expel

GETTING STARTED

NIST Cybersecurity Framework 2.0

Contents

About this doc

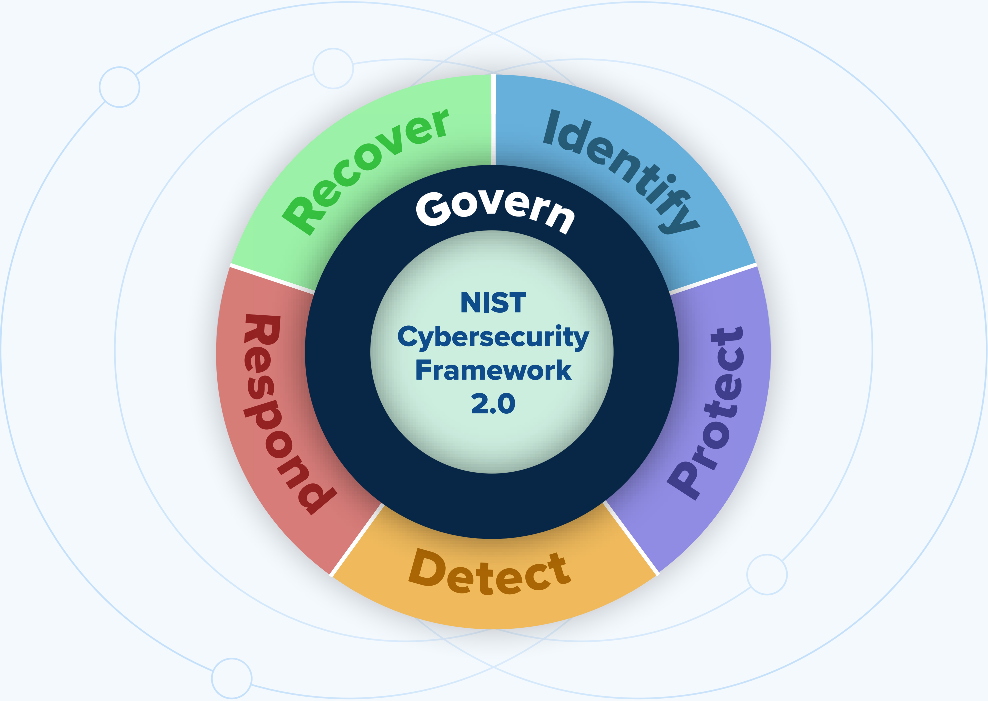
Since the National Institute of Standards and Technology (NIST) first published its Cybersecurity Framework (CSF) in 2014, it's become the most popular resource for security leaders to assess their organizations' cybersecurity postures and maturity. NIST has updated the CSF a few times since its inception, and the release of version 2.0 is the most comprehensive update of this important tool.

We've created this guide to provide a quick tour of the framework, an easy-to-use tool for rating your organization, and an explanation of how Expel can help you meet your goals and improve your ratings—now and in the future.

Introduction to the NIST CSF

To the uninitiated, the NIST CSF can be intimidating. It covers a lot of security controls, extensively delving into various categories and subcategories. If you're at a loss for how to approach or implement it—or not sure where to begin—you're not alone.

Despite its complexity, lots of organizations continue to rely on the CSF framework. A recent research study by the SANS Institute found that almost three-quarters (74%) of companies that use a framework use the NIST CSF—and for good reason. It's proven itself to be a useful tool to help organizations understand where they are and where they're going as they grow their broader cyber risk management programs. The trick is knowing where to start.



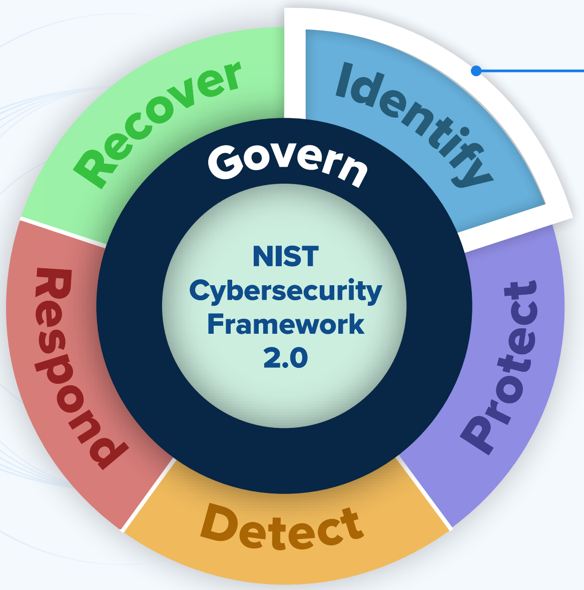
A quick tour of the framework

Let’s start with a short overview

The central component of the CSF is the Core, which is meant to capture the breadth of cybersecurity. To make it more easily digestible, the Core, or the “nucleus” of the framework, is broken down into different functional areas, categories, and subcategories. The functional areas are: Govern, Identify, Protect, Detect, Respond, and Recover—with each function comprised of categories and subcategories.

For example, the Identify functional area’s categories include: Asset Management, Risk Assessment, and Improvement. Each category also contains subcategories. The Asset Management category includes subcategories like, “Inventories of hardware managed by the organization are maintained,” and “Inventories of software, services, and systems managed by the organization are maintained,” to name a couple.

The Core is intended to resonate with operators focused on operationalizing risk management, and is designed to be forward-looking to still be relevant to any future changes in tech and the security landscape.



CATEGORIES

Asset Management

Risk Assessment

Improvement

SUBCATEGORIES

- Inventories of hardware managed by the organization are maintained
- Inventories of software, services, and systems managed by the organization are maintained

Find your baseline (in two hours or less)

Now that you understand the Core, here's what you can do with it

The CSF Core can be helpful in describing where you are and where you want to be with respect to cyber risk management. The next step is establishing a baseline for the current state of your organization—starting with the subcategories.

Within the subcategories, you'll see lots of very specific actions and processes that you may already be doing. It's important to note that they aren't exhaustive, but describe detailed outcomes that support each category. For example, under **Adverse Event Analysis (AE)** in the **Detect (DE)** functional area, there are six subcategories:

- **DE.AE-02**: Potentially adverse events are analyzed to better understand associated activities
- **DE.AE-03**: Information is correlated from multiple sources
- **DE.AE-04**: The estimated impact and scope of adverse events are understood
- **DE.AE-06**: Information on adverse events is provided to authorized staff and tools
- **DE.AE-07**: Cyber threat intelligence and other contextual information are integrated into the analysis
- **DE.AE-08**: Incidents are declared when adverse events meet the defined incident criteria

(You may notice that DE.AE-01 and DE.AE-05 are missing from the list. NIST CSF 1.1 included them, but NIST incorporated them into other subcategories with CSF 2.0.)

Perhaps you already do these things—but how well are you doing them? NIST CSF 2.0 includes Framework Tiers as a sort of scoring system to help determine where you are now, and where you want to be. Tiers characterize the typical rigor of cybersecurity risk governance and management practices throughout an organization, including context for how you view and any processes in place for managing those risks.

NIST provides four tiers (1 through 4), but we added a Tier 0. Here's a summary of what the tier scale looks like and the practices that define each:

- **Tier 0: We're not doing this at all**
- **Tier 1: Partial**
  - The organization manages this area in an ad hoc manner
  - There's limited awareness of this in the organization
  - The organization is generally unaware of the risks of the products and services it uses
- **Tier 2: Risk Informed**
  - These practices are approved by management but may not be established policy
  - The organization is aware of the risks but isn't managing them regularly
  - The organization is aware of the risks associated with its supplier and the products and services it uses, but isn't consistent in responding to those risks
- **Tier 3: Repeatable**
  - The organization's risk management practices are formally approved and expressed as policy
  - There's an organization-wide approach to managing cybersecurity risks
  - The organization consistently and accurately monitors the cybersecurity risks of assets
- **Tier 4: Adaptive**
  - There is an organization-wide approach to managing cybersecurity risks that uses risk-informed policies, processes, and procedures to address potential cybersecurity events
  - The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators
  - The organization uses real-time or near real-time information to understand and consistently act upon cybersecurity risks associated with the products and services it provides and uses

You can get more comprehensive explanations of the Tiers from the NIST CSF. If you've used our guide for NIST CSF 1.1, you may notice that these Tiers replace the scoring system we provided before. NIST CSF 1.1 didn't provide users a way to score their organizations, so we created one. Now we're using NIST's Tiers for scoring.

By applying this scale to the 106 (!) subcategories, you end up with a good measure of where your organization stands. Just don't forget that there are 106 subcategories. So, in the interest of time, don't overthink or debate the finer points of each score.

On your first pass, try to stick with whole and half numbers. Resist the urge to use smaller increments than that. Quarter-points, tenths and hundredths places are too granular for what's meant to be a quick assessment of your current standing.

Now you might be wondering, "How and where do I keep track of all these numbers?" With this "getting started" guide, we include the NIST self-scoring spreadsheet. Each function has its own tab, which includes their associated categories and subcategories. Simply go line by line and put your current scores into the columns labeled "Score today."

At a leisurely pace of two subcategories per minute, you'll be done in an hour and even have time for a break.

