What is the NIST Cybersecurity Framework?

Imagine building your network's cyber defenses from scratch without having any experience or guidance on how to do it. Sure, you might still be able to put a system in place.

Whether it can stand up against sophisticated cyber-attacks, however, is another story.

That's the value of having a framework. It guides you with the best practices and provides you with a standard to reach for, putting you on the right track.

An effective cybersecurity framework (CSF) will provide useful guidelines on how to plan, implement, and optimize cybersecurity programs, as well as set goals for you to aim for. A program like that can improve an organization's threat detection, risk mitigation, and incident response capabilities.

There are a lot of security frameworks for you to choose from, but one of the most popular is the one created by the National Institute of Standards and Technology (NIST). The framework has been downloaded over 1.5 million times across 185 different countries, and there's a good reason for that.

Intelligent Technical Solutions (ITS) is a cybersecurity-focused IT support company servicing the Chicago, Detroit, Las Vegas, Los Angeles, Phoenix, and San Francisco areas. Equipped with years of experience, our team is dedicated to helping businesses like yours bolster their cyber defenses by sharing our insights. In this article, we'll demystify the NIST CSF by addressing the following:

- What is NIST CSF?
- 5 Core Functions of NIST CSF
- How to Get Started with NIST CSF
- Why is the NIST CSF Important?

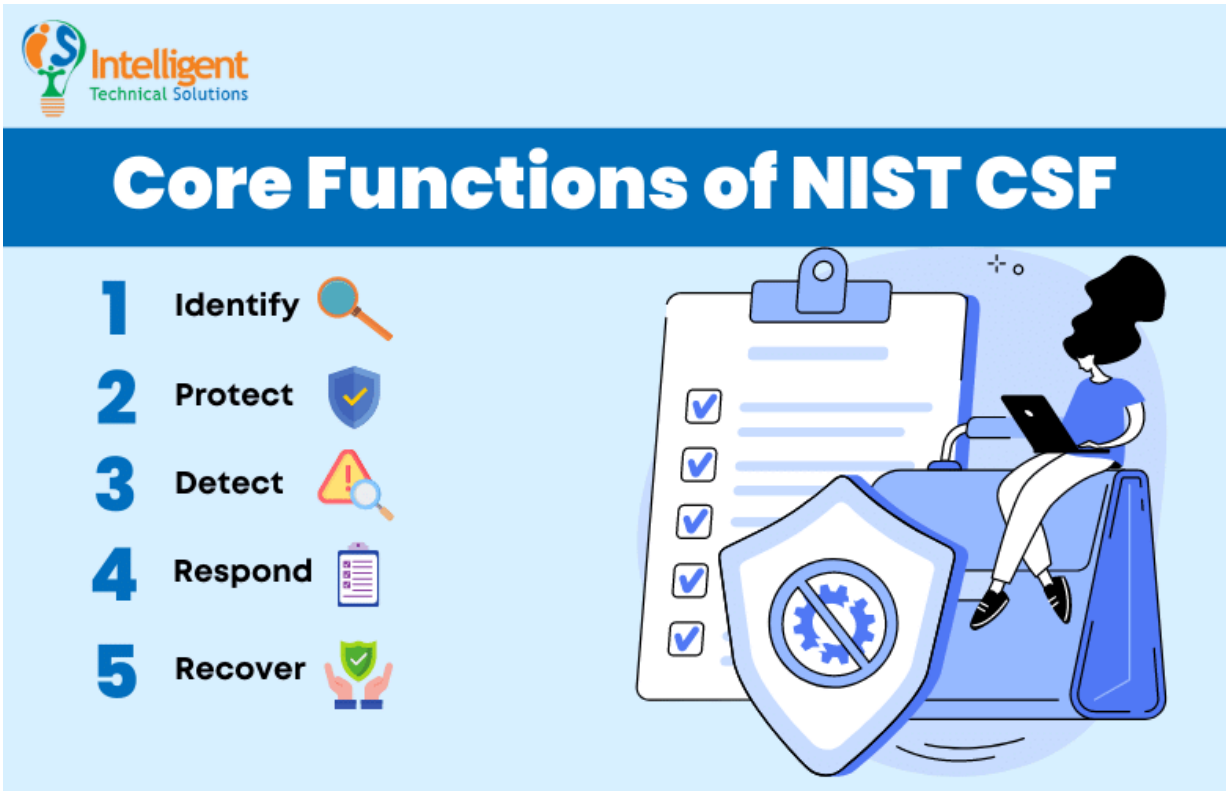
What is NIST CSF?

