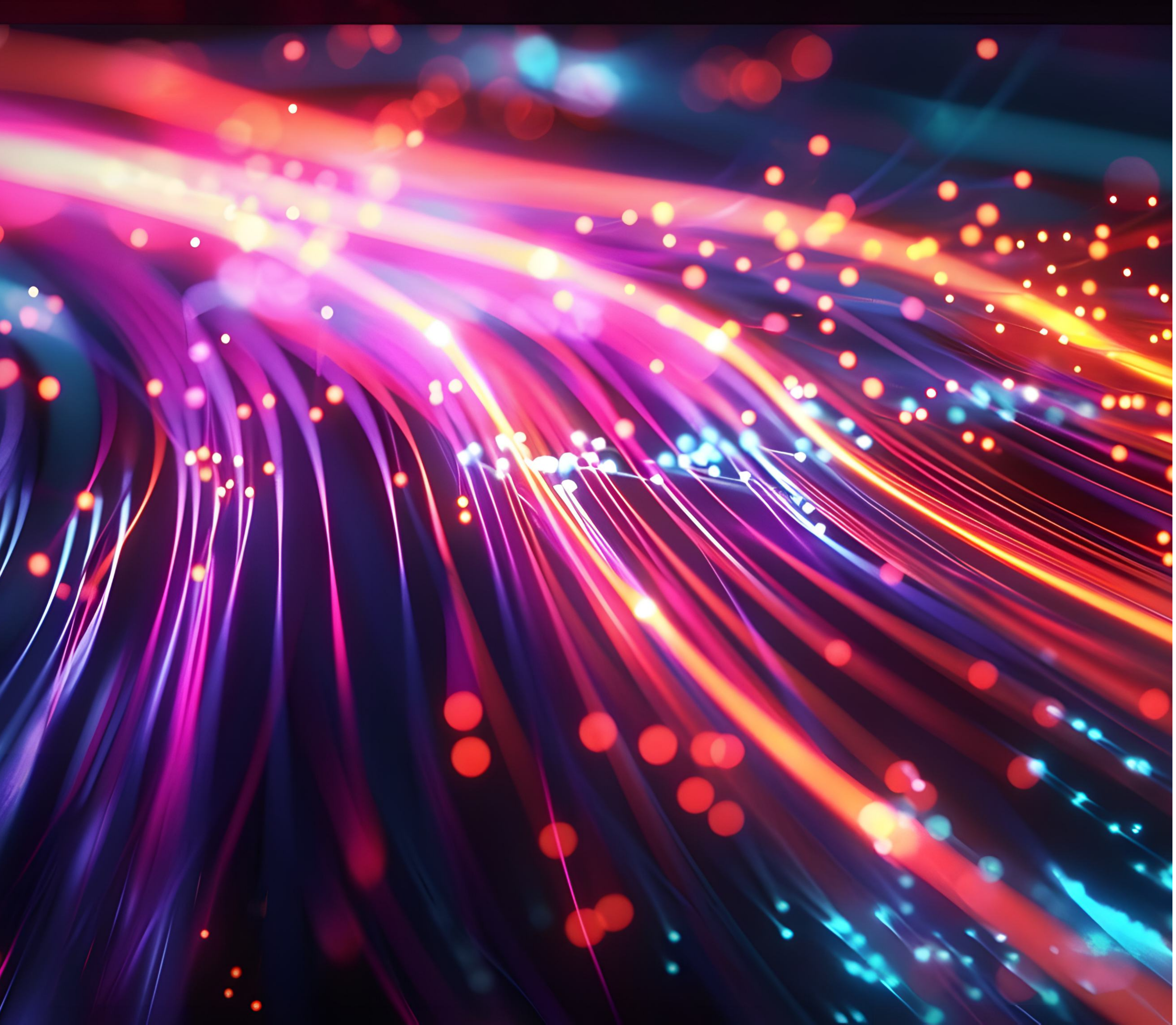
AUDITBOARD

NIST CSF 2.0: A CISO’s Guide

By Claude Mandy



The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) has become one of the most widely adopted standards for organizations seeking to enhance their cybersecurity posture and inform their cybersecurity control requirements. It provides a level of business abstraction into non–technical terms that other standards have been missing. This makes it easy to describe what the controls in each function are intended to do in non-technical terms: Identify, Protect, Detect, Respond, and Recover. Recently, NIST released the 2.0 version of the framework.

In this blog, I highlight the key changes from NIST CSF 1.0 and the implication of these changes based on how CISOs generally use NIST CSF. Most importantly, I encourage CISOs to consider the usage of NIST CSF as intended by the framework's creators.

