

## Towards Trusted Innovation: Our Vision for U.S. AI Policy

At Workday, we believe that AI is [powering the future of work](#) by unlocking human potential, driving business value, and enabling our customers and their employees to focus on more strategic and fulfilling work. Consistent with our [commitment to ethical AI](#), Workday has been helping to lay the groundwork for smart AI safeguards since 2019. Building on our [call for AI regulation](#), Workday offers the following recommendations for AI regulation that is meaningful, technically sound, and advances responsible innovation.

### A Risk-Based Approach to AI Governance

The development and use of AI tools is growing—and rapidly. To navigate these dynamics, policymakers are [converging](#) on a risk-based approach to AI governance that maximizes the benefits of AI and minimizes the risks of potential harm. As key U.S. trading partners are demonstrating, including the [European Union](#), [Canada](#), the [United Kingdom](#), and [Singapore](#), a risk-based approach means applying rules to contexts where AI carries the highest risk of potential harm to individuals. To achieve a risk-based approach to AI governance in practice, Workday recommends that policymakers:

- **Focus on consequential decisions.** When an AI tool is used for a decision about an individual’s access to an essential opportunity, it has the potential to pose harm to that individual. AI regulatory frameworks should focus on these kinds of consequential decision tools, which may be used to hire, promote, or terminate an individual’s employment, or in other contexts, determine access to credit, healthcare, or housing. The [American Data Privacy and Protection Act](#), among other leading [proposals](#), focuses on AI tools used in ways that pose a “consequential risk” to individuals. In the U.S., there are also long-standing guardrails in place, such as anti-discrimination laws. These guardrails may [already apply](#) to the use of AI, and should [inform how AI tools](#) used in consequential decisions are further regulated.
- **Distinguish between automated tools and tools with a human in the loop.** An AI tool that *replaces* human decisions poses a higher risk than an AI tool that *enriches* them. This is because an automated tool can make consequential decisions at a higher volume and velocity than a human, and without the judgment that a human brings. By contrast, when an informed human is in the loop they can leverage an AI tool’s insights and remain in control of and accountable for the final decision. California’s [AB 331](#), a promising benchmark for AI regulation, makes this distinction by targeting AI tools that are the *controlling factor* in a consequential decision. New York City’s [Local Law 144](#) takes a similar approach, focusing on AI tools that overrule or have a greater weight than a human’s decision making.

## Workable Accountability Tools and Governance Frameworks

The field of AI governance is nascent, with best practices, standards, and accountability tools still maturing. When considering guardrails for high-risk AI tools, policymakers should consider which proven, workable approaches are available today and which require additional building blocks to be in place before they can be implemented effectively. As AI governance continues to mature, we recommend that policymakers:

- **Leverage impact assessments as a proven accountability tool.** Impact assessments are a tool that organizations use to identify, document, and mitigate the risks posed by technology. Widely used in the fields of [privacy](#) and [data protection](#), impact assessments are already familiar to many organizations, as they are required under the *General Data Protection Regulation* and multiple U.S. state privacy laws. They are practical because impact assessments are a holistic and iterative risk evaluation that can be carried out by a developer and deployer of a high-risk AI tool and do not rely on still-nascent technical standards. There is a growing consensus among lawmakers, [business leaders](#), and civil society that impact assessments for high-risk AI tools are the most [promising AI accountability tool](#) available today.
- **Implement and promote the NIST AI Risk Management Framework.** The [NIST AI Risk Management Framework](#) was developed at the direction of Congress through an open, multi-stakeholder process and with participation from [academia](#), [civil society](#), and [the business community](#). Launched in January 2023, the Framework is a how-to guide for organizations of all sizes, industries, and geographies to develop and use trustworthy AI. Workday was an [early advocate](#) for the creation of a NIST AI framework, participated in its development, and is [incorporating](#) it into our AI risk management process. As policymakers look to support trustworthy AI, we urge the public sector to lead by example and: (1) implement the NIST AI Risk Management Framework; and (2) require vendors providing high-risk AI tools to the federal government to implement the Framework as well. These recommendations are echoed in the National AI Advisory Committee's [Year 1 Report](#).
- **Avoid premature third-party audit requirements.** Although promising in the medium- and long-term, AI auditing is a field that is still in development, as there are neither consensus technical standards nor a common set of criteria to audit AI tools against. Nor are there professional standards that are binding on third-party AI auditors, which are necessary for ensuring auditing quality and integrity. As noted in the White House's 2023 [National AI Research and Development Strategic Plan](#), absent such standards, the scalability of AI auditing is a significant practical challenge. A recent bipartisan [letter](#) by 23 attorneys-general similarly noted the need for AI audits to follow a “common set of criteria set by independent standards” and for these standards to be developed. Without such building blocks, premature third-party audit requirements may unintentionally diminish trust in the AI marketplace by failing to promote consistent accountability.

## A Shared Responsibility and Partnership

AI governance is a shared and cooperative project between the organizations that develop and use AI tools and between the U.S. and its key allies and partners. To ensure regulatory frameworks account for the distinct roles of different organizations in the AI marketplace and are interoperable across borders, we recommend that policymakers:

- **Assign role-based obligations.** AI governance is a [shared responsibility](#) between developers, which design, code, and produce an AI tool, and deployers, which operate and use the tool and interact with end users. *Developers* typically have insight into how an AI tool is built but may not have access to their customers' data or control over how a customer configures and uses the tool. By contrast, *deployers* determine how an AI tool is implemented and used, but typically do not have control over how the AI tool was designed. Similar to [privacy and data protection laws](#), AI regulatory frameworks should distinguish between these roles and assign obligations accordingly. The [OECD](#) has recognized this distinction in the risk management context as AI “in the lab” (i.e., developers) versus AI “in the field” (i.e., deployers).
- **Drive international cooperation on AI regulation.** Policymakers should closely collaborate with key U.S. allies and partners to build interoperability between emerging AI regulatory frameworks. While a priority should be building bridges with the conformity assessment regime established in the [EU's AI Act](#), cooperation with other governments exploring AI governance, including, Australia, Canada, Japan, Singapore, South Korea, and the United Kingdom, is crucial. Following a [recommendation](#) from the National AI Advisory Committee, the U.S. should seek to “internationalize” the NIST AI Risk Management Framework to avoid global regulatory fragmentation, prevent barriers to cross-border trade in AI services, and support effective AI governance by promoting a consistent benchmark.
- **Support and accelerate development of AI technical standards.** Technical standards play an essential role in AI governance. Standards help manage risk and promote security, safety, privacy, and quality in the development of new innovations. Accountability tools, such as [audits and conformity assessments](#), rely on technical standards to be developed. As [global](#) and [regional](#) standards bodies begin this important work, policymakers should increase U.S. investment in, and seek to accelerate, the development of open, consensus-based technical standards by the private sector, in partnership with academia and civil society, and in line with long-standing [U.S. standards policy](#) and [international norms](#) on standards development.

## Enabling a Skills-Based Approach to Talent

A skills-based approach to talent can increase both workers' and employers' ability to respond more nimbly to shifts in the economy, while also expanding opportunities for diverse and underrepresented candidates. AI is [essential](#) to enabling a skills-based approach to the workforce at scale. This is because of AI's unique abilities to parse massive amounts of skills data, generate insights into existing and in-demand worker skills, drive informed decision-making in the current and future job market, and maximize the impact of workforce development efforts by helping target policy interventions. We support a [full consideration](#) of not only the impact technology can have, but also the opportunities [AI tools can unlock](#) when applied to skills-based approaches to talent. We recommend policymakers:

- **Encourage a skills-based approach to talent in the public sector.** To make the most of AI's potential to unlock workforce opportunities, policymakers should begin with a skills-based approach to talent. Federal hiring practices are already moving in this direction, with momentum also building [at the state level](#). The President's Management Agenda, for example, [highlights](#) the importance of strengthening the federal workforce, including through skills development. In 2022, the Office of Personnel Management released federal [Skills-Based Hiring Guidance](#), building on efforts that span the last two administrations. In addition, the House of Representatives recently passed the bipartisan [Chance to Compete Act](#), which looks to provide agencies with tools to build on existing federal skills initiatives. Policymakers should consider which technology and AI-related investments are needed to accelerate this shift to a skills-based approach to talent at scale.
- **Modernize labor market data.** While the Department of Labor currently produces important federal macroeconomic information, the U.S. labor market data reporting system does not provide real-time information with sufficient granularity to drive regional or local workforce insights. When coupled with new AI tools, better data can provide public officials, employers, and workers with greater insights into employment patterns, the skills workers already have, and skills that are in demand in the job market. We encourage greater public-private collaboration to modernize labor market data, with the aim of developing interoperable, timely, accurate, and high-quality information suited for the age of AI.

### About Workday

[Workday](#) is a leading provider of enterprise cloud applications for finance and human resources, helping customers adapt and thrive in a changing world. Workday applications for financial management, human resources, planning, spend management, and analytics are built with AI and machine learning at the core to help organizations around the world embrace the future of work. Workday is used by more than 10,000 organizations around the world and across industries—from medium-sized businesses to more than 50% of the *Fortune* 500.