*Available online www.jsaer.com*

***Journal of Scientific and Engineering Research*, 2023, 10(8):150-157**

**Research Article**

**ISSN: 2394-2630**
**CODEN(USA): JSERBR**

# NIST Cybersecurity Framework

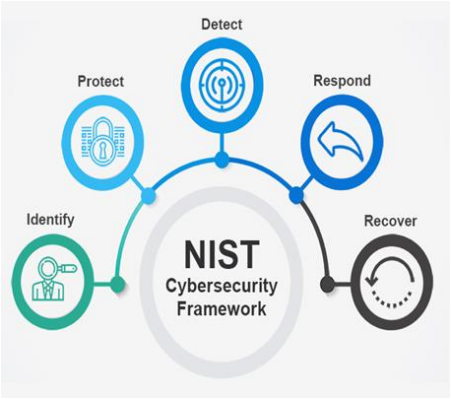
**Mohammed Mustafa Khan**

**Abstract:** The NIST Cybersecurity Framework (NIST CSF) is a voluntary approach to dealing with cyber threats in an organization. The framework is developed by the National Institute of Standards and Technology and it is designed to provide organizations with a structured method and enhance their security priorities. The framework is used across the public and private sectors in various areas such as finance, the government, health care, and critical infrastructure. This essay takes an in-depth look into the NIST Cybersecurity Framework, including its different components, leadership and implementation strategies, merits and demerits, and the framework contributing to cyber awareness.

**Keywords:** NIST Cybersecurity Framework, risk management, cybersecurity posture, critical infrastructure, cybersecurity strategy, NIST CSF, information security, cybersecurity compliance.

## 1. Introduction

The world is an interconnected village via the internet. Every organization has embraced technology and every process has been integrated to technological systems. This migrations and adoption of technology however, has created several problems to organizations. The fact that every person can access the internet, poses a great threat to organizations in terms of safeguarding client's information [1]. For this purpose, the NIST Cybersecurity Framework was developed by the National Institution of Standards and Technology, to use by every organization and should be industry independent. The framework is an appropriate tool for identifying, assessing, and addressing the problems that may affect the people within the organization. Since its inception in 2014, the CSF has been extensively used in organizations, especially in critical infrastructure [1]. It is considered to have been inspired by the potential impacts of an organizational attack. In this essay, we explore the NIST Cybersecurity Framework: breaking down its components, how it is designed to be implemented and leveraged by organizations with valuable use-cases, common pitfalls in the adoption process if not done correctly but more importantly where does a framework such as this fit into today's broader cybersecurity landscape [2].

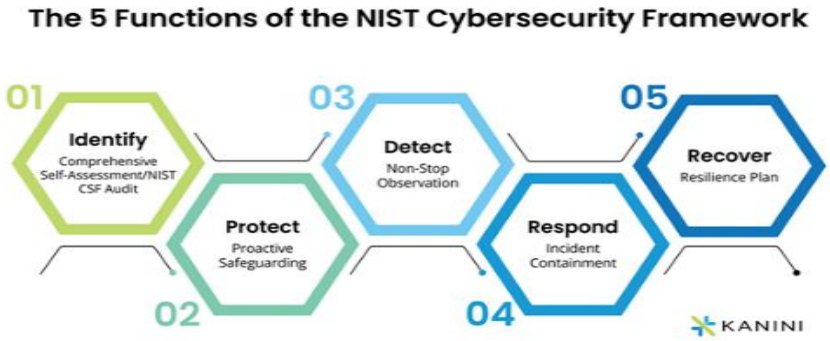



***Source:*** *https://cyberwatching.eu/sites/default/files/NIST-blog-image-1.jpg*

**Overview of the NIST Cybersecurity Framework**

The NIST Cybersecurity Framework resulted from a 2013 Executive Order (EO13636) intended to improve the cybersecurity of critical infrastructure in the US. The framework is a voluntary, risk-based approach organizations can use to improve their cybersecurity posture [6]. These consist of the market identity, a simple protection device, and five critical characteristics within cybersecurity. NIST framework is built around five core functions: Identify, Protect, Detect, Respond, and Recover. These services will be able to cover an organization's full spectrum of cybersecurity, including: How does our vulnerability scanning work [8].

