matures, it will become more difficult to inventory and manage all your assets. Using an automated asset inventory solution or a managed security service provider can help you efficiently and thoroughly inventory and categorize all your business assets.
Document cybersecurity risks to the business assets. ID.RA-03/05/06	Risk is a function of threats, vulnerabilities, the likelihood of an event, and the potential impact such an event would have to the business. Learn more below:	(See Appendix C)	Growing businesses can find success in documenting, categorizing and prioritizing cybersecurity risks using a risk register [4].

Elements of Risk (Adapted from [4])

A ***threat*** is any circumstance or event with the potential to adversely impact organizational operations. These threats might come in the form of personnel or natural events; they can be accidents, or intentional. An example of a threat is an employee accidentally submitting login credentials through a phishing scam. Another example might be an employee accidentally downloading ransomware by clicking on what appeared to be a legitimate link, rendering critical business assets inaccessible

A ***vulnerability*** is a condition that enables a threat event to occur. Any time or situation where information is not being adequately protected represents a vulnerability. A common vulnerability is outdated or unpatched software. Vulnerabilities found in software applications are one of the most common avenues of attack for criminals.

Some threats affect businesses and industries differently. For example, an online retailer may be more concerned about website defacement than a business with little or no web presence. ***Likelihood*** is the chance that a threat will affect your business and helps determine what types of protections to put in place.

Actions to Consider	Rationale	Getting Started	Considerations as Your Business Grows
Securely sanitize and destroy data and data storage devices when they're no longer needed. ID.AM-08	Not doing so means you could be handing over sensitive information, like passwords or intellectual property, to those who should not have access to it.	Many operating systems allow you to electronically wipe the hard drive. Additionally, many devices have built-in remote wipe capabilities in case the device is lost or stolen. Using a shredder is also an effective method for destroying data.	A growing business might consider using enterprise-grade tools or specialist third parties for device wiping or data disposal.
Create a cybersecurity incident response plan ID.IM-04	Before a cybersecurity incident occurs, you want to be ready with a basic response plan.	Begin by documenting key contacts and contractually or regulatorily mandated cybersecurity incident response requirements. See Appendix D.	If you hire others to take on various risk management roles, document their cybersecurity incident response roles and responsibilities. Practice the incident response plan with tabletop exercises.

Additional Identify Function Resources

- Guide to Conducting Risk Assessments
- Take Stock. Know What Sensitive Information You Have
- Evaluating Your Operational Resilience and Cybersecurity Practices

Resources for Threat Intelligence

There are many publicly available sources of system security alerts and advisories, including:

- The Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Bureau of Investigation (FBI)
- Infragard
- Software vendors, subscription services, and industry Information Sharing and Analysis Centers (ISACs) also often provide security alerts and advisories.

Protect Function (PR)

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

Actions to Consider	Rationale	Getting Started	Considerations as Your Business Grows
Limit access to sensitive assets. Restrict sensitive device and information access to only those who need it to do their jobs. PR.AA-05	The principle of least privilege is foundational to cybersecurity. By granting the minimum privileges necessary to perform a task, you are reducing your threat surface. This applies to not only business owners and employees, but also to third parties.	Use a standard user account on your devices, instead of administrator accounts, to perform routine work functions. If you share a device with family members, ensure they have their own unique accounts and cannot access sensitive business data. Limit account access, such as to cloud services, to only those who require access for a specified time, to accomplish specific tasks.	As you hire employees or engage third-party vendors, establish policies and procedures to: Grant access only to systems and information that they need to do their job. Remove access to sensitive assets when an employee transitions into another role where access is no longer needed. Remove access to all the business' information, systems, and devices when an employee leaves the company or when you end a third-party relationship.
Change default manufacturer passwords. PR.AA-01	Many devices, such as your Wi-Fi router, come with default administrative passwords. Default passwords are easily found or known by criminals and can be used to access the device.	Review the security settings on all devices, new and old, to ensure you have created unique, strong passwords. Document within an asset inventory which devices have had their manufacturer passwords updated. See Appendix E.	Establish and regularly review policies and procedures for onboarding and managing devices to ensure default passwords are changed and managed securely.
Enable multi-factor authentication (MFA) on all accounts that offer it and consider using password managers to generate and protect strong, unique passwords. PR.AA-03	Passwords alone are not effective for protecting your data from most attackers, as passwords have become too easy for threat actors to exploit at scale and with limited effort.	Review all account settings to enable MFA, especially phishing-resistant MFA (learn more about MFA below). With so many passwords to keep track of, a common and relatively inexpensive approach is using a password manager to create and maintain unique, strong passwords.	If you grant system access to third parties or to employees, require MFA to be enabled and used on all accounts that offer it. To streamline access, consider implementing Single Sign On (SSO) technologies. These technologies allow users to access multiple applications, tools, and systems with just one set of credentials.

