The Institute of
Internal Auditors
Elevating Impact

April 28, 2022

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Sir /Madam:

The Institute of Internal Auditors (IIA), a founding and sustaining member of The Committee of Sponsoring Organizations of the Treadway Commission (COSO), thanks the National Institute of Standards and Technology (NIST) for the opportunity to share comments on its AI Risk Management Framework (RMF).

For 80 years, The IIA and its now more than 210,000 members across the globe have aided sound governance and risk management efforts in public- and private-sector organizations, encouraging strong internal controls and an enterprise-wide approach. Auditing information systems, including those with artificial intelligence capabilities, is top of mind in this age of digital transformation and disruption.

The IIA recognizes that NIST's AI RMF can be a useful resource for organizations considering incorporating AI into business applications and processes.

In response to your question about alignment with existing practices and broader risk management practices, we concur with the overall approach to risk management articulated in the AI RMF as Map, Measure, Manage, and Govern, and we want to emphasize the importance of positioning AI risks as components of an organization's governance and enterprise risk management (ERM) programs, versus establishing siloed governance and risk management functions dedicated solely to AI.

With that said, The IIA believes that the current depiction of stakeholder groups reflected in Figure 1 could be improved by aligning with the Three Lines Model, widely recognized globally as a critical resource in successful governance. It helps organizations identify roles and responsibilities for setting strategies and objectives, managing risks – including risks related to the use of AI – and delivering benefits and information to stakeholders. The model establishes the three essential functions of governance as:

- Accountability of a governing body to stakeholders for organizational oversight through integrity, leadership, and transparency.
- Actions (including managing risk) by management to achieve the objectives of the organization through risk-based decision-making and application of resources.

GLOBAL HEADQUARTERS | 1035 Greenwood Blvd., Suite 149 | Lake Mary, FL 32746 USA | Phone: +1-407-937-1111 | Fax: +1-407-937-1101

- Assurance and advice by an objective, independent internal audit function to promote trust among stakeholders and continuous improvement through rigorous inquiry and insightful communication.

The Three Lines Model clarifies the roles of governing bodies, management, and independent assurance providers (internal and external). The AI RMF would benefit from adopting a model that differentiates between governance, management, and independent assurance processes. This model is well-suited to ensuring that the organization's objectives for the use of AI are met while mitigating potential harms. In this way, an independent assurance function is fundamental to supporting mutual trust among stakeholders.

In addition, regarding what might be missing from the AI RMF, we submit that there is an opportunity to incorporate some of the key concepts from IIA guidance or thought leadership, as well as the *International Standards for the Professional Practice of Internal Auditing* (*Standards*).The *Standards* establish a framework for governing and managing an internal audit function, which can provide valuable assurance and advisory services, including engagements covering all forms of artificial intelligence (RPA, ML, NLP, ANL, Expert System, Deep Learning, etc.). The *Standards*, together with implementation and other recommended guidance, represent best practices for assessing the design and implementation of processes for governing and managing AI.

For example, guidance for governing and managing AI use-case documentation and approval, as well as the design, development, and operation of AI models, can be found in The IIA's Global Technology Audit Guide (GTAG) "Auditing Business Applications." This GTAG references controls described in frameworks published by NIST, ISACA, and the Center for Internet Security, which provides a broad set of perspectives and suggestions. The AI RMF recognizes the importance of existing control guidance when it states (P. 2): "Risks to any software or information-based system apply to AI; that includes important concerns related to cybersecurity, privacy, safety, and infrastructure… [U]sers of the AI RMF are encouraged to address those non-AI specific issues via guidance already available."

There is also an opportunity to enhance some of the existing components of the AI RMF, such as the description of specialty areas, roles, tasks, knowledge, skills, and abilities. The AI RMF should make clear the importance of the skills sets referenced above (i.e., effective governance by the board members; enterprise-wide strategy, risk management, compliance, reporting, and operational processes by management; and independent assurance by internal and external service providers).

The IIA recognizes that the content related to Implementation Tiers – described in NIST's preceding AI concept paper – as well as Section 8 "Effectiveness of the AI RMF" are still under development. We believe these areas would present excellent opportunities to incorporate references to the Three Lines Model and other relevant control or assessment guidance. In some ways, the AI RMF will not achieve its objectives of describing "how the risks from AI-based systems differ from other domains and to encourage and equip many different stakeholders in AI to address those risks purposefully" until the Implementation Tiers or Section 8 are developed.

The Institute of
Internal Auditors
Elevating Impact

For specific recommendations, we would like to draw attention to the following:

Figure 1 - Please consider revising the stakeholder groups to align with the Three Lines Model. The inner ring would correspond to first line management, the second ring would represent management's review responsibilities (i.e., second line), the third ring would represent independent assurance, and the fourth ring would represent governance, which is responsible for ensuring the needs of various stakeholders are identified and addressed by management.

Section 5.2 – The AI RMF should explain what it means to set "precise threshold values for these [socio-technical] metrics" that "require significant human input and cannot yet be measured through an automated process." Examples of how NIST suggests that can be done would bring some clarity to this section.

Section 6.2 Measure and Table 2 – Please add independent assurance as a subcategory. It is important to stress that independent assurance and management's measurement processes are separate. It is also valuable to recognize that robust metrics, while supporting a healthy risk management culture and control environment, do not obviate the need for independent assurance to validate the organization's overall approach to the use of AI.

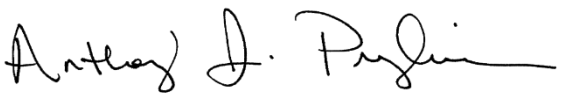
Section 6.4 Governance and Table 4 – Please add "ensuring an adequately positioned and resourced internal audit activity" as a governance subcategory, for the reasons described above. Independent, competent assurance on AI governance and management processes supports trust among stakeholders.

Table 4 and Part 2 Section 8 "Effectiveness of the AI RMF" – The framework describes the need for policies and procedures, but it should also state that organizations need to implement controls that review, test, and monitor those policies and procedures (i.e., second line management).

Harm - We also recommend NIST provide more examples to define and measure the "harm" caused by the use of AI models, and how that should inform the "impact" variable of the risk equation [often, risk is expressed as the product of likelihood and impact].

The IIA offers our on-going assistance to support your review and development of the AI RMF. Please do not hesitate to contact me or our Vice President of Global Advocacy, Policy, and Government Affairs, Mat Young, (mat.young@theiia.org, (202) 270-0170), for any questions, comments, or additional input.

Sincerely,



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