**The Core Functions**




***Source:*** *https://kanini.com/wp-content/uploads/2022/09/5-Functions-of-the-NIST-Infographic.jpg*

**Identify:** This function helps organizations to understand what you have learned about cyber security risks on systems, assets, data, and capabilities [9]. This entails asset management, risk assessment, governance, etc.

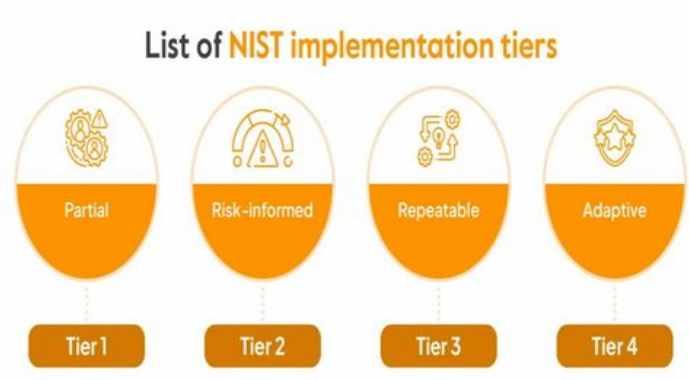
**Protect:** The protect function involves putting the safeguards needed to deliver critical infrastructure services in place. It also requires access control, data security, and maintenance activities.

Detect: this is the need to be able to identify a cybersecurity event as soon as possible so that any potential cyberattack can hopefully have less of an impact than if not detected quickly [3]. It includes continuous monitoring and detection of anomalies.

**Respond:** The Respond function involves developing and implementing appropriate activities to contain and mitigate the impact of a cybersecurity event. This includes response planning, communication, and analysis [5].

**Recover:** this functionality deals with restoring any systems or services that were affected due to an attack and restore the business operations to normalcy. The processes involved are improvements recovery planning and proper communication.

**Implementation Tiers**




***Source:*** *https://sprinto.com/wp-content/uploads/2023/10/Blog_308_Nist-implementation-tiers-Explained-03-1024x429.jpg*

Implementation Tiers, introduced by the NIST CSF, allow an organization to determine its maturity in terms of its cybersecurity practices. The tiers span from Partial (Tier 1) to Adaptive (Tier 4), indicating varying degrees of risk management processes and organizational incorporation [3]. Remember, the tiers are not a one-size-fits-

all approach but simply an aid to provide organizations with a snapshot of where they currently fall and allow them to make plans for each tier moving forward.

**Tier 1: Partial** — Risk management is ad-hoc and reactive. Within an organization, there is no concern over the issue of cybersecurity.

**Tier 2 Risk-Informed:** Practices are approved and may be emerging or partially integrated across the enterprise There is some cybersecurity awareness.

**Tier 3: Repeatable** – Risk management practices are established, likely formalized over time in some manner. The organization has a universal understanding of cybersecurity threats.

**Tier 4: Adaptive —** The organization changes its cybersecurity practices based on lessons learned (good or bad) and Indicators of Change. It is part of your organizational culture to consider aspects of risk management [4].

## 2. Implementing the NIST Cybersecurity Framework

The critical steps of the implementation process under the NIST Cybersecurity Framework include knowing and aligning it with organizational business goals [7]. The method is divided into evaluation or adaptation according to the changes of its surroundings in security within that company.

### Aligning with Organizational Objectives

One of the first steps for NIST CSF implementation is lining it up with the organization's objectives and risk management strategy. This requires a comprehensive approach used across the enterprise, bringing in stakeholders from all levels of the institution, such as senior management and IT, to cyber security teams to ensure that the framework is integrated into the organization's broader risk management processes [10]. This is an essential step for the organization about which the levels of risk they are willing to take, their fundamental capabilities and assets.

### Conducting a Risk Assessment

Risk assessment is one of the best methods to detect cybersecurity risks in your organization. It requires comprehending how much destruction various cybersecurity risks trigger and the opportunity with which some system or data could be targeted. Making a risk assessment is the key to figuring out where in the Framework it makes sense so that you are working on spending all those resources in the right areas [2].

