The Role and Necessity

of the

NIST Cybersecurity Framework

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 300 – Introduction to Cybersecurity

November 23, 2025

Instructions:

The NIST CSF (URL: https://www.nist.gov/cyberframework) was developed to provide "a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses."

1. Do businesses and government agencies need to utilize such a framework to maintain a proper cybersecurity posture?
2. Can an organization mitigate cybersecurity risks without incorporating such a framework?
3. Cite resources and references that back up your assertions.

The Role and Necessity of the NIST Cybersecurity Framework

NIST developed the Cybersecurity Framework (CSF) to provide organizations with a structured, common, high-level language for discussing and managing cybersecurity risk (Solomon, 2021; NIST, 2024 & 2025). CSF 2.0 organizes cybersecurity activities into six core functions—Identify, Protect, Detect, Respond, Recover, and Govern—that help business leaders and IT teams to tie technical controls to business priorities, while sustaining a consistent risk-management posture (Balbix, 2025). Though not legally required for most businesses, the framework's flexibility and scalability make it a good fit for public and private organizations alike.

With so much stress on “secure infrastructures” nowadays, it is important to understand that the CSF is a voluntary tool to help construct a better, more adaptable, and tailored framework that any organization can use while not imposing any regulatory “cost” on your business (NIST, 2025). This level of flexibility is key for small and midsize organizations that may not have dedicated cybersecurity professionals but still require a formal approach to reducing risk (NIST, 2024).

Just because the NIST CSF is not mandatory for most organizations does not mean they cannot mitigate cybersecurity risks in other ways, whether through other formal frameworks or their own internal risk management programs. Other frameworks, such as ISO/IEC 27001 and the CIS Critical Security Controls, include similar processes that cover governance, implementation control, and ongoing monitoring (IT Governance USA, 2024). However, business leaders and IT teams operating and maintaining their organizations without any recognized framework will often lead to inconsistent controls and overlooked vulnerabilities, making it harder to demonstrate due diligence to partners, regulators, and customers.

In practice, while organizations *can* manage risk without the CSF, using a structured framework—especially one as widely recognized as NIST—significantly strengthens cybersecurity posture and improves alignment between security activities and business goals.

References

Balbix. (2025, January 17). *What is NIST Cybersecurity Framework (CSF) 2.0?* Balbix. Retrieved November 18, 2025, from https://www.balbix.com/insights/nist-cybersecurity-framework/

Kim, D., & Solomon, M. G. (2021). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

National Institute of Standards and Technology (NIST). (2025, February 25). *NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide* (NIST Special Publication 1300). U.S. Department of Commerce. Retrieved November 18, 2025, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf

IT Governance USA. (2024, June 6). *What Are 5 Top Cybersecurity Frameworks?* Retrieved November 18, 2025, from https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks