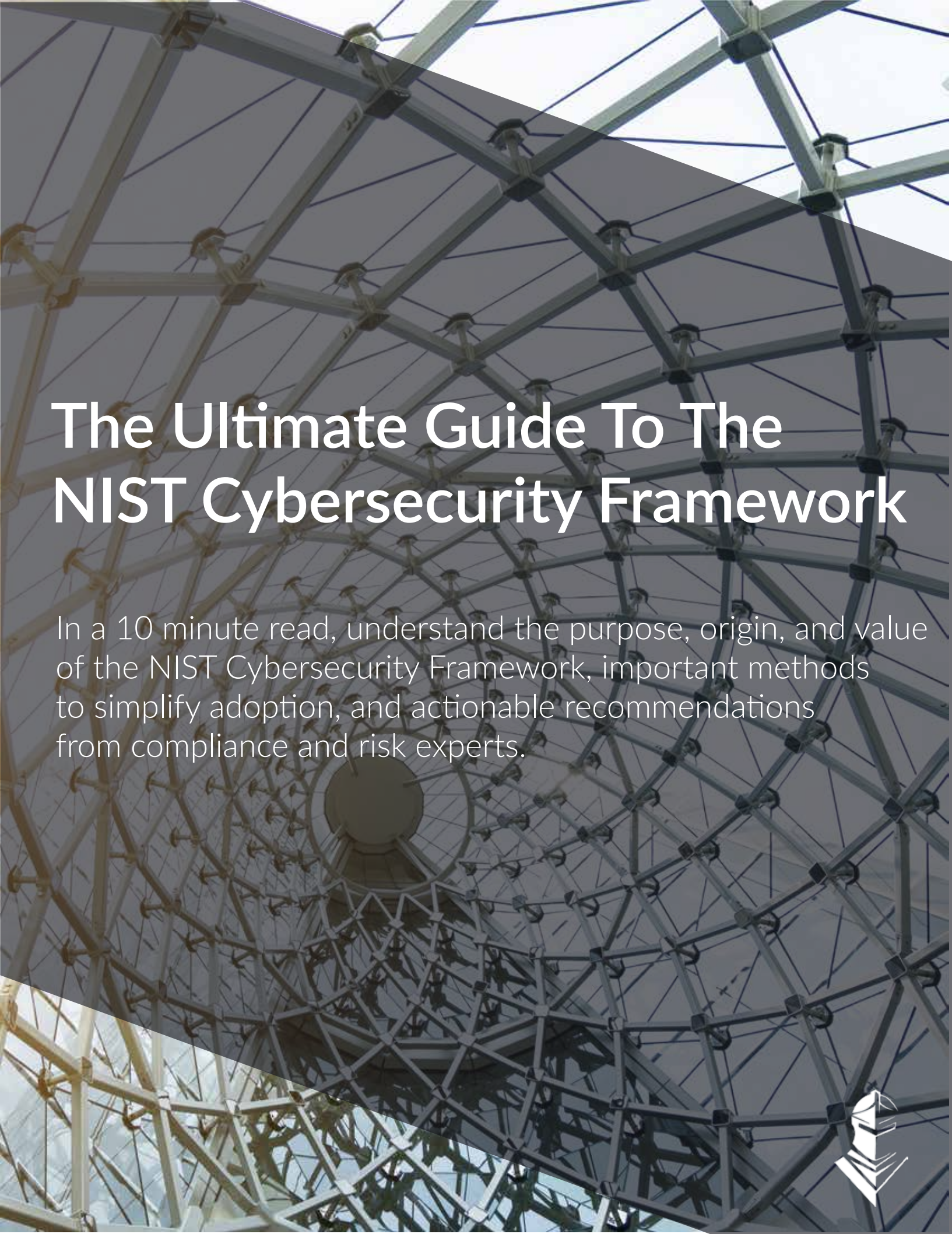

The Ultimate Guide To The NIST Cybersecurity Framework

In a 10 minute read, understand the purpose, origin, and value of the NIST Cybersecurity Framework, important methods to simplify adoption, and actionable recommendations from compliance and risk experts.

Table of Contents

Looking into the NIST Framework?

As the "gold-standard" of cybersecurity frameworks, the NIST Framework can add unparalleled depth and breadth to your cyber program. This guide will cover everything that you need to know to start and improve your NIST Framework-based program.

The Benefits of a Framework-Based Approach

The Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure is motivating action from not only federal agencies but U.S. businesses as well. Recent cyberattacks and breaches have resulted in heightened private sector awareness, which is driving companies to reevaluate how they can reduce enterprise risk.

