

Amyah Robinson

CYSE 200T

Sept 21, 2025

Professor Duval

AI's View On The Differences Of NIST

BLUF: ChatGPT will write a one-page paper on the differences of NIST 1.1 and 2.0. We will analyze the reading and discuss our opinions on the differences.

ChatGPT: NIST Cybersecurity Framework 1.1 vs. 2.0

The National Institute of Standards and Technology (NIST) developed the Cybersecurity Framework (CSF) to provide organizations with a structured approach to managing and reducing cybersecurity risks. Version 1.1, released in 2018, built on the original framework by clarifying language, improving authentication and supply chain guidance, and reinforcing its use for critical infrastructure sectors. In 2024, NIST released CSF 2.0, marking the first major revision to the framework since its inception. This update reflects the evolving cybersecurity landscape and expands the framework's relevance beyond critical infrastructure.

One of the most significant differences between the two versions is the framework's scope. CSF 1.1 was tailored primarily for critical infrastructure, such as energy, finance, and healthcare, while CSF 2.0 broadens its application to all organizations, regardless of size, sector, or cybersecurity maturity. This makes the new version especially valuable for small and medium-sized businesses that previously struggled with implementation.

Another major change is the addition of a new core function. While CSF 1.1 was built on five core functions—Identify, Protect, Detect, Respond, and Recover—CSF 2.0 introduces a sixth function: Govern. This new function highlights the importance of governance, risk management, roles, accountability, and strategic alignment between cybersecurity and overall business objectives. By doing so, CSF 2.0 emphasizes that cybersecurity is not only a technical concern but also a central element of enterprise risk management.

Commented [ar1]: I would replace this with "industries, government agencies, and other organizations". My replacement puts more emphasis on what the organization really are. It would make the reader understand that this is something serious and important.

Commented [ar2]: The NIST framework changed because there needed to be an expansion for use of all organizations. How organization dealt with risk management needed to be changed.

Commented [ar3]: I would like to add that the Quick-Start Guides were made relevant to small and large organizations. The guide helps organizations improve their posture and management. These are brief documents on CFS topics.

Commented [ar4]: The addition of a new core is important because one thing may not work for the next organization. All organizations may experience different unique problems. The way organizations implement CSF will vary depending on the risk at hand.

Usability and guidance have also improved. In CSF 1.1, organizations were expected to adapt the framework largely on their own, which posed challenges for those with limited resources. CSF 2.0 addresses this by providing practical implementation examples, quick-start guides, and sector-specific profiles. These resources help organizations of varying sizes and maturity levels adopt the framework more effectively.

Commented [ar5]: This change was needed to help user better understand different outcomes and scenarios when it comes to different cyber threats and attacks.

In addition, CSF 2.0 significantly strengthens guidance on supply chain and third-party risk management. While CSF 1.1 mentioned these risks, it offered limited detail. Given the rise in breaches involving vendors and partners, CSF 2.0 expands coverage in this area to ensure organizations better manage dependencies across their ecosystems.

Commented [ar6]: I think could possible be about having more secure transaction with vendors in a business. The need for strong guidelines and instruction may decrease fraud or scams.

Finally, CSF 2.0 places a stronger emphasis on international adoption. Although CSF 1.1 was widely used in the United States and informally adopted abroad, CSF 2.0 was explicitly designed for global use. It aligns more closely with international standards, allowing organizations across borders to collaborate more effectively. The new version also integrates references to other NIST resources, such as the Privacy Framework and the Risk Management Framework, to support a more holistic cybersecurity program.

Commented [ar7]: The international use of CSF is important for privacy and protection. When sending and receive data internationally you want to make sure nothing is tampered in the process. Implementing CSF internationally builds strong security across the world.

In summary, while CSF 1.1 provided a strong baseline for protecting critical infrastructure, CSF 2.0 expands the framework's scope and relevance, adds governance as a core function, improves usability, strengthens supply chain risk management, and emphasizes global adoption. These updates ensure that the framework reflects the modern threat landscape and positions cybersecurity as a strategic component of organizational resilience.