NEXTLABS®

White Paper

Understanding the NIST Cybersecurity Framework 2.0

Background

Executive Order 13636 (EO), “Improving Critical Infrastructure Cybersecurity,” was issued on February 12, 2013 to strengthen the resilience of the United States’ critical infrastructure. This Executive Order calls for the development of a voluntary Cybersecurity Framework that provides a “prioritized, flexible, repeatable, performance-based, and cost-effective approach” to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services.

In response, the National Institute of Standards and Technology (NIST) developed and published a Cybersecurity Framework (CSF). This Framework has since been updated and is now in its second iteration (NIST CSF 2.0). The NIST CSF 2.0 is a set of guidelines, best practices, and standards to help organizations manage and improve their cybersecurity posture. It provides a structured approach for organizations to identify, protect, detect, respond to, and recover from cyber threats and incidents. The framework is widely used by businesses, government agencies, and other organizations to assess and enhance their cybersecurity resilience.

The NIST CSF 2.0 complements, but does not replace, an organization’s risk management process and cybersecurity program. The NIST CSF 2.0 is not industry-specific, and the common taxonomy of standards, guidelines, and practices that it includes is not country-specific, allowing organizations outside the United States to also use the CSF 2.0 to strengthen their own cybersecurity efforts. With its broad adoption the NIST CSF 2.0 contributes to developing a common language for international cooperation on critical infrastructure cybersecurity.

Overview of the NIST Cybersecurity Framework (CSF)

The NIST CSF 2.0 consists of three main components:

1. Framework Core
2. Organizational Profiles
3. Tiers

Framework Core

The Framework Core provides a set of cybersecurity activities, outcomes, and references common to organizations. It is divided into six key functions: Govern, Identify, Protect, Detect, Respond, and Recover. Each function is further broken down into categories and subcategories, offering a structured approach for managing and improving cybersecurity posture.

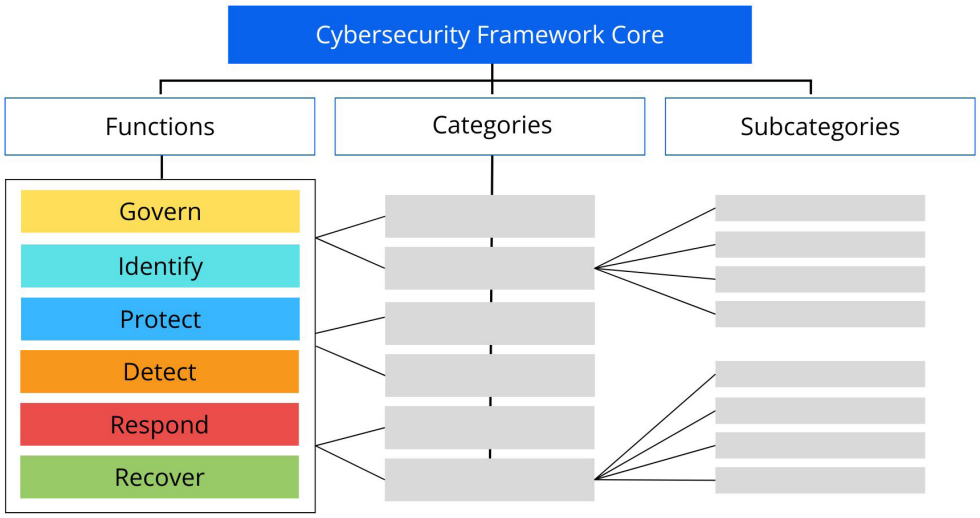

Figure 1: Cybersecurity Framework 2.0 Core Structure

The six CSF 2.0 Core Functions define cybersecurity outcomes at their highest level. Of these six functions, Govern, Identify, and Protect are proactive, focusing on assessing risk and enforcing access controls to prevent breaches before they occur. On the other hand, Detect, Respond, and Recover are reactive and define the actions organizations will take if malicious activity is detected. Both the proactive and reactive functions are necessary and complement one other.

Govern: An organization's cybersecurity risk management strategy, expectations, and policy must be established, communicated, and monitored. This function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five functions in the context of its mission and stakeholder expectations.