Frameworks create a common language for cyber that unifies the conversation around enterprise risk and security.

Traditionally, financial and healthcare companies have been concerned with securing their clients' data. However, following recent attacks, organizations across every sector realize the need to propagate a robust risk-aware culture. Enterprises also understand that securing their organization means securing their supply chain - requiring vendors to adopt frameworks to continue their working relationship.

When CyberSaint's founder, George Wrenn, left his position as a global CSO to start CyberSaint, he set out to accomplish one goal: realizing that the frameworks' nature—by far the most comprehensive— designates that it is the most complex.

Our first conclusion: Cyber must be managed proactively and not reactively.

Our second conclusion: Companies have to be strategic when building and supplementing their programs.

As business leaders, there is a substantial responsibility to execute and keep our companies secure. The pressure is evident, and we see it build with each attack that damages revenue and reputation. A proactive information security professional must stay informed and advocate for increased resilience via a standards-based approach.

Why the NIST Cybersecurity Framework?

The National Institute of Standards and Technology's Cybersecurity Framework, formally titled The Framework for Improving Critical Infrastructure Cybersecurity, can overwhelm even experienced security professionals with its inherent complexity. Increasingly, though, it is recognized as a gold-standard. Its popularity and support is evident: 30 percent of U.S. businesses have adopted the framework as of 2015, and that number is snowballing.

With the new release of Version 1.1 of the Framework, it is even more robust, and still flexible with the ability to be adopted by organizations of any size voluntarily and has proven to be popular enough to have rapid adoption even in its first version.

The Under Secretary of Commerce for NIST, Walter Copan, noted **"From the very beginning, the Cybersecurity Framework has been a collaborative effort involving stakeholders from government, industry, and academia. The impact of their work is evident in the widespread adoption of the framework by organizations across the United States, as well as internationally."**

According to NIST "This second draft update aims to clarify, refine, and enhance the Cybersecurity Framework, amplifying its value and making it easier to use. This latest draft reflects comments received to date, including those from a public review process launched in January 2017 and a workshop in May 2017."

Additionally, the U.S. Secretary of Commerce Wilbur Ross noted that "The voluntary NIST Cybersecurity Framework should be every company's first line of defense. Adopting version 1.1 is a must do for all CEOs."

Small and mid-sized businesses need to be aware that not only large enterprises are targeted, and the Framework may be the most robust method to implement best-practices.

In fact, small businesses are attacked about four thousand times per day, making up 62% of all cyberattacks according to IBM.

The U.S. National Cybersecurity Alliance says that the cost of cleaning up after an attack for a small to mid-sized business can range from $690,000 to over $1 million. The NIST Interagency Report (NISTIR) 7621 entitled “Small Business Information Security: The Fundamentals” states “Because small businesses typically don’t have the resources to invest in information security the way larger businesses can, many cybercriminals view them as soft targets.”

The report also notes that some hackers are attacking not merely for profit, but out of revenge or thrill of causing havoc. To a small business, a robust cybersecurity program is often seen as a task too difficult because of the resources necessary.

Nonetheless, the benefits greatly exceed the cost, as adopting a proactive program and creating a business process will help gain and retain customers - especially in light of publicized cybersecurity attacks, as customers expect sensitive information to be protected.

The NIST Framework is genuinely applicable to any organization regardless of size as a jumping off point to establish their cybersecurity posture. It turns in traditional, more audit-based policies for a risk-based approach to cybersecurity management. It’s a guideline for businesses to update their risk management approach, as many U.S. organizations across sizes and industries already leverage some form of security framework.

Businesses of all sizes and industries are seeing the importance of building a robust cyber program and are seeking more proactive strategies. Its five core functions: Identify, Protect,

Detect, Respond and Recover, are a blueprint for mitigating cyber risk. Appropriately implemented, an organization will have the most rigorous set of tools and procedures in place.

In a sense, the Framework is a dynamic Deming cycle—continuous, logical and always learning.

Your Framework Profile

A Profile enables an organization to establish a roadmap for reducing cybersecurity risk that aligned well with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities.

Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs. Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities.

Your Current and Target Profile

The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the results needed to achieve desired cybersecurity risk management goals.

It's essential here to pull in goals from all business segments - both business and security. That way, you'll have a more well-rounded goal set that aligns with your business's vision for the future.

The Value of Profiles

Profiles support business/mission requirements within your organization to all constituents, and also aid in the communication of risk between organizations. If you have a difficult time translating your current and target risk and cyber strength to your partners (vendors and the like), creating these profiles will be monumental in boosting communication between all parties involved. The better the communication within and around your organization, the more progress you'll make in building a robust program or even creating a faster response plan.

If you're interested in baselining your organization against NIST Cybersecurity Framework best practices in hours, check out CyberStrong. You'll be able to see areas for improvement and gaps across all five NIST functions, and you'll have a plan of action on how to close those gaps within your organization.

The 5 NIST Framework Functions Explained

Identify

NIST defines the identify function as calling on the need to "develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities." In this function, as a cybersecurity stakeholder, you can work on laying a foundation in your organization for effective use of the Framework moving forward. The focus of identify is on the business and how it relates to cybersecurity risk, especially taking into account the resources at hand.

The outcome categories associated with this function:

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

The importance of the identify function is evident: it lays the groundwork for cybersecurity-related actions that your organization will take moving forward.

Identifying what exists, what risks are associated with those environments, and how that relates in context with your business goals are crucial to having success with the Framework.

Successful implementation of the identify function could result in multiple outcomes, for example:

- Defining all assets and environments
- Determining the current and target states of controls
- Making a plan to remediate those gaps
- Prioritizing how to approach mitigation in a business context
- Prioritizing the needs of all stakeholders and business
- leaders involved
- Defining how to communicate on cybersecurity issues
- with all related stakeholders

Organizations have to evolve in their cyber practices and implement the vital safeguards to contain and limit impacts of potential cyber incidents. All digital and physical assets must be accounted for, and roles must be defined with clear communication workflows around incidents and risk. The policies and procedures that you implement will provide the stability needed for your cybersecurity program as it works through all five functions and matures.

Protect

NIST says that the framework functions "aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities."

The protect function is vital because its purpose is to "develop and implement appropriate safeguards to ensure the delivery of critical infrastructure services. The protect function supports the ability to limit or contain the impact of a potential cybersecurity event."

Examples of outcome categories within this function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Protect covers these categories:

- Access Control: Validating identities and access to different systems, facilities, etc.
- Awareness and Training: Giving employees and others the ability to be part of your cyber plan with education and training.
- Data Security: Manage your data according to company standards to mitigate cybersecurity risks, and protect its Availability, Integrity, and Confidentiality proactively.
- Information Protection Processes & Procedures: Put in place the policies, processes, and procedures that you need to manage the protection of your assets.
- Maintenance: Continuously repair your Information System components and mitigate them.
- Protective Technology: Deploy the security solutions needed to protect them in line with company policies.

Examples of ways to attain these requirements are:

- Preventing a data breaches by using 2FA, MFA, and controlling access to all of your environments and data.
- Make sure your people are properly trained in how to handle your company's critical data and their various levels of access. Prevent accidents as much as possible.
- Make sure your data is encrypted, in motion, and protected in all ways possible.

Organizations must evolve as breaches are becoming all the more common. By focusing on the protect function, you can put in place the policies and procedures to lay a strong foundation for your cybersecurity program as it matures in all five functions.

Detect

The detect function requires that you develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

The detect function enables the timely discovery of cybersecurity events. Examples of outcome categories within this function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- Anomalies & Events: Your program will detect unusual activity as soon as possible, and the impact of events is understood by everyone on your team and beyond.
- Security & Continuous Monitoring: You're monitoring your information system and environments at specified intervals to identify cyber events in your organization.
- Detection Processes: Procedures and processes for detection are put in place and tested to ensure timely and broad awareness of cyber events.

The detect function is a critical step to a robust cyber program - the faster you can detect a cybersecurity event, the quicker you can mitigate the effects of it. Examples of how to accomplish steps towards a thorough detect function are as follows:

- Anomalies & Events: Prepare your team to have the knowledge to collect and analyze data from multiple points to detect an event.
- Security & Continuous Monitoring: Make your team able to monitor your assets 24/7 or consider involving an MSS to supplement.
- Detection Processes: Attempt to know about a breach as soon as possible and follow disclosure requirements as needed. Your program should be able to detect inappropriate access to your data as quickly as possible.

The detect function is one of the most important, as detecting a breach or event can be life or death for your business. There is no doubt that following these best practices and implementing these solutions will help you scale your program and mitigate cybersecurity risk.

Respond

NIST defines respond as "Develop and implement appropriate activities to take action regarding a detected cybersecurity incident."

The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

Here are the parts to the respond function and their importance:

- Response Planning: Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
- Analysis: Analysis is conducted to ensure adequate response and support recovery activities.
- Mitigation: Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
- Communications: Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
- Improvements: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

When breaches occur in companies, an incident response plan is critical to managing the immediate aftermath. Surprisingly, lots of organizations don't have an incident response plan, or just haven't tested the method that they have in place.

