# **NIST Framework**

Contenido

[Introduction 2](#_Toc160730139)

[Components of NIST Framework 2](#_Toc160730140)

[CSF Core: 2](#_Toc160730141)

[Core Functions 3](#_Toc160730142)

[Online Resources: 4](#_Toc160730143)

[Historical Points about NIST Cybersecurity Framework 4](#_Toc160730144)

[Areas covered by NIST CSF 2.0 4](#_Toc160730145)

[Success Story of NIST Framework by Saudi Aramco 4](#_Toc160730146)

[Achieving NIST Compliance 5](#_Toc160730147)

[Why should a company adapt NIST CSF? 5](#_Toc160730148)

[Conclusion 5](#_Toc160730149)

[References 6](#_Toc160730150)

## Introduction

NIST CSF contains a set of outcomes that can be utilized by organizations and governments irrespective of their background to achieve the security posture and manage the cybersecurity risks in an efficient manner. The addition of governance function which maintains the other key functions such as identify, detect, protect, respond and recover was the hot update in new release of NIST CST 2.0. The foundation of NIST Framework lies in the six functions and organizations can choose the desired outcomes to manage their cybersecurity programme. NIST framework can play a significant role in assessing, analyzing the risks that are existing and communicate the identified risks between higher level executives. Organizations can utilize NIST Framework to prepare for preventing or minimize the impact of incidents as well as managing the incidents using respond, recover and govern functions. This Framework does not specify how the outcomes are achieved but provides more details to achieve the goals through quick start guides, implementation, and informative references. Recognizing that different organizations use various technologies, CSF 2.0 is not limited to specific types, industries, or sizes. It looks ahead, ready to adapt to changes in technologies like IT, IoT, and OT.

## Components of NIST Framework

### CSF Core:

CSF core can be considered as the heart of NIST framework. It presents a taxonomy of cybersecurity outcomes, organized into Functions, Categories, and Subcategories. This structure is deliberately universal which can be leveraged for the communication by executives, managers, and practitioners, irrespective of their cybersecurity expertise.

### Core Functions

GOVERN (GV): Sets up a plan for dealing with cybersecurity risks, decides what's expected, and creates rules. Helps figure out what needs to be done in the other areas.

IDENTIFY (ID): Figures out what cybersecurity risks exist right now, spots important things like data and systems, and decides what needs attention based on a risk plan.

PROTECT (PR): Puts safety measures in place to handle cybersecurity risks and keep things safe, making it harder for bad things to happen.

DETECT (DE): Looks for signs of cybersecurity problems or attacks, trying to find them early on to analyze and respond quickly.

RESPOND (RS): Acts when a cybersecurity problem is found, managing the situation, figuring out what happened, fixing it, and letting others know.

RECOVER (RC): Gets things back to normal after a cybersecurity issue, restoring what was affected and making sure everything runs smoothly again.

Gráfico, Gráfico de proyección solar

Descripción generada automáticamente

Figure 1 NIST Core Functions

CSF Organizational Profiles:

These profiles give clear view about an organization's current or target cybersecurity posture in terms of the CSF Core's outcomes. Organizational Profiles help organizations understand, assess, and prioritize their cybersecurity risks based on their unique circumstances.

CSF Tiers:

CSF Tiers help organizations be more flexible. They show how serious and careful a group is about handling cybersecurity risks. By giving context, they help organizations decide what actions are most important based on their goals, legal rules, and how they manage things.

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

### Online Resources:

The framework is accompanied by a suite of online resources accessible through the NIST CSF website, enhancing its practical utility. These resources include:

Informative References: Direct organizations to existing global standards, guidelines, frameworks, and policies for guidance on each outcome.

Implementation Examples: Provide practical illustrations of potential approaches to achieve each outcome.

Quick-Start Guides: Offer actionable guidance on utilizing the CSF and transitioning from previous versions to version 2.0.

## Historical Points about NIST Cybersecurity Framework

**Executive Order 13636 - Feb 12, 2013:**

It was according to an Executive order signed by Barack Obama, the development of cybersecurity framework to safeguard critical infrastructure began. The aim was to promote collaborative approach involving industry, media, and government.

**Framework 1.0 Publication - February 12, 2014**: Released as voluntary guidance for critical infrastructure cybersecurity, based on existing standards and practices.

**Framework 1.1 Publication -** April 16, 2018. Version 1.1: Included more information about risk assessments and supply chain risk management.