Multi-Factor Authentication (MFA)

MFA is an important security enhancement that requires a user to verify their identity by providing **more than just a username and password**. If a password is compromised, MFA creates a second barrier that makes it much harder for the threat actor to access your systems and data. It requires a user to provide a combination of two or more of the following:

- ✓ something you know (like a password or PIN)
- ✓ something you have (like a smart card or security key)
- ✓ something you are (like your fingerprint or face)

Enabling MFA on all accounts that offer it is essential for reducing the cybersecurity risks to your business. **This is one of the most important steps a small business can take at no cost to protect their business.** Some forms of MFA are more secure than others, as some forms of MFA can be susceptible to phishing threats. Common **phishing-resistant authenticators** widely available today can take the form of something called a passkey, which works on specific websites and allows you to authenticate in combination with another factor, such as a fingerprint or PIN--without requiring a username and password.

Table 6: MFA Starter Checklist

Account (on-premises software and cloud)	Phishing-Resistant MFA Enabled? (Yes/No)
Banking Account(s)	
Accounting and Tax Account(s)	
Merchant Account(s)	
Productivity Service(s)	
Email	
Password Manager(s)	
Website(s)	
Customer Relationship Manager	
Social Media Sites	

Actions to Consider	Rationale	Getting Started	Considerations as Your Business Grows
Regularly update and patch software and operating systems. PR.PS-02	Un-patched or outdated software can introduce vulnerabilities that attackers can exploit.	Install updates and patches for all assets in your inventory. Enabling automatic updates will help you manage updates. Make a habit of routinely checking for available updates at least monthly.	Growing businesses can utilize an automated patch management system to help identify, prioritize, acquire, install, and verify the installation of patches, updates, and upgrades to systems and devices.
Regularly back up your data. Establish measures to protect and test your backups. PR.DS-11	Backups enable restoration of data in case a computer breaks, or a malicious program infects your system. Without data backups, you may have to re-create your business information manually.	Configure devices and systems to regularly back up information. Consider having multiple data backups, with at least one on media that is not connected to the computer (such as an external hard drive). Periodic testing can give you confidence that the backups will restore your data when needed.	As you add more devices and systems, consider using centralized solutions to conduct and manage backups and identify who within the organization is responsible for backing up data.
Know how to recognize common attacks and perform basic cyber hygiene tasks. PR.AT-01/02	Awareness training equips business owners with the knowledge and skills to perform general tasks with cybersecurity risks in mind.	Take security awareness training at least once a year. Many organizations regularly provide free or low-cost cybersecurity training, such as Small Business Development Centers. There are also many free online cybersecurity courses. One of the most common attacks is phishing. Learn more about phishing below.	As you hire employees, a critical piece of minimizing cybersecurity risks will be creating a culture of cybersecurity. Part of that is regular, effective employee training on information security policies, cyber hygiene practices, and how to recognize and report suspicious activity.

Phishing

Phishing is a type of scam that uses convincing emails or other messages (e.g., text messages, social media messages) to trick us into opening harmful links or downloading malicious software. This is often how ransomware is delivered to organizations and is one of the biggest threats to your business. These messages are often disguised as a trusted source, such as your bank, credit card company, a customer, or trusted advisor.

How to spot a phish

- A request to download an attachment or click on a link—treat all attachments and links with caution.
- A sense of urgency. They want you to act now. Stop and take a moment to think about the request. Verify the request by using known contact information or information from a public company website, not from the message itself. Or if you get an urgent message from someone you know, contact them directly to verify the message.
- A suspicious-looking source email address.
- A request for you to divulge or change sensitive information, like bank account information or Social Security number.

Training on how to identify and report phishing coupled with enabling phishing-resistant multi-factor authentication (MFA), such as biometrics and passkeys, are steps that will significantly reduce the chances of your business falling victim to this common threat.