Identify: An organization's current cybersecurity risks must be understood. This is achieved through assessing the organization's assets, suppliers, and associated cybersecurity threats, and allows for aligning efforts with its risk management strategy outlined in Govern. This process also involves identifying areas for improvement in the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management.

Protect: Security measures are implemented to handle the organization's cybersecurity threats. After identifying and prioritizing assets and risks, the Protect function helps to secure these assets to minimize or prevent cybersecurity incidents and maximize the potential for capitalizing on opportunities. This function encompasses managing identities, authentication and access control, conducting awareness and training programs, ensuring data security, safeguarding platform integrity (including both physical and virtual components), and enhancing the resilience of technology infrastructure.

Detect: Potential cybersecurity breaches and compromises are identified and assessed. The Detect function enables the timely detection and analysis of anomalies, signs of malicious activity, and other potentially adverse occurrences that suggest cybersecurity attacks and incidents may be underway. This function supports successful incident response and recovery activities.

Respond: Steps are initiated upon discovering a cybersecurity incident. Respond supports the ability to contain the effects of cybersecurity incidents. Outcomes within this function include incident management, analysis, mitigation, reporting, and communication.

Recover: Assets and operations impacted by a cybersecurity incident are restored. The Recover function supports the swift restoration of normal operations to mitigate the consequences of cybersecurity incidents and enable effective communication throughout the recovery process.

Organizational Profiles

A NIST CSF 2.0 Organizational Profile describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes. Organizational Profiles are used to understand, tailor, assess, prioritize, and communicate the Core's outcomes by considering an organization's mission objectives, stakeholder expectations, threat landscape, and requirements.

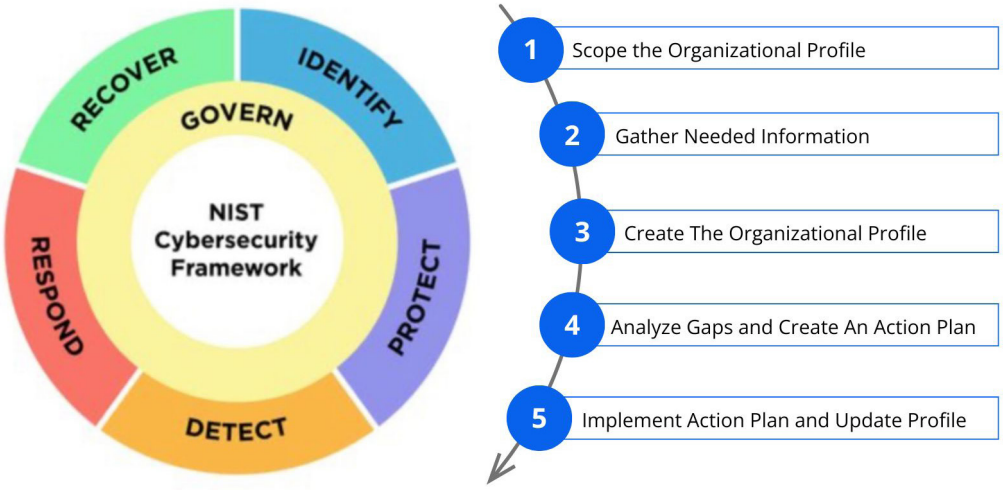

Figure 2: Steps to Creating and Using An Organizational Profile

Tiers

An organization can choose to use Tiers to inform its Current and Target Profiles. Tiers characterize the rigor of an organization's cybersecurity risk governance & management practices and fall into the categories of Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). The Tiers describe a progression from informal, ad hoc responses to agile, risk-informed approaches that are continuously improving. These tiers help organizations assess their current cybersecurity maturity level and establish a roadmap for improvement. By aligning their cybersecurity practices with the Framework Core and advancing through the tiers, organizations can enhance their cybersecurity resilience and better protect against cyber threats.

Differences between CSF 1.0 and 2.0

The first version of the NIST CSF (1.0) was released in February 2014 and was updated in February 2024 following a multiyear process of discussions and public comments aimed at making the framework more effective.

