Workday's Comments on NIST's Initial Draft of the AI Risk Management Framework

April 2022

Workday is pleased to comment on the initial draft (Initial Draft) of the National Institute of Standards & Technology's AI Risk Management Framework (AI RMF or Framework).

Workday is a leading provider of enterprise cloud applications for finance and human resources, helping our customers adapt and thrive in a changing world. Our applications have been adopted by thousands of organizations in the U.S. and globally—from medium-sized businesses to more than 50 percent of the Fortune 500. Workday incorporates machine learning into our software to enable customers to make more informed decisions and accelerate their operations, as well as to assist workers with data-driven predictions that lead to better outcomes.

Achieving AI's full potential requires trust that organizations are developing and using AI in a responsible manner. NIST's AI Risk Management Framework is a pioneering effort for organizations committed to advancing trust in AI, and Workday welcomes the opportunity to offer its feedback on the Initial Draft. These comments build on Workday's previous contributions to NIST's AI work, including comments, workshops, and our whitepaper, *Building Trust in AI & ML Through Principles, Practice, & Policy*.

I. General Comments

A. The Direction of the Initial Draft

Workday finds the general direction of the AI RMF to be the right one. As NIST revises the Initial Draft, we encourage it to not only consider how Version 1.0 of the Framework will effectively manage AI risks, but how to facilitate its rapid, widespread adoption by the business community. We therefore welcome further details from NIST on the AI RMF's Implementation Tiers, Practice Guides, and Profiles. Workday also recommends that NIST issue guidance on how organizations already using its Cybersecurity and Privacy Frameworks can more easily integrate the forthcoming AI RMF into their governance programs. As these tools are already widely used in the business community, the additional guidance will facilitate the AI RMF's timely adoption.

B. AI Risk Management as a Shared Responsibility

AI risk management is a responsibility that is shared by developers, deployers, and end-users of AI systems. The role of each of these stakeholders within the AI risk management lifecycle, however, is conditioned by technical, legal, and organizational considerations which vary from context to context.

Enterprise software providers, for example, typically do not have full visibility into how their customers are using their AI tools due to technical and contractual limitations, including data protection requirements. Consequently, deployers of AI tools are usually better positioned than developers to understand the specific organizational context where a tool is being used and to communicate directly to end-users.

The Framework should explicitly acknowledge the shared responsibility and contextual nature of AI risk management. In doing so, we recommend that NIST review the use of stakeholder designations throughout the document to ensure that the RMF accurately and consistently describes their roles and responsibilities, as well as their limitations. The RMF should explicitly acknowledge when primary responsibilities are shared, unclear, or context-dependent, and consider ways to build in flexibility that allows RMF users to apply the Framework in varying commercial relationships.

C. Impact Assessments

We recommend that NIST integrate AI impact assessments into the next draft of the Framework. NIST's recent publication, *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence,* rightfully highlights impact assessments as a tool for managing AI risks. Impact assessments are a mature tool already used by organizations for privacy, data protection, and environmental protection, and there is growing interest among governments, academics, and the business community in AI impact assessments. We note that impact assessments may be used in every stage of the AI lifecycle to map, measure, and manage risk in support of better governance.

II. Specific Comments

A. Framing of Risks

In our previous submission, Workday raised concerns about treating risks as "one-size-fits-all" under the category of "sociotechnical." We therefore appreciate the lengthy discussion of risk in the Initial Draft, especially its threefold distinction between technical, sociotechnical, and guiding principles, which address these concerns.

B. Clarifying the Use of the Term of "Auditing"

Workday notes that NIST's Initial Draft and a companion paper, *Towards a Standard for Identifying Bias in Artificial Intelligence*, make several references to "audits" and "auditing." As NIST considers what role these tools may serve in the Framework, we urge it to clarify that audits may be conducted within an organization by its personnel and not only by external parties. In fields with mature consensus-based technical standards, such as privacy and cybersecurity, audits by external parties can serve as an important governance tool and a valuable mark of trust. With consensus-based AI technical standards still in development, however, AI audits are an unproven tool that vary in quality, effectiveness, and scalability. Without clarifying its use of the term

"audits," NIST may inadvertently overstate the maturity of these tools and undercut its efforts to develop a law- and regulation-agnostic Framework.

III. Conclusion

Thank you for the opportunity to comment on NIST's Initial Draft of the AI Risk Management Framework. We stand ready to provide further information and to answer any additional questions. Please do not hesitate to reach out to Evangelos Razis at ...for assistance.