Learn more about phishing:

- NIST Small Business Cybersecurity Corner: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing.
- NIST Human-Centered Cybersecurity Phishing Resources: https://csrc.nist.gov/projects/human-centered-cybersecurity/research-areas/phishing
- Recognize and Report Phishing (Cybersecurity and Infrastructure Security Agency) https://www.cisa.gov/secure-our-world/recognize-and-report-phishing

Additional Protect Function Resources

- Data Backup Recommendations
- Cybersecurity Training Resources
- Multi-Factor Authentication

Detect Function (DE)

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

Actions to Consider	Rationale	Getting Started	Considerations as Your Business Grows
Continuously monitor assets to find indicators of attacks or compromises. DE.CM	If you can identify common indicators of a cybersecurity incident, you are better equipped to quickly take action to minimize disruption to your business.	Installing and maintaining security software (e.g., antivirus) is a good first step in detecting incidents. These often have the capability of keeping a log to identify suspicious activity. Ensure this functionality is enabled (check the operating instructions for how to do this). Logs can be a helpful tool during an incident investigation.	You can enhance and automate your detection capabilities. Depending on your operating systems and resources, you might consider: • using intrusion detection and prevention systems. • configuring technology to audit and alert on certain events. • engaging a service provider to monitor computers and networks. • using an all-in-one endpoint security product.
Assess your physical environment for signs of tampering or suspicious activity. DE.CM-02	Cybersecurity is not confined to the internet. There is a physical component as well. Imagine if someone broke into your home, office, or vehicle and stole a device that has sensitive information on it.	Assess your physical office space and implement tactics that will reduce the chances of unauthorized individuals having physical access to your systems and data (e.g., locks on filing cabinets, securely storing devices, and enabling automatic screen locks). Understand the unique physical threats that might come with each location where you work (e.g., home, café).	You might consider advanced physical access control mechanisms, such as biometric authentication or access cards to better enable you to control and monitor access. You might also consider having surveillance equipment installed or a security guard screening guests prior to entering your office or facility.

Related Resources:

- Ransomware Protection and Response
- Detecting a Potential Intrusion

Respond Function (RS)

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

Actions to Consider	**Rationale**	**Getting Started**	**Considerations as Your Business Grows**
Execute your incident response plan in coordination with relevant third parties. RS.MA-01	Implementing your prepared cybersecurity incident response plan will help to minimize the impact of the incident.	When you detect an incident, document as much information as you can about it to share with your incident responder. This would include: a description of the incident, when you first detected it, and what actions you've taken, if any. Reach out to those experts you have documented in your cybersecurity incident response plan to seek assistance. See Appendix D, Respond and Recover Worksheet.	When you grow to the point where you have multiple internal functional areas (e.g., human resources, cybersecurity, communications), include individuals from across your business to execute your response plan alongside any external stakeholders. Conduct tabletop exercises to test your incident response plan.
Communicate with internal and external stakeholders on your response activities as required by laws, regulations, or policies. RS.CO	There are situations where you will have a legal, regulatory, or contractual responsibility to communicate certain details of a confirmed incident with relevant stakeholders.	Refer to your incident response plan to identify what your responsibilities are for communicating a confirmed cybersecurity incident with business stakeholders as required by laws, regulations, contracts, or policies. See Appendix D, Respond and Recover Worksheet.	Effective response communications can become more complicated as your business grows. Organizations with more resources will often consult crisis communications professionals to help craft appropriate internal and external messaging.

Sample Response Contact Table* (from Appendix D, Respond and Recover Worksheet)

Table 7: Sample Response Contact Table

Contact Type	Contact Name	Phone	Email
Business Champion:			
Technical Contact:			
State Police:			
Legal Contact:			
Bank Contact:			
Insurance Contact:			
CISA Regional Advisor *Find your CISA Regional Office*			
Regional FBI Contact *Find your FBI Field Office*			

**Those listed in this table are examples. You might have other individuals or organizations in your own list.*

Additional Response Function Resources:

- NIST Incident Response Preparation Resources Page
- Cyber Readiness Institute Incident Response Plan Template
- Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile
- FBI’s Internet Crime Complaint Center
- Best Practices for Victim Response and Reporting of Cyber Incidents

Recover Function (RC)

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

Actions to Consider	Rationale	Getting Started	Considerations as Your Business Grows
Execute the recovery portion of your incident response plan. RC.RP.01	Recovery activities will help you get your business back operational.	Verify the integrity of any backups and other assets before you put them back into use so that you minimize chances of re-infecting your system.	When you have multiple functional areas (e.g., human resources, cybersecurity, communications), include individuals from across the business to execute the recovery plan alongside any external stakeholders.
Coordinate restoration activities with internal and external parties. RC.CO	Regular communication with internal and external parties is critical for an effective recovery. In some instances, you might have legal responsibilities to communicate with the public or designated stakeholders.	It is encouraged that you seek input from legal counsel prior to distributing communications about an incident.	Like with response, recovery communications can become more complicated as your business grows. Consider seeking assistance from a crisis communications resource.
Document lessons learned from the incident. RC.RP-06	Documenting lessons learned can provide business owners with insights on how to minimize the chances of a cybersecurity incident happening in the future.	Prepare 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.	As recovery concludes, impacts will be felt across the business. Clear and respectful conversations should continue across all parts of the organization after the event to capture insights and lessons learned.

Related Resources:

- Guide for Cybersecurity Event Recovery
- Creating an IT Disaster Recovery Plan
- Backup and Recover Resources

3. Conclusion

The six CSF Functions from above (Govern, Identify, Protect, Detect, Respond, and Recover), when considered together, provide a comprehensive and strategic view of managing cybersecurity risk. The activities listed for each Function within this guide offer a good starting point for creating a basic cybersecurity risk management strategy for a small non-employer business. The activities are not all encompassing. They are considerations to help establish a cybersecurity risk management strategy and create a strong foundation upon which to build. As the business grows and adds employees and additional complexity, the cybersecurity risk management strategy will need to be revised to reflect the increased risks.

To access more NIST small business resources, visit the NIST Small Business Cybersecurity Corner: https://www.nist.gov/itl/smallbusinesscyber

References

[1] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[2] U.S. Small Business Administration (2019), A Look at Nonemployer Businesses. (U.S. Small Business Administration Office of Advocacy. https://advocacy.sba.gov/wp-content/uploads/2019/06/A-Look-at-Nonemployer-Businesses.pdf

[3] U.S. Small Business Administration (2024), Frequently Asked Questions About Small Business, July 2024 (U.S. Small Business Administration Office of Advocacy. https://advocacy.sba.gov/wp-content/uploads/2024/12/Frequently-Asked-Questions-About-Small-Business_2024-508.pdf

[4] Stine KM, Quinn SD, Witte GA, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[5] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 10. https://doi.org/10.6028/NIST.CSWP.10

[6] Fisher W, Craft RE, Ekstrom M, Sexton J, Sweetnam J (2024) Data Confidentiality: Identifying and Protecting Assets Against Data Breaches. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 1800-28. https://doi.org/10.6028/NIST.SP.1800-28

[7] Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

[8] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[9] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) NIST FIPS 199. https://doi.org/10.6028/NIST.FIPS.199

[10] Nelson A, Rekhi S, Souppaya M, Scarfone KA (2025) Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-61, Rev. 3. https://doi.org/10.6028/NIST.SP.800-61r3

[11] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63-3, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[12] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v2r1

[13] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) NIST FIPS 200. https://doi.org/10.6028/NIST.FIPS.200

[14] International Organization for Standardization (2022) *ISO 31073:2022– Risk management — Vocabulary* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/79637.html

[15] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[16] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[17] Ross RS, Pillitteri VY (2024) Assessing Security Requirements for Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171Ar3. https://doi.org/10.6028/NIST.SP.800-171Ar3

[18] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[19] Stine KM, Quinn SD, Witte GA, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8286. https://doi.org/10.6028/NIST.IR.8286

Appendix A. Glossary

application
A software program hosted by an information system.

assets
An item of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation). The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Such concerns include but are not limited to business or mission concerns. [12]

authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. [13]

availability
Ensuring timely and reliable access to and use of information.

backup
A copy of files and programs made to facilitate recovery, if necessary.

confidentiality
Protecting information from unauthorized access and disclosure.

cyber resiliency
The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment. [12]

cybersecurity risk
An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. [14] [15]

integrity
Protecting information from unauthorized modification.

least privilege
The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. [16]

risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [17][18]

threat
Any circumstance or event with the potential to adversely impact organizational operations (a negative risk). [19]

vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [19]

vulnerability assessment

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [19]

