



The Institute of
Internal Auditors

Elevating Impact

November 6, 2023

Laurie E. Locascio, Ph.D
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

RE: IIA Comments Regarding NIST Cybersecurity Framework 2.0

Dear Director Locascio:

On behalf of The Institute of Internal Auditors (The IIA), the international professional association representing over 235,000 internal auditors, I appreciate the opportunity to comment on the National Institute of Standards and Technology's (NIST) public draft entitled: "[The NIST Cybersecurity Framework \(CSF\) 2.0.](#)"

According to a recent survey of chief audit executives published by The IIA, cybersecurity was identified as the number one risk confronting organizations in North America.¹ As companies of all size and sophistication race to address this omnipresent threat, the existence of an authoritative cybersecurity taxonomy – such as the proposed CSF 2.0 – accomplishes two primary objectives:

- Provides organizations with a needed framework to better understand and assess cybersecurity risk
- Facilitates access to resources, guidance, and controls designed to promote appropriate risk management outcomes.

Due to the internal audit profession's central role in evaluating cybersecurity risk, The IIA commends NIST for its continued leadership on this important issue. CSF 2.0, upon implementation, has the potential to increase positive risk management outcomes through an agile framework capable of adapting to a dynamic cybersecurity risk environment.

Upon a comprehensive review of the proposed CSF 2.0, The IIA recommends the following enhancement to Section 2.1:

GOVERN (GV) – Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy. The GOVERN Function is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management strategy. GOVERN directs an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; ~~and the~~ oversight of cybersecurity strategy, including assurance from an internal audit team that reports to the board of directors or audit committee.

¹ "2023 North American Pulse of Internal Audit: Benchmarks for Internal Audit Leaders," *The Institute of Internal Auditors*, March 2023

While The IIA supports inclusion of governance as one of the six “framework core functions,” the present language does not adequately address the need for assurance – such as that provided by an internal audit function – over an organization’s cybersecurity governance, compliance, and risk management. In other words, the proposal tacitly acknowledges the role of management in establishing and monitoring enterprise risk management but fails to recognize the importance of utilizing independent assurance to validate these actions.

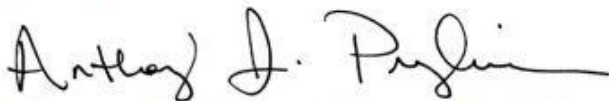
An organization’s internal audit function – operating in conformity with the *International Standards for the Professional Practice of Internal Auditing* – is the entity responsible for ensuring independent assurance over cybersecurity risk management and internal control processes. The presence of an internal audit function is widely considered a corporate governance essential practice for promoting organizational transparency, accountability, and trust.

Since internal audit represents a core element of any effective risk framework, its inclusion in Section 2.1 will strengthen CSF 2.0’s ability to successfully drive “high-level cybersecurity outcomes that can be used by any organization.”² Moreover, The IIA intends to supplement the concepts outlined in CSF 2.0 – as we have previously done in collaboration with NIST – with targeted Global Technology Guides (GTAGs). These publications will complement CSF 2.0 and provide organizations with the technical resources necessary to implement and align with the cybersecurity framework.

Should you or your staff have any questions regarding this matter or wish to discuss ways in which the internal audit profession can support your work, please contact Michael Downing, IIA Senior Director for U.S. Advocacy, at

Thank you for your consideration of our comments.

Sincerely,



Anthony J. Pugliese, CIA, CPA, CGMA, CITP
President and Chief Executive Officer
The Institute of Internal Auditors

² “The NIST Cybersecurity Framework 2.0,” *The National Institute of Standards and Technology*, August 2023