Once you're finished with the self-assessment (built-in break included), go back to the top and do it again. But this time, instead of documenting where you are today, assess where you want to be in six months, 12 months, and your eventual goal state. Or if you don't want to have goals for six and 12 months, change those time periods to whatever fits your needs.

When building your goals, be aware that you probably don't need to strive for Tier 4 across every subcategory. Getting there takes a lot of effort and resources. Organizations that require world-class security controls generally know it and are prepared to dedicate significant budget to achieve it.

Charting your course ... literally

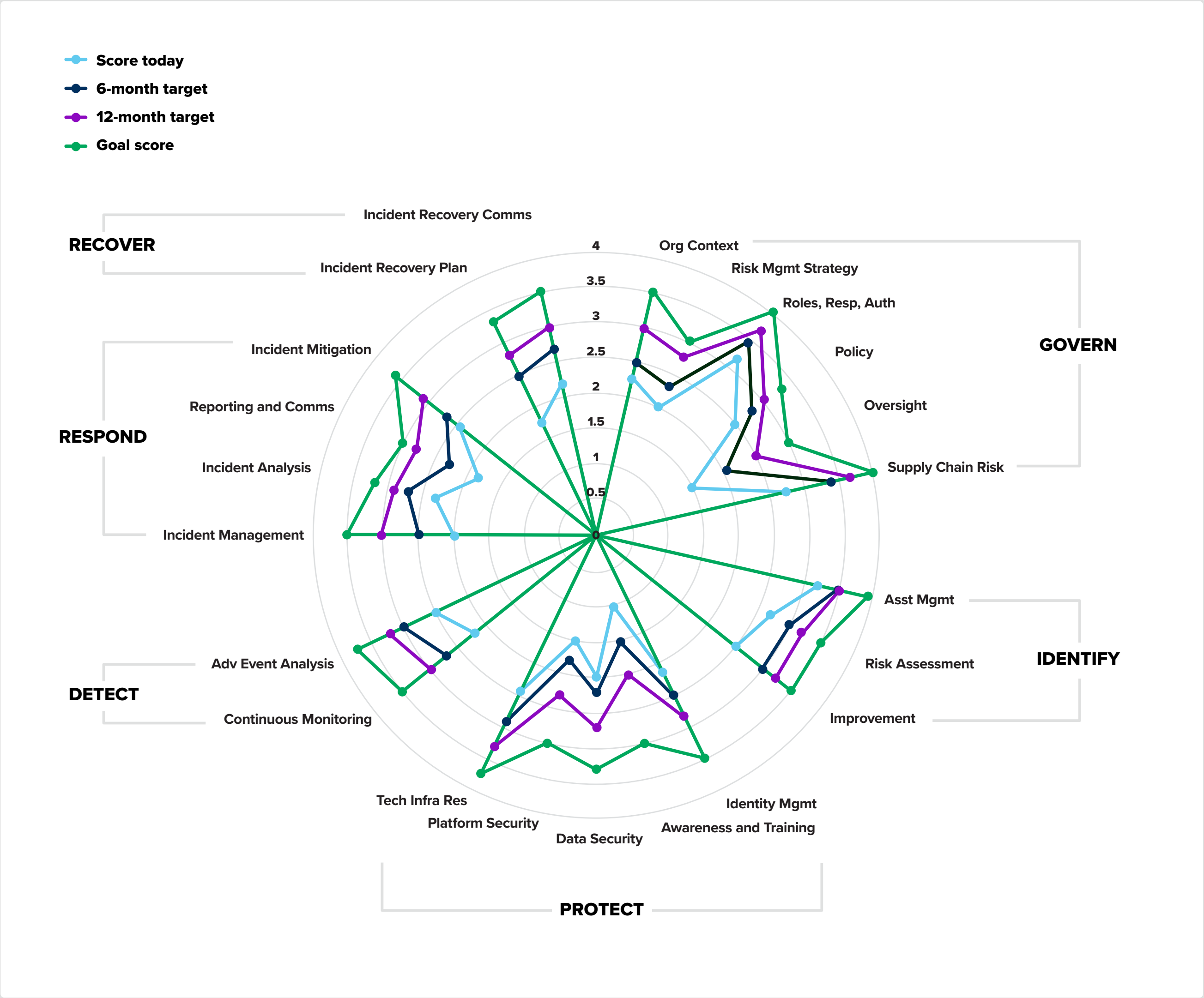
Now you might be wondering why you're inserting all this data. You'll see that each tab has a radar chart, and that chart automatically updates based on the scores you insert.

The spreadsheet rolls up all of your scores for each subcategory into an average for the category that you can use to visualize exactly where you stand and where you want to be. (See an example of the type of graph the spreadsheet creates below.)

These graphs do a good job of highlighting the areas where you're doing really well (in this example, Identify and Govern) and areas where you need to focus your efforts (Protect, Detect, Respond, and Recover). Every organization is different, so don't let the gaps worry you too much. Remember that the CSF is an attempt to cover everything in cyber risk management. So even in large, mature organizations there are going to be areas that haven't been a priority and large gaps between where you are and where you want to be.

Now it's time to prioritize and plan. Unfortunately, there's no easy-to-use spreadsheet to autogenerate that—it's for you to decide. You'll need to figure out what gaps you want to work on and how you're going to close them based on your business needs and the types of risks you're most concerned about. It's important to set expectations (with yourself and up the chain). Closing gaps isn't a short-term program. What usually emerges is a strategic plan with lots of little pieces that fall into place along the way.

NIST CSF 2.0 analysis: current state compared to future and goal states



Pro Tip

Re-evaluate yourself quarterly. It's a good way to check your progress, identify areas for improvement, and adjust your plan accordingly.

Using Expel to color in your CSF

Like we said, we've done this exercise at Expel. And since we also use Expel managed detection and response (MDR) to protect ourselves, we know from experience how Expel can positively impact CSF scores.

But to fully understand how, first you need to understand a bit of what we do. Expel is the industry-leading MDR provider, delivering rapid detection and response and helping companies build their cyber resilience. Our security operations platform, Expel Workbench™, breaks down silos across a variety of tech and attack surfaces to achieve measurable outcomes, improve overall security, and minimize business risk. Expel's technology-driven approach to MDR uses automation and AI, coupled with a close partnership and 24x7 access to our own expert SOC analysts, to bring our customers best-in-class managed services.

Expel’s first-year impact

For this example, let’s assume you’ve got a reasonable set of existing security controls: robust endpoint detection and response (EDR) capabilities, a next-gen firewall of some sort, and maybe even some cloud security solutions. But you don’t have a person on staff dedicated to looking at those systems. Instead, you’re hoping those systems are defending your network on their own and will sound a siren or blast a red light when something’s wrong. In that case, your CSF graph may look a lot like the one above. Now, let’s say you’re considering Expel. There are a number of ways Expel MDR can impact your scores. Let’s dive a bit deeper into a couple of the functions.

Detect

Since Expel is a 24x7 service that detects bad and anomalous activity on your network, it lifts all of the Detect scores across the board. Our detection and correlation capabilities, which our analysts and engineers are constantly refining, detect threats in your enterprise and present them to our analysts in a structured and consistent way. Think threats like business email compromise (BEC), adversary-in-the-middle (AiTM), and phishing attacks to start. So, it makes sense that outsourcing your security operations leads to better scores in the Detect function.

Respond

Expel also has a dramatic impact on each category in the Respond functional area, thanks to our remediation actions. When we detect a potentially bad activity, we kick off an investigation. Our analysts look at the alerts, gather related data, and if we find there’s something malicious going on, we declare it a security incident.

But we don’t stop there—we also provide remediation actions for each incident. These actions are concrete steps that you can take to address the threat, accompanied by analysis and other supporting information. This process adds consistency and technical completeness to your incident response, so you can quickly address the attack and get back to running your business.

Our remediation actions allow you to stand on the shoulders of our world-class platform and analysts, so you get a world-class response capability.

Recover

Expel impacts the Recover functional area a bit less than Detect and Respond. Recover is focused on longer-term incident response issues like corporate lessons-learned, updating plans, and reputation management. That said, Expel still impacts your Recover score since you're more informed about the incidents you've experienced and the remediation steps you've taken. The net result is that your Recover activities are better informed and more mature.

Really?

Really. Expel can help you rapidly close the gaps between where you are and where you want to be from a security risk management perspective.

We feel strongly about helping businesses of all sizes be more secure—not just big companies with huge security and risk programs. Expel is unique in this regard and can provide a nearly instantaneous lift for your security posture for relatively little expense and time.

Expel self-scoring tool for NIST CSF

Score yourself in less than two hours

Complete your own assessment with Expel's self-scoring tool for NIST CSF. It's a downloadable, interactive Excel worksheet based on what we built right into Expel Workbench. Now it's even easier to see where you are today—and where you can be in the future.

Get the tool

About Expel

Expel empowers companies of all shapes and sizes to disrupt their adversaries and help build their security resilience. Expel's leading managed detection and response (MDR) services protect organizations by reducing risk and strengthening their security postures, augmenting existing security programs, providing detections and automation that drive world-class results, and even securing across their clouds—while providing full transparency into everything we do. Powered by our security operations platform Expel Workbench™, our people, expertise, and technology help organizations focus on building trust—with their customers, partners, and employees. For more information, visit our **website**, check out our **blog**, or follow us on **LinkedIn**.