### Developing a Current Profile

Documentation of existing cybersecurity control demonstrations. Align the organization's existing practices with NIST CSF core functions and categories. This can inform the current and future state of where your organization is falling short on cyber security, acting as a before-and-after-snapshot benchmark to track success [1].

### Defining a Target Profile

A target profile is established following the current profile, representing how that organization should practice cybersecurity. Target profile: Describes the organization's risk management goals, regulatory requirements, and industry best practices [10]. It guides the implementation of the Framework and attaining target cybersecurity maturity levels.

### Creating an Action Plan

The organization then develops an action plan to bridge those profiles between as-is and target. The plan should identify focus areas, specify actions, and layout timetables for doing them. This reliable plan must provide an inventory of standards and specifications, a way to monitor performance results, and room for improvement [5].

### Continuous Improvement

The NIST CSF should be customized to change as maturity in security capabilities increases. Achieving this requires you to audit the implementation regularly, keep an eye on what is going abroad in the cybersecurity world, and then modify your action plan [6]. Furthermore, this helps keep the organization strong from new threats and compliance requirements.


***Source**: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcT0YPS88rN3j81JrT2l_AuhYga6FeZSnAhekg&s*

**3. Advantages of the NIST Cybersecurity Framework**

**Enhanced Risk Management**

The NIST Cybersecurity Framework's most significant benefit is its focus on risk management. The Framework offers a structure that identifies and defends various risks in an organized manner to minimize the possibility of cyber-attacked impact on organizations, which should be kept within tolerable margins [8]. Using risk management as a guide, this approach invests resources where they will do the best (the make it or break it), resulting in more for your cybersecurity buck.

**More Regulatory-Compliant**

Numerous industries boast heavily regulated plumbing in the cybersecurity and privacy landscape. The NIST CSF makes this link more tangential by mapping these controls to the specific risk requiring mitigation so that when audited, organizations can demonstrate they have realigned security practices using cost and legal protections from an audit, which could go after them at a later date [4]. Regulators also accept the Framework, which can be used as proof of effort in cybersecurity audits, assessments, or any evidence thus needed by auditors.

**Greater Business Resilience**

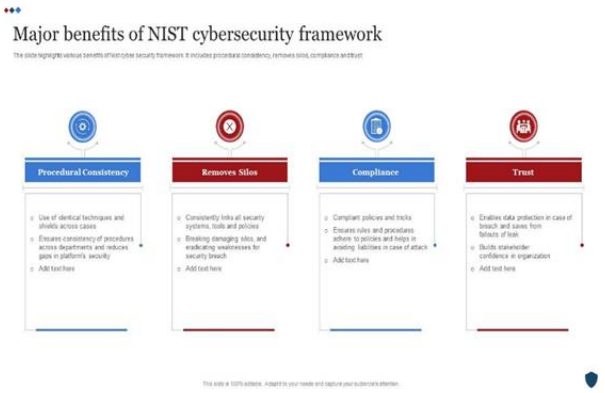
The emphasis of NIST CSF on continuous monitoring, detection, and (real-time) response is critical to organizations' readiness, which will need to not just deal with global cyber threats but do so as resiliently as possible [9]. The Framework enables enterprises to quickly identify and address an incident, reducing the potential harm cyberattacks can create. A further benefit of the Recovery function is that it allows organizations to get back up and running quickly following an incident, reducing detrimental downtime and lost business [5].

**Facilitates communication**

The NIST CSF can assist in harmonizing cybersecurity risk taxonomy and practices, enabling communication across organizational locations. A shared language facilitates the communication of cybersecurity priorities and objectives throughout an organization at all levels in a way that both technical and non-technical staff can comprehend [3]. Better decisions will come from good communication and collaboration in cyber security risk management.

**Flexibility and Scalability**

The NIST CSF is intentionally designed to be adaptable and flexible, making it appropriate for organizations of all sizes across any industry. This variable depends on the size of an organization and can, therefore, be adjusted as appropriate relative to the organization's needs/risk profile [2]. A system like this can be implemented whole or piecemeal, but some elements may get a heavier lift than others due to pathway ties back into an organization.




***Source:*** *https://www.slideteam.net/media/catalog/product/cache/1280x720/m/a/major_benefits_of_nist_cybersecurity_framework_slide01.jpg*

**4. Challenges in Implementing the NIST Cybersecurity Framework**


***Source:*** *https://www.centraleyes.com/wp-content/uploads/2022/12/Group-25206-1024x578.png*

The NIST Cybersecurity Framework is highly beneficial, but implementing it presents challenges. Resource shortages, complexity, and ongoing cybersecurity commitment requirements can challenge organizations.

**Resource Constraints**

Something like the NIST Cybersecurity Framework (CSF) can be an enormous lift in time and resources, personnel reassessment, and other potential investments. For SMEs, these constraints are often even more pronounced. But as a complete stack framework, this demands regulatory bodies to perform audits of the current cyber security facets, devise methods on account& make improvements. Cybersecurity tools and technologies are not cheap to purchase/ deploy, nor is training on such practices [9]. It is well known that a complete recognition or an immediate implementation of some cybersecurity framework, such as NIST, can be very expensive for many organizations. On top of that, it would have to fit in with all the other things a business need. Therefore, it is sometimes impossible to get the required level of support from senior leadership so that they can allocate resources towards cybersecurity that would enable you to operationalize this framework [9].

**Complexity of Implementation**

The NIST CSF is a broad, sophisticated framework for the entire cyber security effort. The framework is extensive, and implementing it can be daunting for organizations with no or a very immature cybersecurity program. Yet, arriving at an accurate risk assessment, an up-to-date target profile, and mapping strategies will require technical cybersecurity strategic know-how [9]. Thus, it is difficult for companies to adapt the framework to their existing technology processes. Add to this the presence of legacy systems, old software, and multiple methods for cybersecurity, which only multiply implementation problems [1].

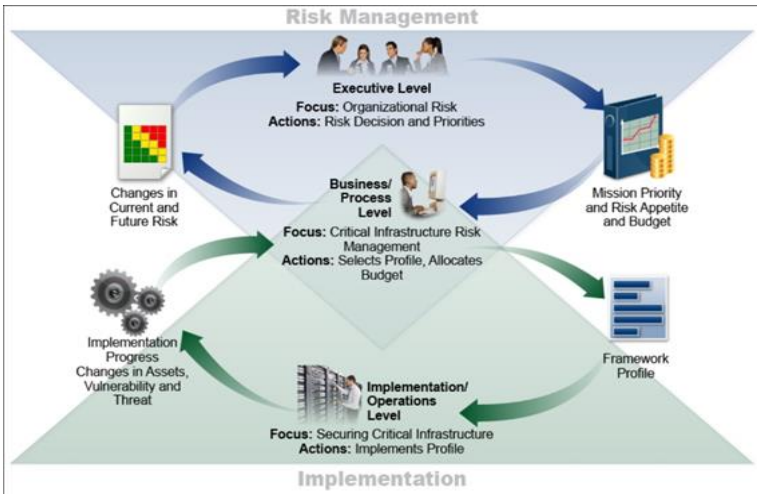
**Persistent Commitment Necessity**

Deployment of the NIST CSF is not a lifecycle or one-and-done exercise but an ongoing effort that involves actual work necessary to create meaningful change and improve cybersecurity practices over time [3]. This long-term effort means the framework must be continually reviewed, audited, and improved to stay up-to-date as threat actors change their techniques. At the same time, technological capabilities advance along with regulatory obligations. Sustaining such a commitment can be challenging, especially in an organization whose primary mission does not involve cybersecurity [7]. However, if demand for training, awareness programs, and resource commitment remains constant, it can lead to "compliance fatigue," causing organizations to let up on or lose sight of cybersecurity over time. Doing so could add significantly to an organization's risk profile if weaknesses implicated in such a framework might be rendered less effective [7].

**Adapting to Emerging Threats**

The cybersecurity industry evolves rapidly and new threats by attackers and the highest number of vulnerabilities in legacy software are found virtually daily. Although NIST CSF has been created to be flexible and accommodating, keeping up with the rate at which an organization's attack surface growth might find them struggling, this security pyramid has begun to crumble as, in reality, it is unable to fix the issues that are arising with these new technologies such as IT & IoT and cloud computing [6]. Because cybersecurity risks are constantly evolving, NIST CSF should be crafted and updated often, diverting resources away from its main effort at the time of creation.

