protiviti®
Global Business Consulting

NIST Releases Version 2.0 of Its Cybersecurity Framework (CSF): What This Means for Your Organisation

28 February
2024

Background

On 26 February 26 2024, The National Institute of Standards and Technology (NIST) released version 2.0 of its updated and widely used Cybersecurity Framework (CSF). This latest edition of the CSF is designed for all audiences, industry sectors and organisation types, regardless of their degree of cybersecurity sophistication.

With version 2.0 of the CSF, NIST has updated the framework to expand its core guidance and has developed resources that will help users get the most out of the new iteration of the CSF. NIST CSF 2.0 has an expanded scope to help organisations of all sizes and sectors to manage and reduce their cybersecurity risks. It contains new features to highlight the importance of governance and supply chains, encompassing how organisations make and carry out informed decisions on cybersecurity strategy.

> "The CSF has been a vital tool for many organisations, helping them anticipate and deal with cybersecurity threats," said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. "CSF 2.0, which builds on previous versions, is not just about one document. It is about a suite of resources that can be customised and used individually or in combination over time as an organisation's cybersecurity needs change and its capabilities evolve."

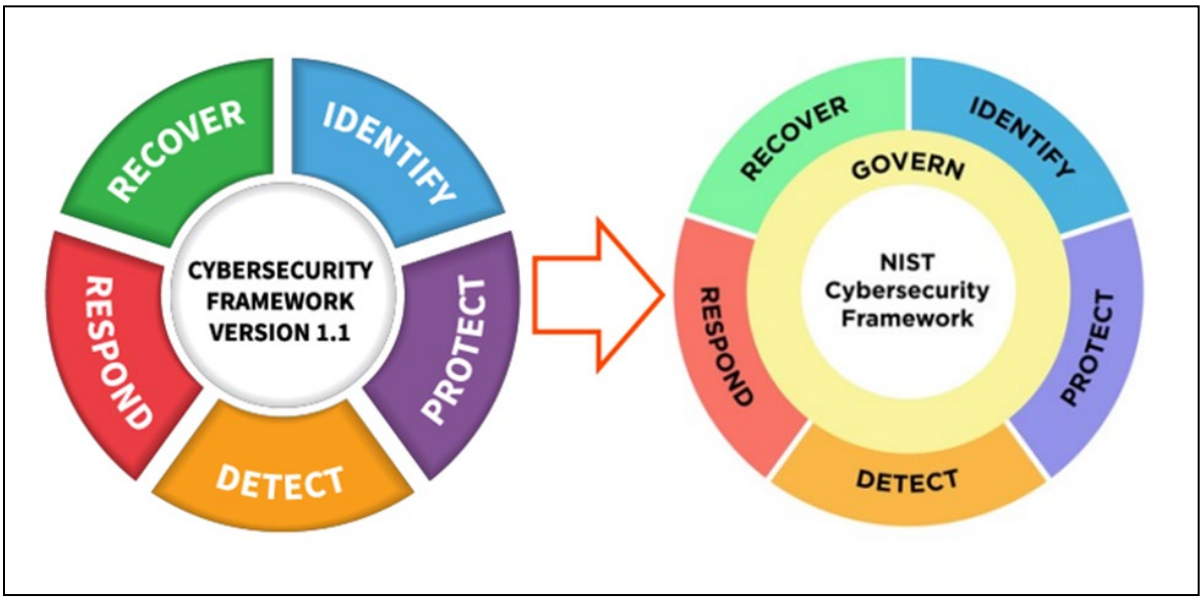
How NIST CSF 2.0 was developed

NIST released a draft version of NIST CSF 2.0 on 8 August 2023, and sought comments from key stakeholders, multiple industries and organisations. NIST also held multiple workshops starting in August 2022 to develop a collaborative process to update the CSF with the intention of making version 2.0 easier to implement across multiple industries and businesses of all sizes. Comments were accepted until November 2023 and influenced the final iteration of NIST CSF 2.0.

What's new with NIST CSF 2.0

NIST CSF 2.0 builds upon previous versions of the CSF and introduces some new concepts and elements that help to make the framework more comprehensive. The previous iteration of the CSF had five core functions: Identify, Protect, Detect, Respond and Recover. NIST CSF 2.0 adds a new core function, Govern, which informs and supports the other five functions.

The CSF Core is the basis of the framework, which is a taxonomy of high-level cybersecurity outcomes that can help any organisation manage its cybersecurity risks. NIST evaluated the functions, categories and subcategories that made up the NIST CSF 1.1 framework and as part of the build out of NIST CSF 2.0, added new categories, combined similar subcategories together and retired other subcategories. From that, NIST CSF 2.0 has reduced its categories from 23 to 22 and subcategories from 108 to 106.



NIST CSF 2.0 introduces the Govern function as a foundational element of the framework.