**Framework 2.0 Publication** – Feb 26, 2024: The NIST Cybersecurity Framework (CSF) 2.0

## Areas covered by NIST CSF 2.0

The NIST Cybersecurity Framework (CSF) can a play a key role in identifying the weakness and risks associated with Cyber security. The core functions cover all the areas of cybersecurity such as physical, identity and network security to mitigate and recover from incidents. In the Identify function, organizations understand their current cybersecurity risks and prioritize efforts based on a risk management strategy. The Protect function involves implementing safeguards to prevent adverse cybersecurity events and secure assets. Detect focuses on finding and analyzing potential cyber attacks, while respond involves taking actions in response to a detected incident. The Recover function aims to restore assets and operations affected by a cybersecurity incident. The newly added Govern function emphasizes the establishment of a cybersecurity risk management strategy and policy, ensuring effective governance. These functions work together to form a comprehensive life cycle for managing cybersecurity risk, providing organizations with a flexible framework adaptable to their unique risks, technologies, and mission considerations.

## Success Story of NIST Framework by Saudi Aramco

The NIST Cybersecurity Framework has been successfully implemented by Saudi Aramco, a major energy, and chemicals producer, to enhance its cybersecurity governance. By adopting the framework, Saudi Aramco improved communication among various departments, measured cybersecurity maturity regularly, and set corporate-level targets. The framework served as a roadmap for the organization, facilitating compliance with national and international regulations. It also allowed benchmarking with other leading oil companies, contributing to mutual learning. The initiative resulted in consistent cybersecurity language, gap identification, compliance readiness, and translation of the framework into Arabic for wider dissemination. As a result of NIST Implementation, there will be annual assessments, automation of maturity assessment, ongoing benchmarking, community assistance, and the development of cybersecurity Key Performance Indicators aligned with the framework functions.

## Achieving NIST Compliance

Define Scope: Figure out what parts of your organization you want to focus on, like the whole company, specific departments, or dealing with cyber threats like ransomware.

Gather Information: Gather important details like company policies, how you manage risks, profiles of risks, business impact studies, and rules and tools for cybersecurity.

Create Profile: Write down the cybersecurity outcomes you've chosen from the CSF. Think about how your current situation affects your goals for improvement (Target Profile). You can use a Community Profile as a starting point.

Analyze Gaps and Plan: See where you fall short compared to your goals. Plan to fix those gaps, like making a list of risks or a step-by-step plan.

Implement and Update: Put your plan into action, fixing those gaps and moving toward your goals. Keep your Profile updated, noting any changes over time.

By following these steps, organizations not only achieve compliance but also engage in a continual improvement process.

## Why should a company adapt NIST CSF?

Using the CSF helps organizations talk about and manage cybersecurity risks better. They can decide how to deal with risks based on their goals. The CSF guides them internally and externally, helping prioritize actions. It also helps make smart decisions about cybersecurity spending and activities. Communication improves, creating a flow of information between executives, managers, and practitioners. The CSF acts like a guidebook for organizations, making sure everyone is on the same page about cybersecurity.

# Conclusion

In summary, the NIST Cybersecurity Framework is a strong and flexible guide for organizations to make their cybersecurity better. It has different parts like Functions and Categories that work for all kinds of organizations, no matter how big or small. The Organizational Profile and Tiers make it customizable and focused on getting better all the time, helping organizations handle cybersecurity challenges and improve continuously. NIST framework when compared to ISO 27001 is more flexible and can easily adapted by organization to manage their risks. ISO 27001 sets the standards to acquire high security posture in which organization needs to keep up with the best practices. NIST CSF which provides implementation examples for each categories in the core function can be easily utilized to design the cyber security programme for organizations.

## References

“NIST CSF vs. ISO 27001: What’s the Difference?” Vanta, www.vanta.com/collection/iso-27001/nist-csf-vs-iso-27001#:~:text=The%20difference%20here%20is%20that. Accessed 7 Mar. 2024.

Aramco, Saudi. NIST Cybersecurity Framework Success Story

The NIST Cybersecurity Framework (CSF) 2.0. 26 Feb. 2024, nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, [https://doi.org/10.6028/nist.cswp.29. Accessed 27 Feb. 2024](https://doi.org/10.6028/nist.cswp.29.%20Accessed%2027%20Feb.%202024).

Nelson, Erin. “NIST CSF 2.0: Everything You Need to Know about the Update.” Hyperproof, 4 Mar. 2024, hyperproof.io/resource/nist-csf-2-0-update/. Accessed 7 Mar. 2024.

“NIST CSF 2.0: Key Changes to Know About.” Https://Blog.netwrix.com/, blog.netwrix.com/2023/12/21/nist-csf-key-changes-to-know-about/.

Security, CyberSaint. “What Are the NIST CSF Implementation Tiers?” Www.cybersaint.io, [www.cybersaint.io/glossary/what-are-the-nist-csf-implementation-tiers](http://www.cybersaint.io/glossary/what-are-the-nist-csf-implementation-tiers).

Wikipedia Contributors. “NIST Cybersecurity Framework.” Wikipedia, Wikimedia Foundation, 5 July 2019, en.wikipedia.org/wiki/NIST\_Cybersecurity\_Framework.

“History and Creation of the CSF 1.1.” NIST, 8 Feb. 2018, www.nist.gov/cyberframework/history-and-creation-framework.