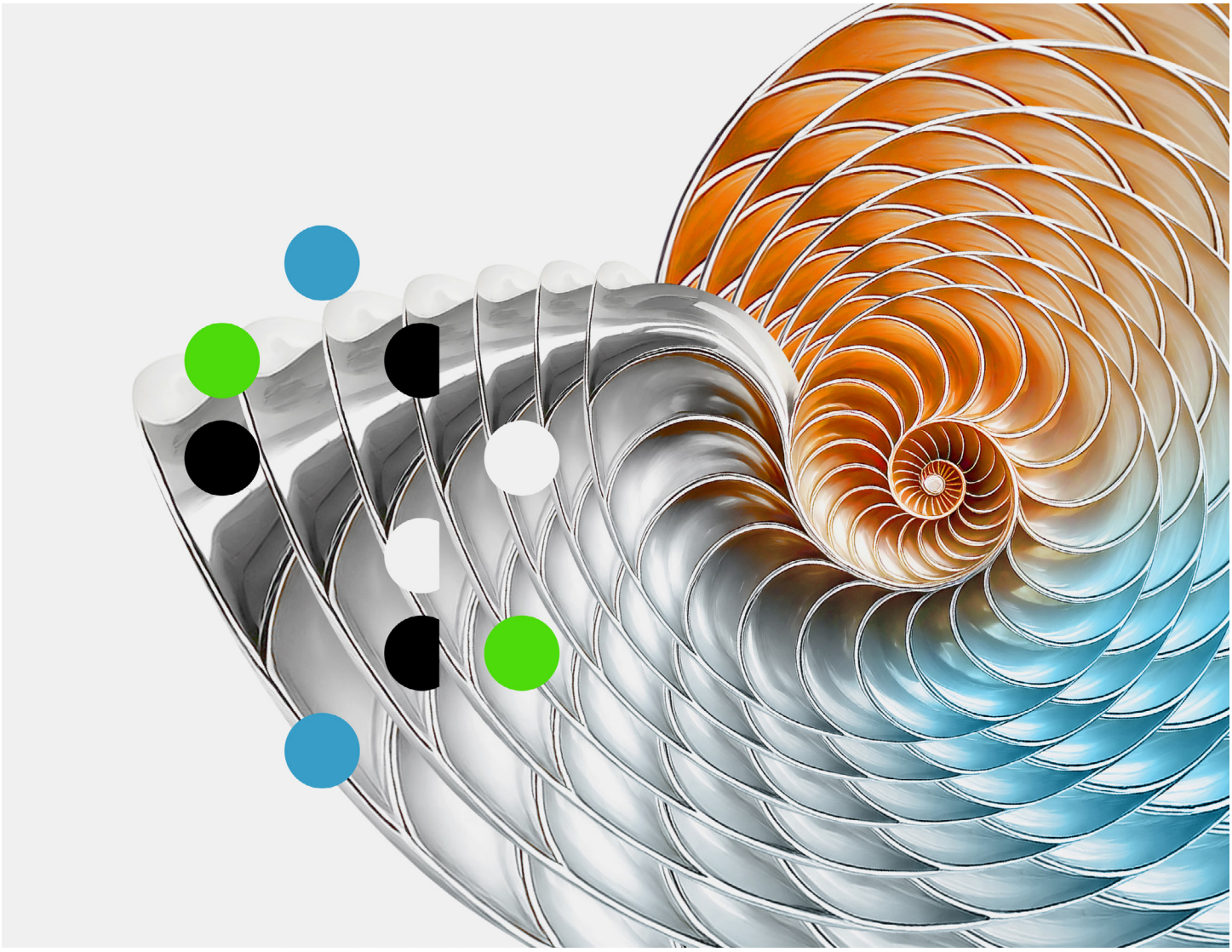
Deloitte.

Together makes progress



GovTech Trends 2026 | Deloitte Insights

GovTech Trends 2026

The artificial intelligence (AI) imperative for government innovation

AI has become a foundational force in enterprise technology. This year's Tech Trends report shows how governments can shift from experimentation to impact, using AI to accelerate innovation and deliver measurable results. Discover the trends most relevant to the public sector and how to harness them to redesign processes, align investments with mission goals, and transform operations.

This report provides a government-specific take on Deloitte's Tech Trends 2026, spotlighting the accelerating technology trends most likely to disrupt enterprise IT over the next 18 to 24 months. We explore which innovations may matter most for governments and assess their readiness to scale. Learn how public sector organizations can harness emerging technologies, especially AI, to redesign processes, align investments with mission objectives, and transform operations for the future.

Relevance and readiness scale:

We looked at each trend and assigned a value from one (low) and five (high) based on the trend's relevance and readiness of government adoption.

READINESS:

How ready is the government to adopt the trend?

RELEVANCE:

How impactful would it be if the government adopted the trend?

AI goes physical
Navigating the convergence of AI and robotics

Physical AI is evolving robots from preprogrammed machines into adaptive systems that perceive, learn, and operate autonomously in complex environments. These capabilities show up in industrial robots, autonomous vehicles, drones, and other systems. Current challenges include gaps in training, safety concerns, and cybersecurity risks, but falling costs are extending adoption beyond smart warehousing and supply chain operations into the mainstream. Humanoid robots are the next frontier; future developments may include bio-hybrid robots and quantum robotics.

Trend in action

Physical AI offers governments new ways to strengthen safety, resilience, and service delivery. Beyond traditional automation, intelligent machines can take on tasks that are dangerous or resource-intensive. For example, drones can provide rapid structural assessments after earthquakes and autonomous vehicles can support snow removal during severe storms to keep transportation networks open. Even routine tasks like identifying potholes can be streamlined by robotics. Yet realizing value will require investing in training and change management to prepare government employees for new ways of working with these technologies. Leaders should make sure that they're not allowing point solutions to overwhelm organizational capacity, focusing instead on flexible, scalable platforms, and interoperability. Solutions will also need to account for public safety, cybersecurity, and ethical considerations. By starting small and embedding these principles into planning and execution, smart governments can pave the way to move beyond pilots to realize constituent value, deliver smarter services, and foster greater public trust.

READINESS: 2

RELEVANCE: 3

The agentic reality check
Preparing for a silicon-based workforce

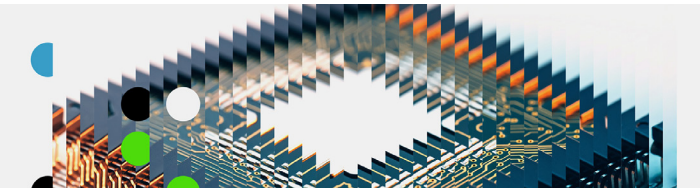
Despite early enthusiasm, many businesses have yet to see significant transformation from agentic AI implementations because most simply automate existing processes rather than fundamentally redesigning operations. Only 11% of surveyed organizations have deployed agentic systems in production, with challenges including legacy system integration, data architecture constraints, and inadequate governance frameworks. Leading organizations are adopting agent-first process redesign, implementing multiagent orchestration using emerging protocols, and treating agents as a silicon-based workforce requiring specialized management frameworks. This includes agent onboarding, performance tracking, and FinOps cost management. The future points toward graduated autonomy levels, hybrid human-digital workforces, and leveraging agent-generated data for continuous learning, transforming how enterprises operate and compete.

Trend in action

Many government organizations have not embraced agentic AI, in spite of its promise to automate more complex and nuanced tasks. Early efforts have often been focused on automating current processes rather than reimagining operations, reinforcing legacy constraints. Yet some leaders have worked to transform citizen engagement by deploying digital agents that handle complex services across languages and channels, each guided by defined onboarding protocols and escalation rules. Digital agents can coordinate multistage internal processes, manage compliance checks for citizens and transform paperwork into "clickwork," fast-tracking solutions at the speed of need. Move beyond incremental gains by prioritizing process redesign and leveraging autonomous decision-making and orchestration across systems. Build workforce capability by upskilling existing resources and designing systems to work as a human/AI team. Develop scaled capability by focusing on integration and scalability to set the stage for agentic AI to become a foundational element of adaptive, citizen-centered government operations.

READINESS: 2

RELEVANCE: 5



The AI infrastructure reckoning

Optimizing compute strategy in the age of inference economics

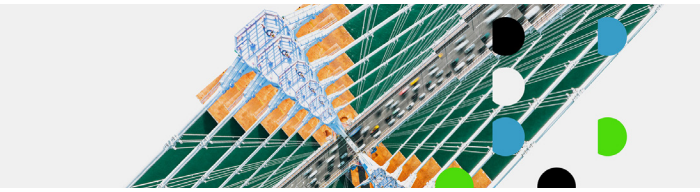
As AI moves from experimentation to production, enterprises face an infrastructure dilemma. While token costs have dropped substantially, overall AI spending is exploding due to massive usage growth. Organizations are hitting a tipping point where cloud services become cost-prohibitive for high-volume workloads, with monthly bills reaching tens of millions. Leading enterprises are adopting strategic hybrid architectures: cloud for variable workloads, on-premises for consistent production inference, and edge for latency-critical applications. This can require purpose-built AI data centers featuring hardware optimized for graphics processing units, advanced networking, and specialized cooling. Future challenges include workforce reskilling, AI agents managing infrastructure, and sustainable computing innovations like renewable-powered and potentially orbital data centers.

Trend in action

As government agencies accelerate their AI ambitions, decisions about where and how to run workloads are expected to significantly shape the future of public service. Choices made today could determine whether agencies respond with agility during crises or struggle to keep up. For example, during a wildfire, edge computing could enable firefighters and first responders to fuse data from drones, thermal cameras, and weather sensors to map fire hotspots and predict their movement—even if cellular networks are down. Or an owned data center without a pre-planned contingency option could be overwhelmed during a national crisis. The available data center options continue to proliferate, now starting to include space-based resources. With this wide range of technology options and ambitions, agencies should evaluate which solutions best align with their mission and long-term impact. Thoughtful planning now can empower governments to deliver resilient and innovative AI services well into the future.

READINESS: 3

RELEVANCE: 3



The great rebuild
Architecting an AI-native tech organization

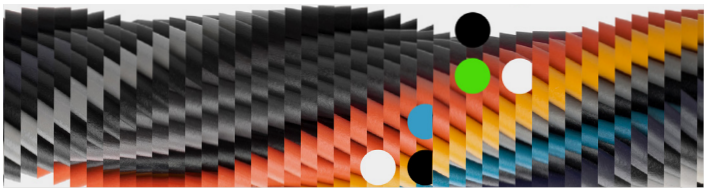
AI is fundamentally restructuring technology organizations beyond simple automation. With 64% of organizations increasing AI investments and tech budgets for AI rising, priorities are shifting from infrastructure maintenance to strategic leadership. Leading organizations are anchoring AI initiatives to measurable business outcomes, designing modular architectures for flexibility, and redefining talent strategies around human-machine collaboration. New roles are emerging, such as AI collaboration designers, edge AI engineers, and prompt engineers, while chief information officers evolve from tech strategists to AI evangelists and orchestrators. Future tech organizations will feature agentic architectures, lean product-led teams, blended human-agent workforces, adaptive governance, and ecosystem-oriented innovation. Success requires embracing continuous evolution and boldly reimagining operations rather than incremental change.

Trend in action

As AI begins to reshape how agencies deliver services and operate, technology teams should be prepared to outline their specific plans for adopting and integrating AI solutions. Some agencies are rising to the challenge by utilizing AI tools to drive rapid prototyping, accelerate legacy modernizations, and provide customer support. Agentic AI solutions can bridge IT silos, providing speed and visibility by automating complex processes that cross internal boundaries. Advanced code generation tools can accelerate the process of understanding legacy systems, writing requirements and user stories, and generating the resulting code of modernized systems. Together, technology teams are learning from internal AI-enabled transformation to better support mission transformation. Success depends on more than just adopting new tools; it requires rethinking structures, clarifying responsibilities, and empowering teams. Adaptability isn't optional, it's essential. By embracing new ways of working, leaders can meet the moment and turn opportunity into real-world results.

READINESS: 2

RELEVANCE: 3



The AI dilemma
Securing and leveraging AI for cyber defense

AI creates a cybersecurity paradox: The same capabilities driving business innovation are also introducing new risks. Organizations face threats from shadow AI deployments, adversarial attacks, and intrinsic AI system weaknesses across four domains: data, models, applications, and infrastructure. Existing security practices can be adapted to address AI-specific risks through robust access controls, model isolation, and secure deployment architectures. And AI offers powerful new capabilities to counter the very vulnerabilities it creates. Leading organizations are leveraging AI defensively through red teaming with AI agents, adversarial training, and automated threat detection at machine speed. Future challenges include AI-physical infrastructure convergence, autonomous cyber warfare, and quantum/space security threats. Success requires embedding security into AI initiatives from inception, treating it as an enabler rather than a constraint on innovation.

Trend in action

While AI tools may be poised to transform service delivery, they introduce new challenges that will need to be managed. Forward-looking agencies are moving to embed security into their Generative AI initiatives. With efforts flourishing across organizations, departments are discovering that they need to identify Generative AI uses to prevent inadvertent data disclosures or other issues. Leading agencies are hardening their models against manipulation utilizing adversarial testing and training. With malicious actors turning to AI solutions, there is an increasing use of automated, AI-driven monitoring to detect and respond to incidents in real time. As threats such as autonomous cyber attackers and quantum risks increase, leaders should make security a foundational priority, develop plans for multiple scenarios, and maintain transparency around risks and benefits. Building security into every step can enable governments to seize the promise of AI while protecting against cyber risks and sustaining public confidence.

READINESS: 3

RELEVANCE: 5

Learn more

Follow

@DeloitteGov

Related reports

Tech Trends 2026

Authors

For questions regarding GovTech Trends 2026, please contact:

SCOTT BUCHHOLZ
Government & Public Services CTO
Deloitte Consulting LLP
sbuchholz@deloitte.com
+1 571 814 7110
@scott_buchholz

Deloitte.