One major change to CSF 2.0 is the addition of the Govern function (GV) to the existing core functions of Identify, Protect, Detect, Respond, and Recover (IDPRR). This additional function highlights the significance of setting up a robust governance structure to oversee cybersecurity risk management at the organizational level. In CSF 1.0, elements of the new Govern function were present, such as leadership commitment, risk, but are now explicitly addressed within the Govern function.

CSF 2.0 expands the applicability of the NIST CSF. CSF 1.0 mainly focused on critical infrastructure entities and providing a standardized approach for managing their cybersecurity posture, which is reflected in the original title, "Framework for Improving Critical Infrastructure Cybersecurity." To address the growing cyber threat landscape and the need for a broader framework, NIST has broadened the applicability of the NIST CSF to industries beyond critical infrastructure in CSF 2.0.

In addition, CSF 2.0 underscores the importance of securing supply chains. Recent notable cyberattacks aimed at third-party vendors have underscored potential weaknesses within interconnected networks. Although not directly covered in CSF 1.0, addressing supply chain risk has become a central aspect within the framework, pushing organizations to evaluate the security stance of their vendors and deploy measures to minimize potential vulnerabilities.

The experience in using the CSF is also different for CSF 2.0 NIST has introduced the CSF 2.0 Reference Tool, a digital resource offering users a more accessible way to navigate the framework. The CSF 2.0 Reference Tool integrates a searchable repository of informative sources, enabling organizations to compare the framework's recommendations with pre-existing cybersecurity materials and utilities.

"The NIST Cybersecurity Framework has become the gold standard for cybersecurity over the past decade, providing guidance to organizations on assessing, prioritizing, and communicating cybersecurity risks and strategies," said Cherilyn Pascoe, Director of the NIST NCCoE. "With this major update, NIST worked with the community to build on CSF 1.1 to address current and future cybersecurity risks, as well as make the Framework easier and more effective for organizations to use. The NIST Cybersecurity Framework 2.0 now addresses cybersecurity risks for all organizations, not just those in critical infrastructure, as well as places additional focus on critical topics such as cybersecurity governance, supply chain security, and incident response and recovery. We look forward to working with the community, including through our work at the NIST NCCoE, to help organizations best leverage this new version of the Framework to address their specific risks and needs."

Overall, the shift from NIST CSF 1.0 to 2.0 reflects a crucial advancement amidst the continually shifting cybersecurity environment. With its expanded focus, emphasis on governance and supply chain security, and improved user interface, the framework emerges as an invaluable resource for organizations striving to enhance their cybersecurity resilience.

How Should Organizations Use the NIST CSF?

Implementing the principles of the NIST CSF offers numerous benefits for organizations looking to enhance their cybersecurity posture and resilience. By following the CSF 2.0's guidelines and best practices, organizations can establish a comprehensive cybersecurity program tailored to their specific needs and risk profile.

The CSF 2.0 promotes a risk-based approach to cybersecurity, focusing resources and efforts on mitigating the most significant threats and vulnerabilities. By prioritizing cybersecurity activities based on risk assessment, organizations can allocate resources more effectively and efficiently, maximizing the impact of their cybersecurity investments.

Another crucial aspect of the CSF 2.0 is its alignment with industry standards and best practices. By implementing the CSF 2.0, organizations can ensure that their cybersecurity program meets recognized benchmarks and is consistent with industry norms. This alignment not only enhances the organization's cybersecurity posture but also fosters trust and confidence among customers, partners, and stakeholders. Furthermore, adopting the CSF 2.0 can help organizations improve their cybersecurity governance and oversight. The CSF 2.0 emphasizes the importance of executive leadership and board-
level involvement in cybersecurity decision-making, promoting a culture of cybersecurity awareness and accountability throughout the organization.

Implementing the NIST Cybersecurity Framework 2.0 offers organizations a structured, flexible, and risk-based approach to managing cybersecurity risks. By following the CSF 2.0's guidelines and best practices, organizations can enhance their cybersecurity resilience, align with industry standards, and foster a culture of cybersecurity excellence.

