The Agentic State

How Agentic AI Will Revamp 10 Functional Layers of Government and Public Administration

Whitepaper **|** Version 1.0 **|** May 2025

Lead Author **|** Luukas Ilves

Contributors **|** Manuel Kilian, Tiago C. Peixoto, Ott Velsberg

About this Whitepaper

Version 1.0 of this whitepaper represents a starting point, not a finished product. Rather than providing a fixed roadmap, its purpose is to stimulate discussion, challenge assumptions, and establish a shared basis for experimentation. The authors aim to work openly, iterate quickly, and learn alongside the wider GovTech community.

As the landscape of agentic AI in public services continues to evolve, so will this white paper in successive versions. In collaboration with practitioners, policymakers, technologists, and researchers shaping the next generation of government, we will expand, adapt, and refine it. We welcome contributions from anyone working on these challenges. If you would like to get involved, please email us at: contact@globalgovtechcentre.org.

About the Global Government Technology Centre Berlin

The Global Government Technology Centre Berlin (GGTC) is a pioneering initiative, launched in 2024 by GovTech Campus Deutschland and the World Economic Forum. A fellow Centre in Kyiv, Ukraine, has since been established.

The GGTC's mission is to help governments turn technology into tangible public value by connecting national GovTech ecosystems with a global network of experts from government, industry, and academia. This international collaboration helps to shape national strategies, define best practices, and accelerate the adoption of proven solutions.

The GGTC delivers impact through four core areas:

GovTech Agenda-Setting	Supporting public institutions through high-level dialogue, whitepapers, and strategic playbooks.
GovTech Networks	Bringing digital leaders together through a set of structured initiatives.
Intelligence and Insights	Sharing impactful, actionable research and deep analyses via the GovTech Intelligence Hub.
Upskilling	Making training programs for public servants accessible across borders.

Together, these areas enable governments to implement digital solutions more effectively, align on shared standards, and build the capabilities needed to deliver better public services in an era of rapid technological change.

Table of Contents

Executive Summary

This whitepaper explores how agentic AI will transform ten functional layers of government and public administration. The *Agentic State* signifies a fundamental shift in governance, where AI systems can perceive, reason, and act with minimal human intervention to deliver public value. Its impact on key functional layers of government will be as follows:

Layer	What agents do	What changes
🤖💬 Service Delivery	Tailor, fuse, and launch services in real time; speak any language and channel	Hyper-personal, inclusive services at near-zero marginal cost
⚙️🤝 Back Office	Digest messy data, decide along KPI targets, escalate only edge cases	Bureaucracy melts away; cycle-times and admin spend collapse with full auditability
🗄️🔒 Data	Stitch public and private data with fine-grained consent control	Privacy-safe insight everywhere. Policy, service, and market innovation accelerate
🚨🛡️ Crisis Response	Spot weak signals, simulate scenarios, launch machine-speed actions	Lives and assets better secured; AI-enabled national resilience
📜✅ Compliance	Scan live data, issue real-time compliance checks	Red tape eliminated; risk-based oversight that lets business grow
🏛️📝 Policy-making	Stress-test options, retune rules continuously, negotiate in real-time with markets	'Living laws' that stay precise, hit policy targets sooner, and cut societal drag
🎯👑 Leadership	Make performance visible; spotlight hidden risks	Strategic clarity and faster pivots; leaders steer by impact, not anecdote
👥🧠 Workforce and culture	Co-pilot routine tasks, upskill everyone to democratise access to tech	Humans focus on judgment and empathy, cultural change and organisational development accelerate
🏗️💻 Tech Stack	Orchestrate agents on modular stack from ID to compute	Elastic, low-cost government platform enabling new functionalities and oversight
🛒💰 Procurement	Auto-tender, negotiate, and pay purely for outcomes	Public money buys measurable results; SME-friendly cycles shrink to days

An Introduction to Agentic AI for Governments

The long-standing trend of 'software eating everything' describes a fundamental shift in which software-based solutions are replacing traditional processes, physical hardware, and even entire industries. The rapid advancement of AI is accelerating this trend and pushing its boundaries into areas that were previously considered to be the exclusive domain of humans. This is fundamentally altering the nature of what is 'being eaten'.

Previous rounds of digital transformation transformed industries by virtualising infrastructure (e.g. cloud and software at the core of hardware, from cars to radios), dematerialising products (e.g. music, films, and books) and processes (e.g. e-commerce and e-banking), and automating rule-based tasks (e.g. business process automation and robotic factories).

Generative AI, with its capacity to create novel and human-like content (e.g. text, images, audio, code, or synthetic data), is now 'eating' functions that involve complex cognition, creativity and understanding, such as content creation and communication, software development, customer engagement, data analysis, public administration, education, and research and development (R&D). In many executive, academic, public administration, and research-related roles, generative AI is already seeing widespread adoption.

AI agents take this a step further by introducing systems that can not only generate and analyse data, but also perceive, reason, and act with minimal human intervention. These so-called agentic systems can manage end-to-end processes, learn, self-optimise, and collaborate with humans and other agents (see table below for different types of agents).