## 5. **Positioning the NIST Cybersecurity Framework in Context**




***Source:*** *https://www.ssh.com/hubfs/Imported_Blog_Media/Cybersecurity_Framework_Proces_Overview-2.png*

Essential legislation like the NIST Cybersecurity Framework, causing wider adoption of common standards amongst organizations has a great innovative scope for securing data rights across borders [7]. It has been elevated from a tool for managing cyber risks to being in the security conversation.

**Impact on Industry Standards 5.1 Influence on Standards**

Since its release, the NIST CSF has become popular in many industries—especially those with a stake in cybersecurity such as finance, healthcare, energy, and critical infrastructure. Its risk-based approach and focus on well-known industry requirements have made it applicable to many US federal agencies in meeting domestic and international standards [10]. It also has affected the development of other standards and guidelines on cybersecurity. It has also helped in developing a broader consensus on issues that matter for cybersecurity [2]. This framework applies the best practices that many industry groups and professional organizations have also adopted so it is unified in security throughout different sectors.

**Government & Regulatory Acceptance**

The NIST CSF is now part of the framework that all government organizations use as a critical national cybersecurity policy component. In the USA, for example, federal agencies are directed to follow a framework

to enhance their cybersecurity and secure critical infrastructure [9]. It has been employed in numerous legislative and regulatory proposals for increased national cybersecurity readiness. Indeed, the NIST framework has gained enough traction internationally that several countries utilize it to their regulatory environments [9]. The widespread use of this framework globally demonstrates its versatility and how it can address different cyber security issues across cultures or regulations.

**Strengthening Public-Private Partnerships**

In the combined fight against cyber threats, NIST CSF has been one of many turning points connecting public and private sector entities. The platform served as a common language which enabled government solutions to talk with each other, and even private companies or outside stakeholders could reach out [5]. Since cybersecurity is an issue that knows no organization or national boundaries, public-private partnerships are a global imperative. NIST CSF provides a common language to share best practices and collaborate on efforts to protect their cyber defenses.

**Contribution to the Global Cybersecurity Effort**

Cybercrime is a global issue, and the international community needs to take action (together). It has been adapted into complementary models for specific countries and is used in industries such as healthcare to support international efforts addressing cybersecurity [7]. It establishes a basis for more systematic and national-caliber public-private sector cybersecurity across nations. It will serve as a model for many other countries and reduce the parochialism of global cybercrime control efforts. Further, given this framework's focus on risk management and continuous improvement principles, it is also a natural fit for cybersecurity globally [8]. These frameworks can genuinely give all the stakeholders a world of good! Therefore, promoting such qualities is something that the NIST CSF can use to help develop more significant cyberspace.

## 6. Case Studies

**The Financial Services Industry**

The financial services industry is one of the top sectors in which cyberattacks occur due to the value associated with handling data and potential monetization for attackers, which can rise higher than thousands of million per successful attack. A leading global bank tasked with securing its cyber posture to satisfy compliance and regulatory requirements using the NIST CSF [5]. The bank also undertook a complete risk assessment to map the likely holes in their systems and processes. It then developed a current profile to understand its existing cybersecurity practices and a target profile to set goals for improvement. That remediation plan strengthened data security, access controls, and incident response capabilities. The bank had significantly reduced its exposure to cyber threats by using NIST CSF. By focusing on continuous monitoring and response, the bank could detect if a threat event had occurred, along with real-time mitigation in place. Moreover, this successful block build enabled the bank to be regulatory compliant and win over their customers'/stakeholders' faith [8].

**Case Study 1: Healthcare Industry**

the healthcare industry has a unique and extraordinary cybersecurity challenges especially around securing patient data with regulations like Health Insurance Portability And Accountability Act (HIPAA) that companies need to comply with. For instance, one of the largest healthcare providers in the country adopted NIST CSF to alleviate these problems and become more resilient overall from a cybersecurity resilience perspective [4]. After all of this information was collected, the healthcare provider completed a risk assessment to determine what they believe are the most significant risks related to patient data and critical systems. From there, the local government worked with stakeholders to add better access controls and employee training as part of an overarching cybersecurity plan [3]. Huls uses whatever tools are available or required under state law but follows those principles in a comprehensive strategic planning process using NIST CSF.