Appendix B. Acronyms

ERM
Enterprise Risk Management

FBI
Federal Bureau of Investigation

CSF
Cybersecurity Framework

CISA
Cybersecurity and Infrastructure Security Agency

HIPAA
Health Insurance Portability and Accountability Act

IAM
Identity and Access Management

ISAC
Information Sharing and Analysis Center

IT
Information Technology

MEP
Manufacturing Extension Partnership

MFA
Multi-Factor Authentication

NIST
National Institute of Standards and Technology

NIST IR
National Institute of Standards and Technology Interagency or Internal Report

PCI DSS
Payment Card Industry Data Security Standard

SBA
U.S. Small Business Administration

SBDC
Small Business Development Center

SMB
Small to Medium-Sized Business

SSO
Single Sign-On

Appendix C. Calculating, Documenting, Categorizing, and Prioritizing Cybersecurity Assets and Risks Worksheet

Beginning with Appendix C, the following appendices are designed to be customizable to your business needs. It is suggested that you replicate, customize, and edit these worksheets in an electronic spreadsheet format so that it will be easily scalable and updatable for your business needs.

Understanding and Managing Your Risks

Risk is a function of threats, vulnerabilities, the likelihood of an event, and the potential impact such an event would have to the business. Most of us make risk-based decisions every day. While driving to work, we assess threats and vulnerabilities such as weather and traffic conditions, the skill of other drivers on the road, and the safety features and reliability of the vehicle we drive.

Elements of Risk

A ***threat*** is "any circumstance or event with the potential to adversely impact organizational operations" [4]. These threats might come in the form of personnel or natural events; they can be accidents, or intentional. An example of a threat is an employee accidentally submitting login credentials through a phishing scam. Another example might be an employee accidentally downloading ransomware by clicking on what appeared to be a legitimate link, rendering critical business assets inaccessible.

A ***vulnerability*** is "a condition that enables a threat event to occur" [4]—a weakness that could be used to harm the business. Any situation where information is not being adequately protected represents a vulnerability. A common vulnerability is outdated or unpatched software. Vulnerabilities found in software applications are one of the most common avenues of attack for hackers. You may consider conducting a penetration test against your business. This test simulates an attack in order to identify weaknesses. The test should include physical, social engineering, and cyber-based attacks. Other tests may also be useful. Work with a cybersecurity professional to identify what is appropriate for your situation.

Some threats affect businesses and industries differently. For example, an online retailer may be more concerned about website defacement than a business with little or no web presence. ***Likelihood*** is the chance that a threat will affect your business and helps determine what types of protections to put in place.

Similarly, most businesses have different types of information. If a marketing pamphlet is leaked online, it will probably not harm the business nearly as much as if, for example, sensitive customer information or proprietary business data was leaked. The ***impact*** an event could have depends on the information affected, the business, and the industry.

List the types of information, processes, important people, and technology your business relies upon.

1. In column 1 of the worksheet, list the assets (e.g., information, people, processes, or technology) that are most important to your business.

2. Go through each asset type you identified and ask:
    a. What would be the impact to my business if this asset was made public?
    b. What would be the impact to my business if this asset was damaged or inaccurate?
    c. What would be the impact to my business if I or my customers couldn't access this asset?
3. Pick an asset value scale that works for you (e.g., low, medium, high, or a numerical range like 1-5).

You can use this sample planning table to help you begin to identify your most important assets, processes, and systems, and then categorize each based on the impact to the business if the confidentiality, availability, or integrity were to become compromised. To learn more, NIST Special Publication 800-60, Vol.1, Rev. 1 [8] provides basic guidelines for mapping types of information and information systems to security categories.

Table 8: Sample Asset Categorization-Appendix

Asset	**Confidentiality Impact (low, moderate, high)**	**Integrity Impact (low, moderate, high)**	**Availability Impact (low, moderate, high)**	**Notes**
Intellectual Property	*High*	*High*	*High*	*Critical to business*
E-Commerce Site	*Low*	*Mod*	*High*	*Availability critical*
Customer Relationship Manager	*Med*	*High*	*High*	*Availability critical*
Social Media Account	*Low*	*Mod*	*Low*	*Integrity important*

FIPS Publication 199 [9] defines three levels of potential impact on organizations or individuals should there be a breach of security:

- **Low Impact:** limited adverse effect on organizational operations, assets, or individuals.
- **Moderate Impact:** Serious adverse effect on organizational operations, assets, or individuals.
- **High Impact:** Severe or catastrophic adverse effect on organizational operations, assets or individuals.

