Devlin Jett
CYSE 200T
Professor Duvall
February 5, 2025

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

The NIST Cybersecurity Framework (CSF) has undergone significant updates from version 1.1 to 2.0, reflecting the evolving landscape of cybersecurity threats and organizational needs. Below is a concise overview of the key differences between these versions:

1. Introduction of the 'Govern' Function: Version 2.0 introduces a new core function, 'Govern,' bringing the total to six:

Govern (GV): Focuses on establishing and overseeing a comprehensive cybersecurity strategy that aligns with organizational objectives and risk tolerance. This function emphasizes the importance of governance and supply chain management, ensuring that cybersecurity measures are proactive and integrated into the organization's overall mission.

lepide.com

2. Expanded Scope and Applicability: While version 1.1 primarily targeted U.S. critical infrastructure sectors, version 2.0 broadens its scope to encompass organizations of all sizes and industries globally. This expansion acknowledges the universal nature of cybersecurity threats and the need for a standardized approach across various sectors.

blog.charlesit.com

3. Enhanced Emphasis on Supply Chain Risk Management: Version 2.0 places a stronger emphasis on supply chain risk management, recognizing the critical role that third-party vendors and partners play in an organization's cybersecurity posture. This includes a dedicated category within the 'Govern' function to address supply chain risks.

cdp.cooley.com

Commented [JD1]: This update was needed to emphasize the strategic role of leadership in cybersecurity, ensuring that governance structures align cybersecurity efforts with business goals and provide accountability at the highest levels.

Commented [JD2]: Expanding the framework's applicability allows all organizations regardless of size or sector—to adopt the CSF, addressing the growing need for a universal approach to cybersecurity risk management

Commented [JD3]: With increasing supply chain attacks, this update was essential to guide organizations in assessing and mitigating risks within their supply chains, which have become a critical vulnerability point in cybersecurity.

4. Improved Integration with Other Frameworks: The updated framework provides guidance on integrating with various cybersecurity frameworks and standards, facilitating a more cohesive and comprehensive approach to cybersecurity risk management.

diligent.com

5. Enhanced Guidance and Resources: Version 2.0 offers expanded guidance, case studies, reference materials, and tools to assist organizations in implementing the framework effectively. This includes practical and actionable suggestions to help organizations immediately improve their cybersecurity posture.

nist.gov

6. Emphasis on Continuous Improvement: The latest version underscores the importance of continuous improvement in cybersecurity practices, encouraging organizations to adapt to evolving threats and enhance their security measures over time.

diligent.com

In summary, NIST CSF 2.0 builds upon the foundation established in version 1.1 by introducing the 'Govern' function, expanding its applicability, enhancing supply chain risk management, improving integration with other frameworks, providing more comprehensive guidance, and emphasizing continuous improvement. These updates aim to provide organizations with a more robust and adaptable framework to manage and mitigate cybersecurity risks effectively.

Commented [JD4]: This update was necessary to help organizations streamline their cybersecurity efforts, avoid duplication of work, and ensure that their cybersecurity practices align across different frameworks.

Commented [JD5]: This update aimed to make the framework more accessible by including detailed examples, case studies, and clearer explanations, helping organizations better understand how to apply the framework in real-world scenarios.

Commented [JD6]: This change reflects the need for organizations to stay agile in the face of evolving cyber threats, ensuring that cybersecurity practices are not static but continuously adapted to new risks and vulnerabilities