SEDARA™

5 Things to Know About NIST CSF 2.0

Information in this guide published February, 2023

The National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) is undergoing a major update.

This booklet will cover the top five things to know about the upcoming NIST CSF 2.0.

But first,
What is the NIST CSF?

The **NIST CSF** was first created in 2014 in response to an Executive Order mandating increased cybersecurity of the nation's critical infrastructure. Since then, the framework has been voluntarily adopted—or mandated for adoption by such regulations as New York State Education Law 2-d—by organizations of all sizes and in all industries.

The framework is organized according to **five Functions** that define the high-level practices of any cybersecurity program: **Identify, Protect, Detect, Respond, and Recover**.

NIST has shared several proposed changes to the CSF in an attempt to make it more useful and aligned with the latest best practices. While the core structure of the NIST CSF is expected to stay the same, several of the proposed changes are promising enhancements to the framework.

1 A New Governance Function

The NIST CSF is most commonly associated with its five color-coded Functions:

Identify | Protect | Detect | Respond | Recover

For 2.0, NIST is planning to include a sixth Function:

\+ Govern

NIST proposes including the **Govern** function to emphasize the importance of “cybersecurity risk management governance outcomes.”

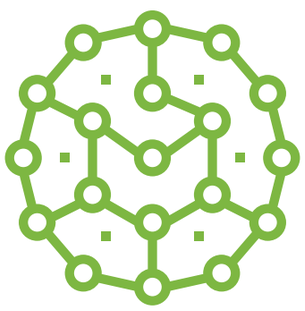
The intent for this change is to highlight the importance for any cybersecurity program to develop appropriate policies and procedures, assess and prioritize risk, and clearly define roles and responsibilities

2 Expanding Supply Chain Risk Management

In 2018 NIST added the Supply Chain Risk Management (ID.SC) category to the CSF. NIST plans to offer even more attention to Cybersecurity Supply Chain Risk Management (C-SCRM) in CSF 2.0.

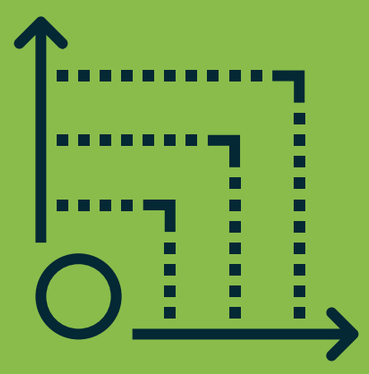
NIST hasn't provided specifics for how 2.0 would expand coverage of supply chain risk management, but they outline several scenarios, such as creating:

- An entirely new Function devoted to supply chains
- Spreading more C-SCRM controls across the entire CSF
- or expanding the ID.SC category



Regardless, as technology services are increasingly complex, outsourced, and interdependent, there is a greater need for organizations to assess and manage their supply chain risks.

3 New Implementation Guidance for Subcategories



The NIST CSF is meant to be **high-level** and **scalable** to any organization. While this provides the benefit of the CSF being a highly adaptable framework, it can also lead to the frustration of the CSF feeling too vague or that the intent behind the subcategories is difficult to discern.

For 2.0, NIST is planning to offer a small number of **“concise, action-oriented processes”** that could help an organization know how to achieve the intended outcome of the subcategory.

These “notional implementation examples” are already present in some of the newest NIST frameworks, such as the Secure Software Development Framework. These guideances offer promising opportunities to improve outcomes for users of the CSF.

4 Providing Measurement Examples for the NIST CSF

For many users of the NIST CSF, one of the most frustrating experiences is tracking “compliance” with the CSF and measuring the evolution of one’s cybersecurity program over time against the CSF.

Because there is no single approach to measure and assess the CSF, NIST will not put forward a single approach to assessment in the CSF 2.0.

However NIST does say 2.0 will include examples of how other organizations have used risk management frameworks and maturity models to assess their CSF capabilities.

Additionally, **NIST encourages community input** on draft SP 800-55r2, the Performance Measurement Guide for Information Security (https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft).

Until –or if–NIST publishes a formal CSF assessment model it’s up to each organization to use a measurement schema that works best for them.

5 More Informative References

The NIST CSF is one of many popular cybersecurity frameworks, such as NIST 800-53, ISO/ISEC 27001, CIS Controls, and COBIT 2019. The CSF has always provided an informative references section that maps each CSF subcategory to other popular frameworks.

For 2.0, NIST promises to:

- Update the informative references section to align with the latest mappings along with providing the most up-to-date and searchable mappings in their Online Informative References

- The OLIR is a recent NIST resource that already provides several exportable and sortable spreadsheet mappings between the CSF and other popular frameworks. NIST promises the expansion and continual update of OLIR with the release of the CSF 2.0.

Contact us

Get in touch with a member of our team

Call Us
+1 (844) 473-3272

Sedara Office
640 Ellicott Street, Ste 102 Buffalo, NY 14203

Connect With Us

www.sedarasecurity.com

Facebook
LinkedIn
Twitter
Visit Our Blog
Subscribe to Our Newsletter

Join Our Team
View Employment Opportunities