2026 EDITION

EXECUTIVE PERSPECTIVES ON TOP RISKS AND OPPORTUNITIES

protiviti®
Global Business Consulting

From Threats to Transformation: The Key Risks and Opportunities Shaping Government Strategy

By Charles Dong
Managing Director, Global Leader, Public Sector, Protiviti

Successful organizations view even challenging times as catalysts for innovation and growth, actively seeking opportunities where others see obstacles.

Over the last 13 years, we have issued annual research reports on the top risks faced by leaders all over the world. This year, we have added an emphasis on opportunities to set the tone for identifying and responding proactively to emerging trends, market shifts and evolving customer expectations. Organizations balancing risk management with a strong focus on transformation are better equipped to innovate services, enhance their resilience, adapt to change, and achieve their strategic goals. It is all about unlocking opportunity.

Our 14th annual **Executive Perspectives on Top Risks and Opportunities Survey** contains insights from 1,540 board members and C-suite executives around the world regarding their views on:

- Three specific areas of opportunity considering the current environment;
- Opportunities and challenges associated with the transformative impact of artificial intelligence (AI) on their organizations;
- The top risks on the horizon for the near term (two to three years ahead) related to 28 specific risks across three dimensions (macroeconomic, strategic and operational) and for the long term (a decade from now) related to 12 risk themes that consider the strategic and operational near-term risks; and
- A discussion of their organizations' near-term strategic investment priorities, given the opportunities and the risks they face.

Our survey participants shared their views through an online survey conducted from early September through mid-October 2025. This paper offers specific insights into these issues from the perspective of the government industry.

Where do leaders in the government industry see the greatest opportunities over the next two to three years?

As pressures mount for governments to modernize service delivery, increase interoperability and efficiency, reduce expenditures and secure government systems and data against increasing and emerging threats, many are turning to ecosystem development — building a network of technology partners, platforms and data-sharing capabilities — as a way to achieve these goals. This top opportunity, identified by 53% of respondents, centers on **modern platforms/cloud** for cybersecurity and interoperability, **data foundations and digitization** for data mining and analytics, and **emerging technologies** (AI and automation) for efficiency gains.

Agencies see ecosystem partnerships as a way to accelerate modernization and respond to citizens' expectations for responsiveness and efficiency without carrying the full burden of cost, talent or development time. This means:

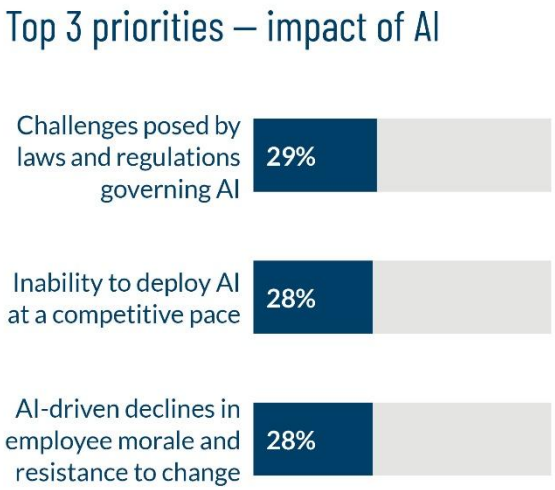
- Access to specialized skills not available in-house
- Faster implementation cycles
- Shared investment rather than full ownership
- Ability to pilot and scale innovations more safely
- Avoiding costly internal build-outs

The same mindset likely accounts for highlighting revenue potential as an opportunity, flagged by one-half of government executives. There is a growing movement within government agencies toward budget optimization, cost reduction and even monetization of government assets to generate revenue, rather than pure spending. This cultural shift encourages government executives and heads of agencies to explore technology solutions like data management, automation and AI to close efficiency gaps and revenue leaks and create public value out of government assets. Embedding these technologies in government processes can help reduce fraud, increase tax collection, and streamline and automate administrative tasks.

One lever for revenue creation is incentivizing private investment in communities to increase the tax base. Data centers have become a recent focus area for governments as a potential source of revenue and economic growth, notably in the U.S., but also the United Kingdom, Europe, Singapore, India and other parts of the world. Designating data centers as critical national infrastructure and creating national data center plans and policies allows governments to fast-track their approval and to target specific strategic locations. In some cases, notably, Europe and Singapore, data centers are also tied to sustainability goals, targeting both short-term revenue and long-term economic resilience.

What will be governments' most significant challenges regarding the impact of AI over the next two to three years?

AI in government is a complicated subject surrounded by regulatory complexity and elevated public scepticism and scrutiny. AI has only recently emerged as a regulatory subject, and the regulatory landscape is anything but uniform or mature. This poses challenges for governments at different levels (national, regional or local) on how to deploy AI confidently if jurisdictional laws are in conflict with each other. So it is not a surprise that laws and regulations emerged as the top AI-related challenge for government executives in the survey.



