Seth Sarauw
CYSE 200T
September 17, 2025
Professor Duvall

AI Assignment: Understanding the Differences between the NIST Cybersecurity Framework 1.1 and 2.0

Synopsis: NIST Cybersecurity Framework 1.1 vs. 2.0

The NIST Cybersecurity Framework (CSF) provides organizations with a risk-based approach to managing cybersecurity. While CSF 1.1 (2018) established the foundation, CSF 2.0 (2024) introduces significant updates to reflect evolving threats, technologies, and stakeholder needs.

Commented [1]: Cyber threats continue to advance every day, so it's crucial for organizations to advance with those threats. Some of the updates are focused on attacks we didn't think were possible back in 2018, as well as how we govern our organizations. Now we have to worry about AI and supply chain attacks.

1. Scope and Audience

- **CSF 1.1: Primarily targeted critical infrastructure sectors (e.g., energy, finance, transportation).**
- **CSF 2.0: Expanded for all organizations (public, private, small, large, across industries) to emphasize universality.**

Commented [2]: In CSF 1.1, it was targeted towards infrastructures, such as healthcare and finance. With the new CSF 2.0, it is now targeted towards every organization. Now, because it's towards every organization, every organization can have their proper security.

2. Structure and Functions

- **CSF 1.1: Five Core Functions — Identify, Protect, Detect, Respond, Recover.**
- **CSF 2.0: Introduces a sixth Function: Govern, focused on governance, roles, responsibilities, and risk management strategy.**

Commented [3]: The original CSF 1.1 was primarily intended for operational security measures. The new CSF 2.0 is now for all objectives and requirements, no matter the organization or enterprise. CSF 2.0 added a sixth function as well, being govern. Govern is the overview to make sure that there is improvement to security continuously happening.

3. Guidance and Implementation

Commented [4]: The guidance in CSF 2.0 is much clearer and easier to understand. It clearly states the risks and how it will work. CSF 2.0 does something that CSF 1.1 struggled to do, which was to make a simple way for security teams to take on this new security and implement it.

- **CSF 1.1: Provided general guidance, often requiring customization for different sectors.**

- **CSF 2.0: Includes Implementation Examples, Quick Start Guides, and Profiles to help organizations of varying sizes adopt the framework more directly.**

4. Risk and Supply Chain Considerations

- **CSF 1.1: Mentioned supply chain risk management but limited detail.**

- **CSF 2.0: Strong emphasis on cyber supply chain risk management (C-SCRM), incorporating third-party dependencies and vendor risk.**

Commented [5]: With the rapid importance of needing a secure vendor, CSF 2.0 addresses this heavily. CSF 1.1, on the other hand, vaguely mentioned its importance. With the rapid increase in supply chain attacks, this is an important thing to know about and have covered.

5. Integration with Other Standards

- **CSF 1.1: Mapped loosely to other frameworks (ISO, COBIT, etc.).**

- **CSF 2.0: Provides updated crosswalks and alignment with global standards and regulatory requirements, supporting harmonization.**

Commented [6]: CSF 1.1 struggled to connect with other frameworks. On the other hand, CSF 2.0 aligns closely with frameworks like ISO 27001 and PCI DSS. With CSF 2.0 alignment, it makes it easier to implement and comply with.

6. Usability Enhancements

- **CSF 1.1: Static PDF-based framework.**

- **CSF 2.0: Launches with an online resource center and interactive tools, making it easier to navigate, tailor, and update practices.**

Summary

- **CSF 1.1 laid the foundation with five core Functions and a focus on critical infrastructure.**

- **CSF 2.0 modernizes and broadens the framework: it adds Govern as a sixth Function, strengthens supply chain risk, provides practical tools for diverse**

organizations, and enhances integration with global standards.

In essence, CSF 2.0 shifts from a sector-specific framework to a truly universal tool for organizational cybersecurity governance and resilience.