- Your Response Plan: Make sure that you're reporting breaches if they occur.
- Mitigate: Make sure you have a plan to mitigate any event that could occur, in-house and with third parties.
- Analyze: Go over your plan with experts inside and outside of your team.

Recover

According to NIST, the recover function is defined as the need to "develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event".

The recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcomes for this function include: Recovery Planning, Improvements, and Communications.

Recover includes these areas:

- Recovery Planning: Recovery procedures are tested, executed, and maintained so that your program can mitigate the effects of an event sooner rather than later.
- Improvement: Recovery planning and processes are improved when events happen and areas for improvement are identified and solutions put together.
- Communication: Coordinate internally and externally for greater organization, thorough preparation and execution.

The recover function is essential not only in the eyes of your business or organization in recovering from an attack but also in the eyes of your customers or market. Swift recovery handled with grace and tactfulness will allow you to end up in a much stronger position internally and externally than you would otherwise.

Prioritizing these focus areas within recover will ensure that your organization has a recovery plan that is up to date and matches your organization's goals and objectives.

Simplify NIST Framework Adoption in 5 Steps

There's little doubt that the NIST CSF is effective, but it's also a sophisticated framework that needs to be tailored to meet an organization's risk reduction goals. When Dimensional Research surveyed 300 IT and security professionals in the US, it found that 64% of respondents using the NIST CSF reported that they were not using all the recommended controls, just some of them. Also, 83% of organizations with plans to implement in the coming year reported an intention to adopt some, rather than all, the CSF controls. Selective adoption can yield results if done properly and can be a great starting point for organizations with limited resources. What's required is a way to reduce the complexity and make the NIST CSF just a little more digestible for your organization.

Below are key concepts that simplify and accelerate a NIST CSF adoption program.

Step 1 – Align a NIST-Based Program with Business Objectives

Map your objectives to the NIST control families. For example, if your organization requires "availability" of systems as the top priority, then starting with "Contingency Planning" (CP) controls is going to align your program with your business objectives better.

Step 2 – Focus on Foundational "Primary Controls" First

Start with a subset of the control families selected and limit your initial custom framework control list to the vital "Primary Controls." This will save "Control Enhancements" for later when your NIST CSF program is more mature. Control enhancements include details beyond the base control, such as frequency of testing, automation, and extensive documentation of the process surrounding the control. While important, these control enhancements only matter if the base control is already in place.

Step 3 – Get the Low-Hanging Fruit by Implementing NIST SP 800-171

Select your base framework controls using an existing framework profile or selection such as the NIST SP 800-171, which covers more than 80% of the full NIST CSF but requires approximately 20% of the effort, significantly reducing the number of controls that need to be adopted. Similar to the 80/20 principle, this approach can dramatically improve security with a fraction of the effort required to implement the full NIST CSF.

Step 4 – Balance the Five Framework Functions Evenly

Distribute your effort equally across all five phases of the NIST CSF. Creating a balanced program. If we follow the natural periods embodied with the NIST
CSF, we can break the various stages down into smaller pieces that are easier to digest and implement.

- Identify the risks to your systems, data, and other assets. You must be able to effectively prioritize your focus, fully understand governance, and carry out accurate risk assessments.
- Protect your critical infrastructure by limiting access to assets, training employees, securing and validating data integrity, implementing protective procedures and systems, and scheduling regular maintenance.
- Detect cybersecurity events that could be attacks. This means flagging anomalies, monitoring traffic and modeling regular noise so you can accurately identify anything suspicious.
- Respond when an event is detected. It would be best if you had a clear response plan with a communication protocol and a fixed timeline. Responses should be analyzed,

mitigation efforts tested, and all lessons learned used to make structural process improvements.

- Recover your vital services and capabilities after an attack as quickly as possible, so the impact to your organization is reduced. Solid recovery plans should be bolstered by a continually evolving approach informed by events and strong communication links with relevant internal and external parties.
- If you're stronger in one phase, then focus your efforts on one of your weaker aspects. Do this until your program becomes balanced across the five framework phases.

Step 5 – Leverage the Entire Organization

Make NIST CSF adoption a team sport. Engage business units and other resources across your organization. Many of the framework's controls can be assigned to business functions such as HR, finance, or IT. The security team doesn't have to own every control.

CyberSaint Security's CyberStrong Platform Streamlines NIST CSF Adoption and Compliance Management.

Learn more: www.cybersaint.io