The NIST CSF is a framework drafted to address the lack of standards when it comes to cybersecurity. It's a voluntary measure that provides a uniform set of rules, guidelines, and standards you can use that will allow you to protect your network from cyber-attacks.

In other words, the framework **serves as a roadmap for companies that are just getting started on their cybersecurity journey**. It's the reason the NIST CSF is designed to be flexible and cost-efficient, so it can serve the entities that need it most. That's why it's most beneficial for small or less-regulated organizations and not so much for companies that already have focused IT security programs.

5 Core Functions of NIST CSF

One of the reasons the NIST CSF works so well is because it simplifies the concept of cybersecurity. It does that by categorizing all your security capabilities, projects, processes, and daily activities into the following five core functions:



1. Identify

This function is focused on laying down the groundwork for an effective cybersecurity program. It helps you develop an organizational understanding of how to manage cybersecurity risks.

The Identify function focuses on the importance of understanding cybersecurity risks in a business context, as well as the resources that support critical functions for your organization. That includes **identifying your physical and software assets, your company's environment and its role in the supply chain, network vulnerabilities, risk tolerance, and more**. Your main objective is figuring out which of your processes and assets need protection.

2. Protect

Your main goal for this function is to protect all critical functions you've identified by preventing, limiting, and containing the potential damage caused by a cyber-attack. You need to take a good look at:

- What tools you're using
- What policies do you have in place
- What processes do you need in order to achieve that goal.

3. Detect

This function's main objective is to implement tools that will detect threats that will enable you to respond to them quickly. Many cyber-attacks go undetected for weeks or even months. If that happens, you are unable to react, and the potential damage could be devastating for your business.

4. Respond

This function focuses on how well and how fast you can respond to a cyber incident. That means your business needs an incident response plan that focuses on communication, mitigation, and analysis of events at the ready.

5. Recover

The Recover function centers on creating plans for disaster recovery and business continuity. Your goal is to devise a plan that will ensure your operations can resume at their previous level in as short a period as possible after an incident.

How to Get Started with NIST CSF

To leverage the framework, you first need to enumerate all your activities and categorize them with one of the core function labels. Going through that exercise will allow you to articulate what your cybersecurity program is missing. With that, you can then adjust and implement new tools, policies, and processes until you can meet the framework's five core functions.

Why is the NIST CSF Important?

Implementing NIST's framework can bring a lot of advantages to your organization. These are some of the benefits you can enjoy:

1. It Makes Cybersecurity More Accessible for Everyone

The NIST CSF uses tried-and-tested security baselines, guidelines, and best practices that enable organizations to manage and mitigate cybersecurity risks. That means any business, small or large, can use the framework as a roadmap or reference to mature its IT security program.

2. It's a Valuable Selling Point for Your Organization

Being one of the most popular cybersecurity frameworks has its merits. For one, implementing an internationally known standard like NIST can become an important selling point that helps establish trust quickly between you and your new customers, suppliers, and providers.

3. It Helps You Achieve World-Class Cybersecurity Standards

The framework is built using the experience and expertise of various security professionals across the globe. It is recognized as an industry best practice worldwide that will elevate your organization's cybersecurity posture.

4. It Supports Your Compliance Goals

Cyber insurance and other regulatory authorities have raised their standards for compliance in recent years. NIST CSF can support your efforts to meet those goals by providing you with a cost-efficient roadmap that can help you meet compliance requirements.

Ready to Implement the NIST CSF for Your Business?

The NIST CSF is a powerful tool that can help businesses organize and improve their cybersecurity programs. It serves as an easy-to-follow roadmap or a reference that can help guide you toward achieving world-class security standards.

In order to do that, you just need to focus on the core functions of the framework, namely:

- Identify
- Protect
- Detect
- Respond
- Recover

At ITS, we are dedicated to helping businesses like yours strengthen their defenses and meet compliance requirements. Learn how IT support companies like us can help you meet those goals by leveraging our experience and expertise. Check out our article titled Can an MSP Help You with Regulatory Compliance?