Key Changes in NIST CSF 2.0:

Lots of industry experts have weighed in on the changes in NIST CSF 2.0, myself included. The biggest visible change to NIST CSF is the introduction of a new "Govern" function. “Govern” has become central to the rest of the pillars, as it informs how an organization will implement the other five functions.

- *Govern:* Establish and monitor your company's cybersecurity risk management strategy, expectations, and policies.
- *Identify:* Determine the current cybersecurity risks to the business.
- *Protect:* Support your ability to use safeguards to prevent or reduce cybersecurity risks.
- *Detect:* Find and analyze possible cybersecurity attacks and compromises.
- *Respond:* Take action regarding a detected cybersecurity incident.
- *Recover:* Restore assets and operations impacted by a cybersecurity incident.

Sustainable use of the CSF is only possible with clear governance and structures to support decision-making. This includes gathering organizational context, establishing oversight committees, defining risk management strategy, and clarifying roles and responsibilities.

To address the formalization, CISOs should start by reviewing (and formalizing, if non-existent) their own governance and cyber risk management practices, and aligning where possible with NIST CSF terminology. By establishing the cybersecurity governance structure, including roles and responsibilities for cybersecurity risk management at all levels, CISOs have a clear decision-making framework to help them decide what should be done within their organizational constraints.

Another significant update is the broadening of the framework's scope. NIST CSF 2.0 now is deemed suitable for all organizations across government, industry, and academia–not just critical infrastructure. This adaptation allows organizations of varying sizes and cybersecurity program maturities to benefit from the framework's guidance, regardless of sector or type. It is important to note that this is not a compliance requirement. These industries do not need to leverage the CSF now. Instead, it is an acknowledgment that the benefits of adopting the CSF are not industry-specific.

Furthermore, NIST CSF 2.0 consolidates a significant amount of guidance and tools aimed at helping organizations better use the CSF. This is especially true for the tiers and profile concepts defined within the framework. To facilitate the effective implementation of NIST CSF 2.0, NIST has created a suite of resources designed to provide organizations with tailored pathways into the framework. These resources include:

- A new searchable reference tool that simplifies browsing, searching, and exporting data from the CSF's core guidance.
- An informative reference catalog with mappings that cross-references the CSF's guidance to over 50 other cybersecurity documents, such as NIST 800-53.
- Community profiles that showcase how different industries and verticals adapt the framework's taxonomy to fit their specific use cases.
- Implementation examples and detailed guidance, including action-oriented steps to help organizations understand and achieve the desired outcomes of the subcategories.
- Quick start guides tailored for small businesses, enterprise risk managers, and organizations seeking to secure their supply chains.

How Organizations Currently Use NIST CSF

A wide variety of organizations with different needs already use the NIST CSF in different ways. Most commonly, I've seen use organizations use the NIST CSF to:

- **Organize and Inform a Security Control Framework:** Many organizations use the NIST CSF Core as a foundation for developing and structuring their security control framework. The framework's core functions provide a logical and comprehensive structure for organizing security controls and ensuring all aspects of cybersecurity are addressed. The NIST CSF is often used as the base framework. Then, it is mapped to other control frameworks like ISO 27002 or NIST 800-53 to provide more granular control descriptions.
- **Measure and Report on Cybersecurity Posture or Maturity:** The NIST CSF enables organizations to measure and report on their cybersecurity posture effectively. This is sometimes referred to as a NIST CSF Maturity Assessment, although NIST took great pains in NIST CSF 1.0 to state that "Tiers do not represent maturity levels." By aligning controls and processes with the framework's subcategories and outcomes, organizations can assess their implementation level and maturity across cybersecurity domains, generating reports and dashboards.
- **Provide a Consistent Framework for Executive Reporting on Cybersecurity:** The NIST CSF provides a common language and structure for communicating cybersecurity risks and initiatives to executives and board members. Using the framework's terminology and concepts, CISOs can present a consistent view of the organization's cybersecurity performance for informed decision-making.

Regardless of the use case, NIST CSF 2.0 offers the same easy-to-understand taxonomy to translate technical details into business outcomes easily.

Impact of NIST CSF 2.0 Changes on These Uses

The changes in NIST CSF 2.0, while welcome, aren't expected to result in too many changes to how organizations and CISOs use NIST CSF. However, CISOs should still proactively address these changes as follows:

Security Control Framework Organization:
With the addition of the new "Govern" function in NIST CSF 2.0, organizations will need to review and potentially restructure their security control framework to incorporate governance aspects within the framework seamlessly. For organizations that have mapped their security controls to the NIST CSF and aligned it with other frameworks (e.g., ISO 27001, COBIT), the updates in version 2.0 will necessitate a review and update of these mappings.