Source: National Institute of Standards and Technology: www.nist.gov/cyberframework

Some of the most notable changes include:

- **Govern function:** The Govern function provides guidance to inform what an organisation may do to achieve and prioritise the initiatives of the other five functions in the context of its mission and stakeholder expectations. The Govern function addresses organisational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities and authorities; policy; and the oversight of cybersecurity strategy, which is the foundation on which the new NIST CSF 2.0 framework is built.

- **Cybersecurity supply chain risk management:** Within the new Govern function, there is an emphasis on cybersecurity supply chain risk management (reflecting NIST's latest guidance) and secure software development. The new practices NIST suggests to organisations include:
    - Create a Cybersecurity Supply Chain Risk Management (C-SCRM) strategy, objectives, policies and processes.
    - Identify the organisation's technology suppliers and determine how critical each one is to the organisation.
    - Establish C-SCRM roles and requirements and communicate them within and outside the organisation.
- **Updated reference tool:** The new and comprehensive online NIST CSF 2.0 Reference Tool allows users to easily navigate NIST CSF 2.0 using keywords and phrases to find subcategory and implementation example references quickly. The tool also educates users on organisational profiles and circumstances by highlighting elements such as mission statement, stakeholder expectations, legal requirements, regulatory accountability and contractual obligations. Ultimately, the updated reference tool is a valuable resource for understanding and implementing the cybersecurity best practices as outlined in NIST CSF 2.0.
- **Cybersecurity risk reduction guidance:** Included in the framework are Quick Start Guides, which have numerous examples as well as detailed guidance that is applicable to numerous entities, such as industry, government agencies, educational and healthcare organisations, and businesses of any size (including smaller businesses with emerging/less mature cybersecurity programs). That guidance has a focus on effectively reducing cybersecurity risk and developing best practices.
- **Expanded profile guidance:** Organisational and Community profiles have been significantly revised and expanded to provide guidance to understand, tailor, assess and prioritise cybersecurity outcomes based on an organisation's mission objectives, stakeholder expectations, threat landscape and requirements. These profiles can be used to assess progress toward targeted outcomes and to communicate pertinent information to stakeholders.
- **Expanded CSF tiers:** CSF tiers can be applied to organisational profiles to characterise the rigor of an organisation's cybersecurity risk governance and management outcomes. Within NIST CSF 2.0, there are two defined CSF tiers:

Cybersecurity Risk Governance, which corresponds to the Govern function, and Cybersecurity Risk Management, which corresponds to the other five CSF functions. Each of these CSF tiers has its own unique guidance to help in achieving organisational goals.

As mentioned earlier, NIST CSF 2.0 builds upon the previous iterations of NIST CSF 1.0 and NIST CSF 1.1, which already were quite comprehensive. That said, there are significant updates throughout NIST CSF 2.0, meaning that care must be taken to ensure that benefits offered are fully realised. Notable changes include a broadened scope to encompass organisations beyond just those operating in critical sectors. NIST CSF 2.0 also emphasises integrating cybersecurity risk management into the organisation's overall risk management process.

What should I do now?

Now that NIST CSF 2.0 has been finalised, organisations will need to take some preparatory steps before implementing components of the new framework. The following steps should help ease adoption of the primary framework elements and give organisations a head start on deriving the potential benefits:

1. Implement a cross-functional cyber task force to oversee the transition to NIST CSF 2.0 to allow for collaboration and communication between the cybersecurity organisation and the rest of the business. The cyber task force should facilitate conversations with their organisation’s board of directors and executives to ensure they understand the impact to the cybersecurity program and overall strategy.

2. Review the NIST CSF 2.0 Quick Start Guides to assist the organisation in implementing key parts of the new framework.

3. Review current policies, processes, procedures and controls against the NIST 2.0 framework elements, especially focusing on the Govern function and its implications for your organisation, and ensure relevant documentation and controls narratives are updated as needed.

4. Review the new implementation tiering guidance around Cybersecurity Risk Governance and Cybersecurity Risk Management, as each of these areas has specific tier rating requirements and objectives.

5. Perform an initial gap analysis against NIST CSF 2.0 and develop an action plan to address deficiencies found.

6. Review and identify appropriate CSF implementation tiers that will help achieve a desired risk posture across critical assets and resources.

How Protiviti can help

Protiviti helps our clients take a holistic business and technology approach of their risk posture to evaluate current cybersecurity capabilities. Protiviti combines the new NIST CSF 2.0 framework with our depth of expertise to understand your current cybersecurity capabilities and business drivers to create a tailored cyber program roadmap to help drive your organisation toward a defined target security operating model.

Protiviti is assisting stakeholders across the three lines of defence, consisting of revising existing frameworks, risk management programs, control design and audit techniques, to align with the new standard. By taking a look at a client's unique risk landscape and cybersecurity maturity, Protiviti advises the board of directors and executives in understanding and assessing business risks for smart cybersecurity strategy investments to serve their customers and grow their business.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

Named to the 2023 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®