

Sean Shreve
February 09, 2026
CYSE 200T
Professor Duvall

I need a one-page synopsis of the differences between the NIST Cybersecurity Framework 1.1 and 2.0

Below is a **one-page, structured synopsis** summarizing the key differences between the *NIST Cybersecurity Framework (CSF) 1.1* and *CSF 2.0*. It focuses on changes in structure, scope, governance, content, and implementation guidance. ([Security Compass](#))

Synopsis: Differences Between NIST CSF 1.1 and CSF 2.0

1. Framework Purpose and Scope

CSF 1.1 (2018)

- Originally framed as “*Framework for Improving Critical Infrastructure Cybersecurity*.”
- Primarily focused on critical infrastructure sectors (energy, finance, healthcare). ([Wikipedia](#))

CSF 2.0 (2024)

- Renamed simply “*Cybersecurity Framework*” to reflect *broader applicability*.
- Explicitly designed for organizations of **all sizes and sectors** (private, public, SMEs, government). ([Scrut](#))

Impact:

CSF 2.0 removes implied sector limitations, making the framework more universally adoptable.

Commented [SS1]: Over the years, the advancement of technology has increased the volume of the attack surface. By broadening the scope, NIST acknowledges that cybersecurity management is on a universal need rather than sector specific.

2. Core Structure: Functions, Categories, and Subcategories

CSF 1.1

- Built around **5 core functions**: *Identify, Protect, Detect, Respond, Recover*.
- Featured 23 categories and 108 subcategories. ([Lepide](#))

CSF 2.0

- Introduces a **6th core function** — ***Govern***, positioned to influence all other functions: *Govern, Identify, Protect, Detect, Respond, Recover*.
- Expanded structure with approximately 22 categories and 106 subcategories, reflecting reorganized and consolidated outcomes. ([Lepide](#))

Fundamental change:

The *Govern* function centralizes governance, aligning cybersecurity risk management with enterprise priorities rather than leaving governance elements distributed across other functions. ([Security Compass](#))

Commented [SS2]: Many organizations treated cybersecurity as a problem control method rather than a risk issue that affects the whole business/organization. The new *Govern* function supports integration of more broad oversight of cybersecurity, ranging all the way up to the heads of board. This overall strengthens cybersecurity and business objects and makes them more synergistic.

3. Governance and Risk Management Emphasis

CSF 1.1

- Governance elements existed but were embedded within other functions, making *leadership accountability and strategic oversight less explicit*. ([NIST](#))

CSF 2.0

- *Govern* function elevates governance into a standalone core function.
- Includes directives for organizational context, risk tolerance, policy establishment, oversight, and accountability at the executive level. ([CRF](#))

Impact:

Cybersecurity is treated as **enterprise risk**, not just a technical or operational concern — a shift that aligns the framework with broader risk management and board-level responsibilities. ([compassmsp.com](#))

Commented [SS3]: In regards to the enterprise risk management process, cybersecurity integration was not explicitly defined. Version 2.0 corrects this issue by linking organizational outcomes to cybersecurity outcomes. There should be no misunderstanding what cybersecurity provides to an organization's operation with this upgrade.

4. Supply Chain and Third-Party Risk Management

CSF 1.1

- Included supply chain risk considerations scattered across functions. ([NIST](#))

CSF 2.0E

- Expands and consolidates *supply chain risk management (SCRM)* guidance, including explicit third-party oversight categories within the *Govern* and *Protect* sections.
- Addresses contractual expectations and continuous monitoring of vendor risk. ([CRF](#))

Outcome:

Provides **enhanced SCRM focus**, reflecting the rising frequency and impact of supply chain attacks.

Commented [SS4]: CSF 2.0 takes supply-chain security much more seriously than its predecessor/previous version. Strengthening the supply chain risk management (SCRM) guidance extends the boundaries of what cybersecurity can provide to any link of a company's profit capability.

