SECURITY GUIDE · 01

Implementing the NIST Cybersecurity Framework

A practical, plain-English guide for business owners

How to understand, organize, and steadily improve your cybersecurity using a framework trusted by organizations of every size — without needing to be a technical expert.

Wagner Cybersecurity LLC
www.wagnercybersecurity.com · joe@wagnercybersecurity.com

Contents

Why this guide exists

Cybersecurity is no longer an IT problem you can delegate and forget. It is a business risk that sits squarely with ownership and leadership — right alongside cash flow, hiring, and reputation.

If your business stores customer information, takes payments, relies on email, or simply needs its computers to work on Monday morning, then a security incident is a business interruption waiting to happen. The good news: you do not need to become a technical expert to manage this risk well. You need a framework, a plan, and a habit of steady improvement.

This guide explains the NIST Cybersecurity Framework (CSF) in plain language and shows you how to put it to work in a small or mid-sized organization. It is written for owners and decision-makers, not just system administrators. Where your IT team or provider needs to take the technical lead, we say so.

> **What you will walk away with**
>
> A clear mental model of how the framework is organized.
>
> A practical, seven-step rollout you can start this quarter.
>
> A short list of high-impact actions that reduce risk quickly.

What the NIST CSF actually is

The NIST Cybersecurity Framework is a voluntary, widely adopted framework published by the U.S. National Institute of Standards and Technology. It was created to help organizations of any size understand, manage, and reduce cybersecurity risk using a common language.

A few things it is — and is not — worth being clear about up front:

- **It is outcome-based, not a product list.** The framework describes results to aim for ("access to systems is controlled"), not specific brands or tools to buy.
- **It is flexible.** A 10-person firm and a 1,000-person company can both use it. You scale the depth to your size and risk.
- **It is a common language.** It gives your leadership, your IT provider, your insurer, and your auditors a shared vocabulary for talking about risk.

The current edition, CSF 2.0, was released in 2024. The biggest change from earlier versions is that it now applies explicitly to organizations of all sizes and sectors, and it elevates governance — leadership's role in setting and overseeing the strategy — to a core part of the model.

How the framework is organized

The framework has three building blocks. Understanding them takes about five minutes and makes everything afterward easier.

Functions, Categories, and Subcategories

At the top sit six Functions — the highest-level grouping of cybersecurity outcomes. Each Function breaks down into Categories (groups of related outcomes), which break down further into Subcategories (the specific, measurable outcomes). You can think of it as a folder structure: Functions are the top folders, and the detail lives in the files inside.

Tiers

Tiers describe how rigorous and consistent your approach is, from ad-hoc and reactive (Tier 1) to proactive and continuously improving (Tier 4). Tiers are not grades to maximize — they are a way to set an appropriate ambition level for your risk.

Profiles

A Profile is a snapshot of which outcomes you are achieving. Your Current Profile is where you are today; your Target Profile is where you want to be. The gap between them is your roadmap.

> **In one sentence**
> Use the Functions to organize the work, the Tiers to decide how rigorous to be, and Profiles to track the journey from where you are to where you want to be.

The six core Functions

Everything in the framework rolls up into these six Functions. The first, Govern, surrounds and informs the other five.

Function	What it means	Why it matters to you
Govern	Set the strategy, assign responsibility, and oversee cyber risk like any other business risk.	Without ownership and a budget, security stalls. This is leadership's job.
Identify	Know what you have: devices, data, software, vendors, and the risks to them.	You cannot protect what you do not know exists. An inventory is the foundation.
Protect	Put safeguards in place to limit or contain the impact of an incident.	This is the day-to-day hygiene: access control, training, backups, updates.
Detect	Find suspicious activity and potential incidents quickly.	The faster you notice trouble, the smaller the damage and the lower the cost.
Respond	Take action once an incident is detected to contain and manage it.	A practiced response turns a crisis into a managed event.
Recover	Restore systems and operations, and learn from what happened.	Getting back to business quickly — and improving — protects revenue and trust.

A simple way to remember the flow: Govern sets direction; Identify and Protect are what you do before anything goes wrong; Detect, Respond, and Recover are what you do when something does.

Implementation Tiers

Tiers help you decide how formal and consistent your program should be. Most small businesses start at Tier 1 and aim for a solid Tier 2 or Tier 3 over time.