Cybersecurity Posture / Maturity Measurement and Reporting:
The updates in NIST CSF 2.0 may impact how organizations measure and report on their cybersecurity posture. At a minimum, CISOs will need to label existing assessments against the NIST CSF 1.0 and make plans to reassess their current posture against the revised framework and potentially recalibrate their metrics and reporting mechanisms to reflect the changes accurately.

Executive and Board Communication:
The addition of the Govern function and the emphasis on cybersecurity as an enterprise risk won't require a drastic reshaping of how CISOs communicate with executives and board members. However, it does provide an opportunity for CISOs to revisit and formalize their governance structures up to the board, by documenting these elements in more detail if missing.

Can CISOs Leverage NIST CSF 2.0 More Effectively Now?

As someone who has used NIST CSF in the past as a practitioner, NIST is a powerful framework. However, it is difficult to implement “as-is” in a mature organization beyond a control catalog or to implement a reporting framework overlay on top of existing processes. Mature organizations typically have processes for defining the current state, target state, and tracking issues and risks already with an associated risk management terminology widely removed from the NIST CSF approach. Meanwhile, smaller organizations simply don’t have the manpower to do it themselves.

The focus in NIST CSF 2.0 to formalize a separate Govern function within the CORE functions is indicative that NIST realizes that these aspects of the framework aren’t being used. It is striving for more accountability on organizations to define their own organizational profiles and define a target state appropriate to their own industry and risks, against the current state.

NIST CSF 2.0 attempts to further simplify this with the raft of tools and examples it now includes concerning organizational profiles and community profile templates and examples. Sadly, managing this all in spreadsheets is unfortunately still too unwieldy to even consider for most organizations and CISOs.

As a result, most organizations have and still will heavily leverage external consultancies to assess their “NIST CSF Maturity” and develop roadmaps to drive improvement. This external assessment is usually a measurement primarily against peers.This is opposed to the approach NIST recommends, which is using the definition of the current organizational profile compared to the target organizational profile to identify gaps for remediation. This approach will ultimately be fine for most CISOs and organizations, who want to show progress using a consistent framework.

CISOs should take note of all deviations, and leverage existing risk management processes to assess the risks and implications of those deviations and high-level estimates of the cost and timeframe to address.

The true test for NIST CSF 2.0 lies in whether organizations will fully embrace it as a framework for implementing their cybersecurity controls or continue to use it as a reference point to articulate their program. While the updates, consolidated guidance, and additional resources are certainly valuable additions, their impact will depend on the willingness of CISOs and organizations to move beyond using the NIST CSF solely as a control catalog or reporting overlay.

The success of the NIST CSF 2.0 therefore hinges on the simplicity of its implementation and the additional time and resources necessary to integrate it into existing governance structures, risk management processes and tools, and overall cybersecurity strategies.

CISOs should take note of all deviations, and leverage existing risk management processes to assess the risks and implications of those deviations and high-level estimates of the cost and timeframe to address.

The true test for NIST CSF 2.0 lies in whether organizations will fully embrace it as a framework for implementing their cybersecurity controls or continue to use it as a reference point to articulate their program. While the updates, consolidated guidance, and additional resources are certainly valuable additions, their impact will depend on the willingness of CISOs and organizations to move beyond using the NIST CSF solely as a control catalog or reporting overlay.

The success of the NIST CSF 2.0 therefore hinges on the simplicity of its implementation and the additional time and resources necessary to integrate it into existing governance structures, risk management processes and tools, and overall cybersecurity strategies.

NOTES

***Note 1:** While some of these may be dependent on how harmonized their internal control framework is to NIST CSF and other widely adopted cybersecurity frameworks and standards, such as ISO 27001 and COBIT, it is infinitely more achievable than starting from scratch. NIST also provides the NIST CSF reference catalog to support this mapping, but it is important that CISOs further this mapping to their own internal policy, any regulatory or legislative needs, and external contractual security requirements.

***Note 2:** It is important to note that NIST CSF only suggests organizations use tiers to measure the current state and define the future state. NIST CSF 2.0 provides little guidance beyond a high-level description of the tiers to help organizations assign a tier. The truth is that it doesn't matter, as long as it is repeatable and can be based on the evidence gathered. Whether this leverages the NIST CSF 2.0 Tiers or their own assessment methodology is not important. It is, however, important that CISOs define and agree on the target tier (or equivalent) with their business leaders and the priority and timeframe for any gaps to be remediated within. This will allow them to prioritize gaps based on identified gaps, and organizational priorities.

About the Author

Claude Mandy is the Chief Evangelist for Data Security at Symmetry Systems, where he focuses on innovation and industry engagement while leading efforts to evolve how modern data security is viewed and used in the industry. Prior to Symmetry, he spent 3 years at Gartner as a senior director. He brings firsthand experience in building information security, risk management, and privacy advisory programs with global scope.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, and compliance management. More than 40% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fifth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: AuditBoard.com.