5. Alignment with Contemporary Threats and Standards

CSF 1.1

- Core guidance primarily reflected threat contexts and enterprise practices up to the late 2010s. ([Wikipedia](#))

CSF 2.0

- **Updated language and structure** to address modern threats and practices, including:
 - Cloud security risk integration
 - Support for Zero Trust concepts
 - Ransomware and AI-related risk awareness
- Stronger alignment and mapping with **NIST SP 800-53** and other standards, aiding comprehensive control implementation. ([Scrub](#))

Impact:

Improves interoperability with regulatory compliance frameworks and supports contemporary security models.

Commented [SS5]: The outlook of threat risks has grown significantly, increasing in both size and severity. It has evolved alongside technological advancements such as cloud-based storage, ransomware growth, and artificial intelligence schemes to name a few. A much-needed update to supported frameworks was a necessity.

6. Implementation Guidance and Usability Enhancements

CSF 1.1

- Provided broad outcomes and suggested practices with limited concrete examples. ([Wikipedia](#))

CSF 2.0

- Includes **expanded implementation examples**, clearer outcome-oriented guidance, and updated organizational profiles:
 - *Current Profile vs Target Profile* constructs to support maturity assessment.
 - Better tools and cyber risk outcome descriptions to assist diverse user needs. (help.vanta.com)

Outcome:

Facilitates more consistent implementation and assessment across teams and industries.

Commented [SS6]: CSF 2.0 improves usability by offering clearer examples and more structured guidance. This reduces confusion by ambiguous interpretations and supports more consistent implementation for organizations. To have a clear instruction for employees and executives to read and follow is imperative for proper business success and safety.

7. Transition and Adoption Considerations

- CSF 2.0 does **not remove content** from CSF 1.1; rather, it reorganizes, clarifies, and expands it for broader adoption and modern risk contexts. ([NIST](#))
- Organizations moving to CSF 2.0 should:
 - Align governance structures with the new *Govern* function.
 - Reassess supply chain risk processes.
 - Update risk profiles and implementation plans to match new core structure and tools.

Commented [SS7]: The continuity of version 1.1 is preserved by not removing content as version 2.0. This was necessary to provide a smoother transition for modern cybersecurity risk management. This methodology also prevents from organizations who were deeply invested in CSF 1.1 to become discouraged by the newer version changes.

References

- CompassMSP. (2024). *Meet the govern function of the NIST cybersecurity framework*.
<https://compassmsp.com/resources/meet-the-govern-function-of-the-nist-cybersecurity-framework>
- CRF Secure. (2024). *Understanding the 2024 updates to the NIST cybersecurity framework*.
<https://crfsecure.org/understanding-the-2024-updates-to-the-nist-cybersecurity-framework>
- Help Vanta. (2024). *Understanding the differences between NIST CSF 1.1 and 2.0*.
<https://help.vanta.com/en/articles/11345799-understanding-the-differences-between-nist-csf-1-1-and-2-0>
- Lepide. (2024). *NIST CSF 1.1 vs 2.0: What's new?* <https://www.lepide.com/blog/nist-csf-1-1-vs-2-0/>
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. U.S. Department of Commerce.
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
- National Institute of Standards and Technology. (2024). *Cybersecurity framework (CSF) 2.0*. U.S. Department of Commerce.
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- National Institute of Standards and Technology. (2024). *Cybersecurity framework frequently asked questions*. <https://www.nist.gov/cyberframework/faqs>
- Scrut Automation. (2024). *Update: NIST CSF 2.0 vs 1.1—What's new and why it matters*.
<https://www.scrut.io/post/update-nist-csf-2-0-vs-1-1-whats-new-and-why-it-matters-for-your-cybersecurity-program>

Security Compass. (2024). *NIST CSF 1.1 vs 2.0: Key differences explained*.

<https://www.securitycompass.com/blog/nist-csf-1-1-vs-2-differences/>

Wikipedia contributors. (2024). *NIST cybersecurity framework*. Wikipedia.

https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework