Alissia Metcalfe

Professor

CYSE 200T #

13 February 2026

AI Assignment

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

Overview: NIST CSF 1.1 vs CSF 2.0

The NIST Cybersecurity Framework (CSF) is a voluntary, risk-based set of guidelines designed to help organizations manage and reduce cybersecurity risk. Version 1.1 was published in 2018, primarily for critical infrastructure sectors; CSF 2.0, released in 2024, updates that approach to reflect evolving threats, governance needs, and broader applicability.

1. Framework Purpose & Scope
   CSF 1.1
   - Retitled as simply Cybersecurity Framework.
   - Broadened scope-explicitly intended for all organizations, regardless of industry or size (including small/medium enterprises).
2. Core Structure & Functions
   CSF 1.1
   - Five core functions:
     Identify, Protect, Detect, Respond, Recover.
     These functions provide a lifecycle view of risk management.

   CSF 2.0
   - Six core functions with the addition of Govern, elevating governance and strategic alignment:
   - Govern focuses on leadership oversight, risk strategy, roles, policies, and accountability.
   - Reorganization within existing functions and updated categories/subcategories improve clarity and current relevance.

   I believe that it was necessary to add emphasis on the leadership oversight because it's important that policies are being properly implemented and adhered to throughout the company. Forming policies that are relevant to

potential threats for the company. Focusing on areas where human error play big factors in breaches.

3. Governance & Organizational Context
   CSF 1.1
   - Governance topics (e.g., risk management, roles) were implicitly included mainly within the identify function.

   CSF 2.0
   - Elevates governance to a standalone function, emphasizing how cybersecurity integrates with enterprise risk management (ERM), executive leadership, and broad involvement.
   - Clarifies organizational context- including strategy policies, and oversight- as a foundational element.

     The updated version focuses on the organizational context as well as risk management. Highlighted functions in policies and oversight, it is important that they added emphases on these because policies that are not governed properly tend to fail.

4. Risk Management & Supply Chain Focus
   CSF 1.1
   - Supply chain risk and third-part issues were acknowledged but lacked comprehensive guidance.

   CSF 2.0
   - Stringer emphasis on supply chain cybersecurity risk management (C-SCRM).
   - Provides more detailed guidance on elevating and mitigating risks throughout the supplier ecosystem.

     2.0 offers a seven-step approach to identify, assess and mitigate cyber threats across the supply chain cycle. Which ensures resilience against threats like tampering and counterfeit both important to the supply chain network.

5. Alignment & Implementation Guidance
   CSF 1.1
   - Focused on the core taxonomy and high-level outcomes with limited implementation examples.

   CSF 2.0
   - Expands implementation guidance, including examples and practical advice.

- Improved linkages to other frameworks (e.g., NIST SP 800-53, privacy and risk frameworks) to support broader compliance and integrations.

  The updated version focuses on creating current/ target profiles and executing action plans to mature security posture. As well as the systems that need to be covered under the prioritize and scoop. It is beneficial for organizations to know what systems are high targets, how they can properly assess the size of threat, and properly secure the systems.

6. Profiles, Tiers & Metrics
   CSF 1.1
   - Including Profiles (Current/Target) and Implementation Tiers to gauge maturity.

   CSF 2.0
   - Retains and enhances Profiles and Tiers for better maturity assessment.
   - Places increased emphasis on continuous improvement, measurable outcomes, and quantitative/qualitative performance indicators.
     It is important that maturity assessments are as accurate as possible so that companies are given the proper development strategies to move up in maturity. As well as ensuring the objectives of that business/ organization is being met as far as cybersecurity.
7. Terminology & Reorganization
   CSF 2.0 reorganizes categories and subcategories to reduce overlap and better reflect contemporary cybersecurity realities:
   - Some subcategories were relocated (e.g., from Identify to Govern).
   - New categories (e.g., Platform Security, Tech Infrastructure Resilience) were added.
   - Overall taxonomy refined for clarity and relevance.

     2.0 adds focus on securing the physical and virtual infrastructure by generating logs and preventing unauthorized software execution. Which is important because it enables organizations to reduce risks through proactive and risk-based strategies.