There is a focused effort to address this issue with legislation such as the European Union AI Act, which requires member countries to make investments in AI governance, algorithmic transparency and high-quality interoperable datasets. Australia's National AI Plan likewise aims at creating a uniform national landscape while emphasizing responsible practices and safety. In the United States, President Trump's executive order on AI attempts to promote a uniform standard for AI governance by banning states from issuing "onerous" AI laws. However, federal AI legislation in the U.S. remains elusive for now, leaving AI to be governed by a patchwork of state regulations.

The still emerging regulatory picture is likely one of the reasons why government leaders worry they may not be able to deploy AI as quickly as they would like. Public agencies must move carefully to avoid accusations of bias, unfairness or personal data misuse, and violations of laws like the General Data Protection Regulation (GDPR) or state-level privacy legislation. While government respondents ranked data privacy and cybersecurity concerns as number four, and lack of governance and accountability for AI deployments as number five, both of these concerns roll up to the top two priorities.

The third highest risk, AI-driven decline in employee morale and resistance to change, points to another government pressure. This risk ranked significantly higher for government than any other industry, by eight percentage points or more — not surprising given the disruptive effect of AI generally but especially on the typically long-tenured, single job-focused government workforce. Without a clear understanding of how AI fits with their jobs, many career public servants are fearful they will be displaced, devalued or let go, or they just lack confidence in using AI tools, depriving AI investments of their potential. Governments are typically at a disadvantage when competing with the private sector for digital talent. The sector must seize the opportunity now to upskill the existing government workforce with targeted training in AI tools and related technologies, as well as consider new management methods for a blended human-AI workforce. Without addressing these capability gaps, any modernization initiatives will struggle to scale effectively.

What are the most significant short-term (two to three years) concerns and risks on the minds of government executives?

There has been a remarkable shift in short-term risk perception among government executives in just one year. Notably, cyber threats climbed up to number one from number six last year, while third-party risks wasn't even in the top ten. Legacy infrastructure and AI-related risks both jumped from the bottom third of last year's ranking.

Top global near-term risks

2026 rank	Risk issue	Average*	2025 rank
1 (tie)	Cyber threats	2.98	5
1 (tie)	Third-party risks	2.98	14
3	Operations and legacy IT infrastructure unable to meet performance expectations	2.86	23
4	Emergence of new risks from implementing AI	2.80	19
5	Economic conditions, including inflationary pressures	2.77	2

* Average based on a five-point scale where 1 reflects "No impact at all" and 5 reflects "Extensive impact."

This sharp reordering of priorities speaks to how the world has changed. A real-world uptick in cyber-enabled crime and ransomware targeting municipal systems, law enforcement databases, hospitals and other public service systems has helped propel cyber to the top. The high-value data and strategic importance of these databases makes them lucrative to both criminal individuals and networks and nation-state actors.

Governments' increasing dependency on infrastructure vendors (cloud, telecom, defense contractors) further amplifies cyber exposure and places third-party risks on par with cyber (they are tied at the top). Geopolitical tensions increase third-party vulnerability — especially for agencies using foreign-sourced technology.

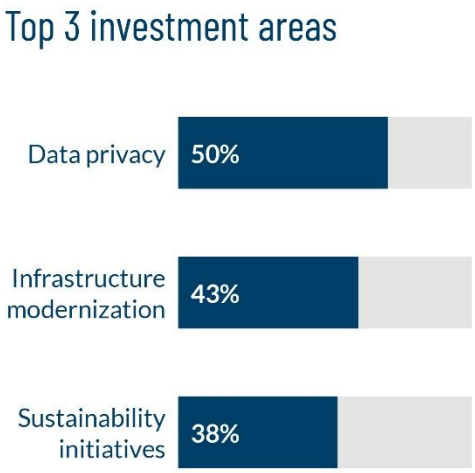
Legacy IT concerns and AI-related risks saw the biggest change in priority year over year. While governments did accelerate digital services during COVID, many did so on fragile, patched systems. Now, technical debt is colliding with technology modernization ambitions and creating operational risk. Addressing legacy IT isn't just an efficiency issue or a technology upgrade; it's security risk control.

To see legacy infrastructure and AI risks rise together isn't a surprise. Agency leaders are grappling with aging systems while struggling to integrate AI in order to do more with less and are facing security and integration issues, workforce resistance and regulatory expectations (or uncertainty) in the process. All of these factors contribute to the elevation of this pair of risks to the near top.

There are some regional differences in the short-term risk perceptions worth mentioning. In North America and Europe, geopolitical shifts and market uncertainty ranked higher, while in Australia AI priorities dominate — likely a reflection of recent national initiatives and frameworks focused on cyber and AI.

Based on these near-term risk issues, in what areas is the organization likely to invest the most over the next two to three years, and why?

Data privacy, infrastructure modernization, cybersecurity and regulatory compliance all fell within the top five investment priorities for government executives across the globe, with only slight regional variations: Government executives in Australia named infrastructure modernization their number one priority. Data privacy, cybersecurity and third-party risks scored higher in Europe and North America.



Data privacy is a regulatory mandate and will require sustained investment as governments scale digital services and begin implementing AI. Investments in data systems and governance will be driven by the EU AI Act's demand for robust data governance, procurement transparency rules, auditability requirements, and continued compliance with GDPR. As more administrations begin to develop AI pilots, ensuring lawful and ethical data use and privacy-by-design practices becomes critical.