The results of applying the framework described in the cases above are as follows. The provider managed to reduce the risk of data breaches, improve compliance with HIPAA, and increase its preparedness for cyber incidents [10]. Increased cybersecurity awareness was also achieved: better collaboration between IT specialists, clinicians, and administrators was facilitated, which played a significant role in ensuring that all parties understood their roles concerning cybersecurity [9]. The energy provider applied the NIST CSF to protect one of the most vulnerable critical infrastructures from cyber threats. The instrument helped improve its performance to detect and respond to cyber incidents.

**Conclusion**

While using the NIST CSF comes with obstacles like resource constraints, complexity and requires continual investment, at its core are many advantages far surpassing these challenges [7]. The framework is also intended to provide a consistent and cost-effective mechanism for organizations, regardless of their reliance on cyberspace-based systems or capabilities, that are willing to protect themselves against cybersecurity threats and the necessary business linkages with standard requirements across sectors within a comprehensive system of systems. Springing from individual adoption, the NIST CSF—used by federal government agencies and their suppliers—has catalyzed voluntary efforts within industry sectors and contributed to the global cybersecurity ecosystem. Cyber resilience is fundamentally a resilient culture; having the framework written in this fashion keeps perceived novelty low since it uses language and practices that cyber professionals are more than familiar with [6]. With cyber threats evolving, the NIST Cybersecurity Framework will guide organizations in securing their enterprise. Its flexibility, scalability capabilities and commitment to continuous improvement will ensure its ongoing importance in strengthening cybersecurity resilience for many years [7].

**References**

[1]. M. Frayssinet Delgado, D. Esenarro, F. F. Juárez Regalado, and M. Díaz Reátegui, "Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations," 3C TIC: Cuadernos de desarrollo aplicados a las TIC, vol. 10, no. 2, pp. 123–141, Jun. 2021, doi: https://doi.org/10.17993/3ctic.2021.102.123-141.

[2]. G. B. White and N. Sjelin, "The NIST Cybersecurity Framework," Research Anthology on Business Aspects of Cybersecurity, 2022. https://www.igi-global.com/chapter/the-nist-cybersecurity-framework/288672

[3]. M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," Sustainability, vol. 15, no. 18, p. 13369, Jan. 2023.

[4]. K. Thakur, M. Qiu, K. Gai, and M. L. Ali, "An Investigation on Cyber Security Threats and Security Models," IEEE Xplore, 2019. https://ieeexplore.ieee.org/abstract/document/7371499

[5]. "Public Draft: The NIST Cybersecurity Framework 2.0 National Institute of Standards and Technology Note to Reviewers," Aug. 2023. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf?ref=zimmergren.net&utm_campaign=zimmergren&utm_medium=blog&utm_source=zimmergren

[6]. H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," Electronics, vol. 11, no. 14, p. 2181, Jul. 2022, doi: https://doi.org/10.3390/electronics11142181.

[7]. I. Lee, "Cybersecurity: Risk management framework and investment cost analysis," Business Horizons, vol. 64, no. 5, Feb. 2021, Available: https://www.sciencedirect.com/science/article/pii/S0007681321000240

[8]. R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. Gupta Gourisetti, "Cyber Threat Dictionary Using MITRE ATT amp;CK Matrix and NIST Cybersecurity Framework Mapping," IEEE Xplore, Oct. 01, 2020. https://ieeexplore.ieee.org/abstract/document/9241271

[9]. M. Barrett et al., "Approaches for Federal Agencies to Use the Cybersecurity Framework," Aug. 2021, doi: https://doi.org/10.6028/nist.ir.8170-upd.

[10]. U. Saritac, X. Liu, and R. Wang, "Assessment of Cybersecurity Framework in Critical Infrastructures," IEEE Xplore, Feb. 01, 2022. https://ieeexplore.ieee.org/abstract/document/9753250/