Tier	Name	What it looks like
1	Partial	Security is handled ad-hoc and reactively. Few documented processes; risk is rarely discussed at the leadership level.
2	Risk Informed	Leadership is aware of risk and approves practices, but they are not yet consistent across the whole organization.
3	Repeatable	Practices are formally documented, applied consistently, and updated as risks change.
4	Adaptive	The organization actively improves based on lessons learned and adapts to new threats in near real time.

> **Don’t over-invest in a tier you don’t need**
>
> Reaching Tier 4 across the board is expensive and unnecessary for most small businesses. Pick a target that matches your risk and your customers’ expectations — then get consistent at it.

Profiles: where you are vs. where you want to be

Profiles turn the framework into something actionable. The process is straightforward:

1. Build a Current Profile by honestly assessing which outcomes you are achieving today.
2. Build a Target Profile that reflects where you need to be, based on your business, your obligations, and your risk tolerance.
3. Compare the two. The differences are your prioritized to-do list.

You do not need expensive software to do this. A spreadsheet with the outcomes you care about, a column for “today,” and a column for “target” is enough to get started and have a productive conversation with your IT provider.

A practical rollout in seven steps

Here is a sequence that works well for a small or mid-sized organization adopting the framework for the first time.

4. **Assign ownership and get leadership behind it.** Name one accountable person and put cyber risk on the leadership agenda. This is the Govern function in action.
5. **Inventory your assets and data.** List your devices, key software, where sensitive data lives, and which vendors can access it.
6. **Assess your current state.** Walk through the six Functions and note what you already do well and where the gaps are.
7. **Prioritize gaps by risk.** Focus on the issues most likely to happen and most damaging if they do — not the ones that are simply easiest to fix.
8. **Build a roadmap.** Turn priorities into a short, dated plan with owners. Quarterly milestones work well.
9. **Implement quick wins first.** Bank early progress to build momentum and reduce real risk fast (see the next section).
10. **Measure, review, and repeat.** Revisit the plan on a set cadence. Security is a cycle, not a one-time project.

Quick wins you can start this quarter

These high-impact actions map to the Protect, Identify, and Recover functions and reduce risk quickly without major spend.

- Turn on multi-factor authentication (MFA) everywhere it is offered, starting with email and remote access.
- Confirm you have backups of critical data — and test that you can actually restore from them.
- Keep systems and software updated; enable automatic updates where practical.
- Give every employee a short, plain-language security awareness briefing, especially on phishing.
- Create a simple asset inventory and remove access for people who have left.
- Write down who to call during an incident — internal owner, IT provider, insurer — and keep it somewhere reachable.

> **The 80/20 of small-business security**
>
> MFA, tested backups, timely updates, and trained staff prevent the large majority of common incidents. If you do nothing else this quarter, do these.

Common mistakes to avoid

- **Treating it as a one-time project.** Threats change; your program has to keep pace.

- **Buying tools before having a strategy.** Software does not fix unclear ownership or bad processes.
- **Skipping governance.** Without leadership sponsorship and a budget, good intentions fade.
- **Chasing perfection.** Steady, prioritized progress beats an exhaustive plan that never ships.
- **Forgetting your vendors.** A supplier's breach can become your breach. Know who has access to what.

Where to go from here

Adopting the framework does not have to be daunting. Start small: assign an owner, inventory what you have, and knock out the quick wins. From there, the seven-step rollout gives you a repeatable rhythm of assess, prioritize, improve.

If you would like a hand running an assessment, building your roadmap, or closing specific gaps, we are happy to help — at whatever level of involvement suits you.

> **Talk to us**
>
> **Wagner Cybersecurity LLC**
>
> joe@wagnercybersecurity.com · www.wagnercybersecurity.com

Glossary

CSF — Cybersecurity Framework — the NIST framework described in this guide.

Function — One of the six top-level groupings of cybersecurity outcomes: Govern, Identify, Protect, Detect, Respond, Recover.

Profile — A snapshot of which outcomes you are achieving (Current) or aiming for (Target).

Tier — A rating of how rigorous and consistent your security approach is, from Partial (1) to Adaptive (4).

MFA — Multi-factor authentication — requiring a second proof of identity (such as a phone prompt) in addition to a password.

Phishing — Fraudulent messages designed to trick people into revealing credentials or installing malware.