Infrastructure modernization is also critical for the many reasons we highlighted earlier. Many administrations still operate on mainframe-type platforms that impede interoperability, efficient service delivery and new technology adoption. Investments will focus on cloud migration, re-platforming legacy software, and implementing common service layers across regions and municipalities.

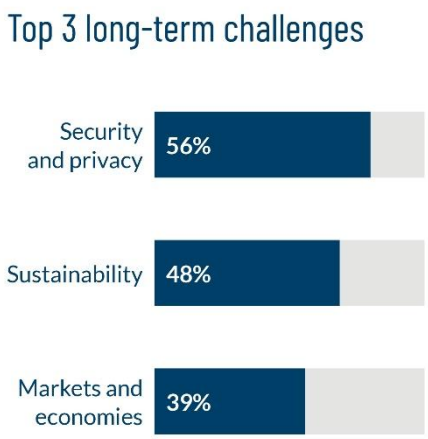
Sustainability investments did not make the top five in Europe and North America, but they were deemed second most important, after infrastructure, for Australia, affecting the global ranking of this priority. This result is likely regulatory-driven; the Australian government operates under an enforceable sustainability framework comprising net-zero legislation, transparent climate planning, procurement mandates and green trade pacts, and is exploring border-carbon measures.

Europe does not have a binding sustainability reporting regime for governments but the European Green Deal, together with the Carbon Border Adjustment Mechanism (CBAM) and EU Deforestation Regulation shape how individual governments and public administrations plan and implement climate-related policies and direct investments.

In North America, agency focus has shifted from sustainability to issues that impact citizens more directly and have clear measurable impacts. Infrastructure modernization, security, privacy and regulatory compliance form a natural cluster of areas that governments can invest in for synergetic results. Investing in sustainability may be a priority for municipalities or individual states but it did not reflect in the region's ranking as a whole.

How do government leaders view the 10-year risk outlook for their organization?

Security and privacy will remain top priorities in the foreseeable future as governments accelerate digital transformation, expand their ecosystem and third-party relationships and seek opportunities to embed AI in processes — all of which will require strong cybersecurity and data-protection frameworks. Frameworks like NIS2 in Europe, NIST CSF in the U.S., SOCI Act in Australia and ongoing GDPR enforcement are pushing administrations to invest in SOC services, zero-trust architectures, secure cloud migration, and improved identity management. High-profile attacks on public hospitals, municipalities, and regional systems have further heightened this urgency.



Regulatory and financial drivers and the reality of natural disasters make focus on sustainability and overall resilience unavoidable for most governments. Climate-vulnerable municipalities and regions are likely to focus attention and resources on shoring up infrastructure, climate adaptation, and monitoring and early-warning systems. Where laws or citizens require it, governments will be investing in improving the energy efficiency of building, reducing emissions from the public fleet, implementing sustainable mobility plans, and integrating sustainability into procurement criteria.

The economy is a perennial concern for governments as it most directly affects tax revenue. Market uncertainty, tariffs and geopolitical realignment keep this concern elevated for the foreseeable future. Governments and public agencies are likely to seek an increase in public-private partnerships along with creative revenue generation opportunities to alleviate the economic pain.

Guidance/call to action for next two to three years

The challenge for government leaders is to turn the risks and opportunities identified in the survey into concrete government actions with measurable outcomes. Our recommendations include:

- **Build a public–private tech ecosystem.** Partner with hyperscalers and specialized companies to accelerate cloud migration, cybersecurity services and data digitization and to develop AI pilots. Focus on getting pilots into production. Structure MOUs and outcome-based contracts to move faster on citizen-facing services.
- **Address legacy infrastructure issues.** Prioritize re-platforming mainframes, adopting secure cloud, and implementing common service layers to enable interoperability, efficiency and security at scale; fund multi-year technical-debt retirement tied to measurable service KPIs.

- **Strengthen cyber defense and third-party risk management.** Stand up (or expand) SOC services, adopt zero-trust architectures, and enforce vendor risk controls to address ransomware, nation-state threats and supply chain exposure.
- **Establish AI governance and data privacy-by-design.** Create cross-agency AI policies, transparency and audit requirements, and high-quality interoperable datasets; set guardrails for AI use in accordance with existing laws and regulations.
- **Upskill the workforce for AI and digital operations.** Launch targeted training and change management programs to reduce morale impacts, build confidence with AI tools and close digital talent gaps.
- **Align investments to near-term priorities.** Direct funding to data privacy, infrastructure modernization, cybersecurity and regulatory compliance.

About the author

Charles Dong is a Managing Director with Protiviti and serves as the firm's Global Public Sector Industry Leader. He brings extensive experience advising state and local government agencies, educational institutions, and not-for-profit organizations on accounting, financial management, regulatory compliance, and organizational transformation. His work bridges financial integrity, operational efficiency, and mission delivery — helping public organizations modernize systems, strengthen accountability, and improve service outcomes.

Contact Charles at charles.dong@protiviti.com.