Below are examples of possible threat events and potential risks to the identified assets.

Table 9: Sample Potential Events and Risks to Assets-Appendix

Asset	Possible Threat Actor/Event	Possible Risks
Intellectual Property	• Ransomware • Malicious insider or competitor	• Critical information becomes unavailable • Critical information is stolen or modified
E-Commerce Site	• Denial of service attack on site • Compromise of site	• E-commerce site is unavailable, impacting sales and revenue generation • E-commerce site is compromised, impacting integrity of business
Customer Relationship Manager	• Malicious insider or competitor • Denial of service attack on site	• Customer information stolen or modified • Customer relationship information becomes unavailable, impacting business
Social Media Account	• Malicious attacker or competitor	• Social media account is compromised, resulting in loss of integrity and possible damage to business reputation

Appendix D. Respond and Recover Worksheet[3]

Incident response is a critical part of cybersecurity risk management and should be integrated across organizational operations. The six CSF 2.0 Functions play vital roles in incident response:

- Govern, Identify, and Protect help organizations prevent some incidents, prepare to handle incidents that do occur, reduce the impact of those incidents, and improve incident response and cybersecurity risk management practices based on lessons learned from those incidents.
- Detect, Respond, and Recover help organizations discover, manage, prioritize, contain, eradicate, and recover from cybersecurity incidents, as well as perform incident reporting, notification, and other incident-related communications.

An adverse cybersecurity incident is "…an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies" [7]. Examples include an attacker:

- Using phishing emails to compromise user accounts
- Identifying a vulnerability in network management appliances and exploiting the vulnerability to gain unauthorized access to network communications
- Deploying ransomware to prevent the use of computer systems

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' communications/reporting responsibilities as required by laws, regulations, contracts, or policies.

Table 10: Sample Contact Table-Appendix

Contact Type	Contact Name	Phone	Email
Business Champion:			
Technical Contact:			
State Police:			
Legal Contact:			

[3] Worksheet content adapted from NIST SP 800-61, R3, Incident Response Recommendations and Considerations for Cyber Risk Management: A CSF 2.0 Community Profile [10]

Contact Type	Contact Name	Phone	Email
Bank Contact:			
Insurance Contact:			
CISA Regional Advisor *Find your CISA Regional Office*			
Regional FBI Contact *Find your FBI Field Office*			

Coordinate response activities with internal and external stakeholders as required by laws, regulations, or policies.

Incident response reporting and communication activities tend to fall into four categories:

- **Incident coordination** involves communicating current and planned incident response activities for a particular incident among the internal and external parties who have incident response roles and responsibilities.
- **Incident notification** involves formally informing affected customers, employees, partners, regulators, or others about a data breach or other incident.
- **Public communication** involves communicating to the public about the status of a particular incident, such as responding to media inquiries.
- **Incident information sharing** involves sharing cybersecurity threat information with others, usually voluntarily, based on activity observed within the organization's technology assets.

Table 11: Sample Reporting Requirements Table-Appendix

Document the Regulation, Contact, or Law	Document the Reporting Requirement	Document the Reporting Timeframe	Reporting Requirement Contact Information

Appendix E. Authentication Worksheet

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 that your own list will be longer than this:

Table 12: Sample MFA Table-Appendix

Account	MFA Enabled (Yes/No)	Phishing-Resistant MFA Enabled? (Yes/No)
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)		
Customer Relationship Manager Account		
Social Media Sites		

Sample Default Manufacturer Passwords Table

Table 13: Sample Default Manufacturer Passwords Table-Appendix

Account	Default Password Changed (Yes/No)
Wi-Fi Router	
Smart Device 1	
Smart Device 2	
Security Camera System	
Industrial Control System	
Network-Connected Printer	

Appendix F. Change Log

Changes from Revision 1 to Revision 2 include:

- Updated title.
- Specified the audience to focus on single owner and operator business with no employees.
- Narrowed the scope from information security to cybersecurity.
- New, updated introductory content
- Simplified the language and concepts.
- Moved the primary content into tables for ease of reading.
- Updated content to more closely align with the CSF 2.0
- Eliminated Section 4, “Working Safely and Securely” and moved content into appropriate CSF Function discussions.
- Combined Section 1, “Background” and Section 2, “Understanding and Managing Your Risks.
- Added new appendices