Using NextLabs Solutions to Adopt the NIST CSF

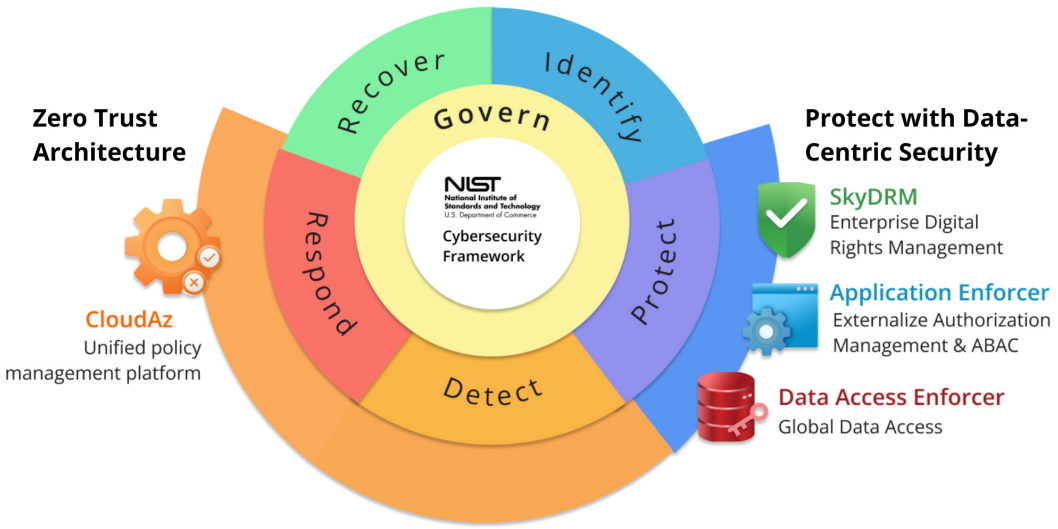

Figure 3: NextLabs Solution for CSF 2.0

The NextLabs solution enables organizations to implement the NIST CSF 2.0's core functions and subcategories and is highly customizable, enabling organizations to tailor it to their specific needs and risk profile. Additionally, the solution provides a range of reporting and analytics capabilities that enable organizations to monitor and measure their cybersecurity performance and to demonstrate compliance with regulatory requirements.

Govern

The Govern function's main goal is to ensure that the organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

With NextLabs Zero Trust Data Security, organizations can implement the Govern function by establishing dynamic security policies to protect business-critical assets and mitigate the risk of a cybersecurity breach (GV.PO). These policies are set according to an organization's needs and the types of data they store and can be defined based on various factors such as user roles, resource classifications, time of day, location, and more. This granular control enhances security and helps enforce the principle of least privilege. These policies are then centrally managed and deployed across all applications with our patented, dynamic authorization policy engine. Centralized policy management allows for increased agility as policies can be easily modified or updated without making significant changes to the underlying system or application (GV.OV). This flexibility also allows organizations to adapt quickly to evolving business requirements, regulatory changes, or new security needs.

Identify

The Identify function's purpose is ensuring the organization's current cybersecurity risks are understood.

NextLabs helps organizations implement the Identify function. Enforcers, which augment an application's underlying security model, can leverage data classification by automatically identifying sensitive data types based on the app's data model, then organizes this data (ID.AM). Enforcers can discern and collect relevant access activity data to facilitate centralized correlation and detection of anomalous activity, therefore potential threats can be recorded (ID.RA).

Protect

For the Protect function, organizations must put safeguards in place to manage the organization's cybersecurity risks.

To implement the Protect function, NextLabs offers functional solutions based on Zero Trust data security principles. NextLabs enforcers persistently protect files across the information cycle using attribute-based policies. Attribute-based policies dynamically grant permissions for specific actions, such as viewing, editing, copying, forwarding, printing, and extracting content, based on the recipient's identity (PR.AA). The solution provides persistent control of access and usage of digital information stored in files regardless of where it exists. It can safeguard and monitor business-critical documents such as intellectual property and product design, wherever it lives or travels – across devices, data centers, apps, cloud services, and on-premises (PR.DS). Like NextLabs' other solutions, enterprises can continuously monitor and audit access, providing increased visibility. (PR.PS).

Detect

The Detect function covers the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring.

To implement the Detect function, NextLabs offers solutions with centralized logging and monitoring. The NextLabs solution allows for enterprise-wide activity logging to promptly identify any suspicious activity and anomalies (DE.CM). With NextLabs, organizations can track and store real-time user and data access activity across apps and services in a central audit repository, simplifying the process of auditing security controls (DE.AE).

Respond

The Respond function is designed to manage the impacts of cybersecurity incidents. It encompasses outcomes related to incident handling, analysis, mitigation, reporting, and communication.

NextLabs' solutions support the Respond function with our patented dynamic authorization technology. Because the attribute-based policies are dynamically evaluated at the time of the data access request, if there are threats detected, that information can be automatically incorporated into the policy decision and enforcement (RS.MA).

Govern (GV)	Identify (ID)	Protect (PR)	Detect (DE)	Respond (RS)	Recover (RC)
Organizational Context (GV.OC)	Asset Management (ID.AM)	Identify Management, Authentication, and Access Control (PR.AA)	Continuous Monitoring (DE.CM)	Incident Management (RS.MA)	Incident Recovery Plan Execution (RC.RP)
Risk Management Strategy (GV.RM)	Risk Management (ID.RA)	Awareness and Training (PR.AT)	Adverse Event Analysis (DE.AE)	Incident Analysis (RS.AN)	Incident Recovery Communication (RC.CO)
Roles, Responsibilities and Authorities (GV.RR)	Improvement (ID.IM)	Data Security (PR.DS)		Incident Response Reporting and Communication (RS.CO)	
Policy (GV.PO)		Platform Security (PR.PS)		Incident Mitigation (RS.MI)	
Oversight (GV.OV)		Technology Infrastructure Resilience (PR.IR)			
Cybersecurity Supply Chain Risk Management (GV.SC)					

Figure 4: CSF 2.0 Core Function and Category Names and Identifiers

Key Takeaways

The Cybersecurity Framework 2.0 is a vital tool for organizations navigating the complexities of digital security. It operates as a complement to existing risk management processes and cybersecurity programs, rather than a replacement. By providing a structured approach to cybersecurity, the CSF 2.0 offers a roadmap for organizations to assess and strengthen their defenses against cyber threats.

Version 2.0 of the CSF introduced has several notable enhancements. The addition of the Govern function underscores the importance of governance and leadership in driving cybersecurity initiatives, while the framework's expanded applicability ensures its relevance across various industries and organizational sizes. Version 2.0 also places greater emphasis on supply chain security, reflecting the evolving nature of cyber threats in interconnected digital ecosystems.

In today's rapidly evolving digital landscape, implementing the CSF 2.0 is essential for organizations seeking to safeguard their assets and data against cyber threats. By adopting the framework's latest principles and best practices, organizations can enhance their cybersecurity measures and adapt to emerging challenges effectively. Ultimately, the CSF 2.0 empowers organizations to proactively manage cybersecurity risks and protect against potential vulnerabilities, thereby safeguarding their operations and reputation in an increasingly interconnected world.

References

Davis, N. (n.d.). *Navigating the Evolving Cybersecurity Landscape: A Deep Dive into NIST CSF 1.0 vs. the New February 2023 Release of NIST CSF 2.0.* Retrieved from LinkedIn: https://www.linkedin.com/pulse/navigating-evolving-cybersecurity-landscape-deep-dive-davis--tcvbc/

Lasenko, N. (n.d.). *NIST CSF 1.0 and 2.0 Comparison: A List of Key Changes*. Retrieved from LinkedIn: https://www.linkedin.com/pulse/nist-csf-10-20-comparison-list-key-changes-lasenko-bba-cisa-cissp-anuqe/

NIST CSF 1.0. (n.d.). Retrieved from National Institute of Standards and Technology: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

NIST Cybersecurity Framework 2.0. (n.d.). Retrieved from National Institute of Standards and Technology (NIST): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.