Types of agents currently in use

Agent Type	Description	Examples
Information and Analysis	These agents specialise in gathering, processing, synthesising, and analysing information from diverse sources. Their primary function is to provide insights, answer complex queries, make comparisons, or offer decision support.	Agents performing product comparisons by browsing the web or personalised agents assisting individuals in making complex decisions, such as selecting insurance plans or educational institutions.
Task Execution and Automation	These agents are designed to perform specific actions and automate workflows within digital (and sometimes physical) environments. They follow instructions or pursue defined goals to complete tasks.	Agents that buy goods online, book flights, conduct software engineering tasks, or provide office support by managing schedules and documents.

Interaction and Communication	These agents focus on engaging with humans or other AI agents. Their capabilities centre on natural language understanding, dialogue management, negotiation, and facilitating collaboration.	Agents capable of making phone calls or engaging in complex interactions with other agents using specialised communication protocols to coordinate activities or make agreements.

Systems of agents, what we refer to as agentic AI, are predicted to take over tasks that previously required significant human oversight and judgement, such as software engineering, IT operations, human resources, finance, customer service, marketing, operations, and supply chain management (see figure below).

Job function groups with the highest exposure to generative AI[1]

Percentage of Tasks

Automation — Augmentation — Lower potential — Non-language tasks
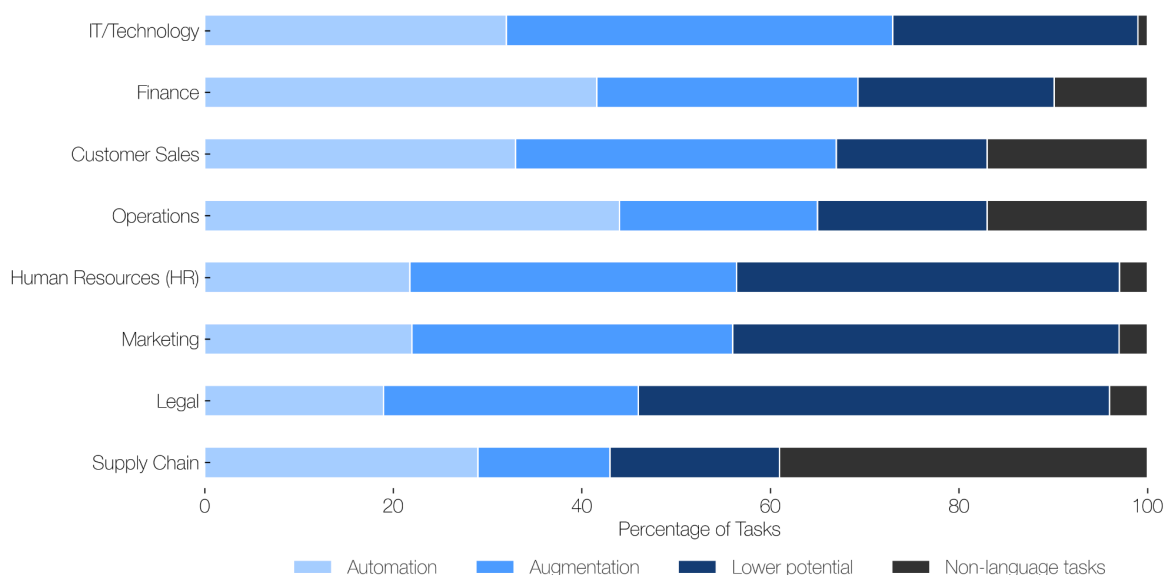
The Agentic State

The rise of agentic AI will have a particularly profound impact on government and public services, as well as the provision of public goods such as education and healthcare.

Previous rounds of digital transformation have altered the medium by government functions, replacing paper forms and physical front offices with online forms and apps or portals, but have not altered the fundamental organisational structure or business model of government.

This time will be different. Agentic AI's software will be capable of 'eating' the core functions of government. The *Agentic State* is not simply the automation of existing processes or the replacement of human rules with AI agents, but marks a shift in the nature of government and

---

public administration on par with the invention of the bureaucratic state in the 19th century (which was itself a reflection of the technological and organisational paradigms of the Industrial Revolution).

The *Agentic State* will be driven by outcomes, not process; customised and personalised, not consistent and formulaic; real-time, not predictable; and will orchestrate public goods without acting itself. The associated changes may be profound, presenting new risks, but they may well be inevitable if government and public administration are to maintain their fundamental role in delivering public value and serving the public interest.

A Blueprint for Transformation

This whitepaper breaks down the broad notion of an *Agentic State* into ten distinct functional layers of government, ordered across three dimensions:

Operations	1. Service Delivery and User Experience
	2. Internal Workflows
	3. Data Governance, Management, and Operations
	4. Crisis Response and Resilience

| Regulation and Governance | 5. Compliance and Reporting |
| | 6. Policy and Rulemaking |

Foundations	7. Leadership
	8. Workforce and Culture
	9. Tech Stack
	10. Public Procurement

For each layer, this whitepaper follows a common structure, moving from present realities to future possibilities, with key questions for reflection. Each section is structured around three components:

a. **How it (doesn't) work today:** An honest account of how the government and public administration currently operate, and where existing processes, technologies, or institutional norms fall short.

b. **A vision for agentic government:** A reimagined approach that leverages the potential of agentic AI to deliver public value in new ways, often by rethinking long-held assumptions.

c. **Key questions:** Critical reflections and practical considerations designed to support further debate and help substantiate the path toward realising the vision.

This format is designed to help practitioners and policymakers navigate the tension between today's world and the changes needed to make good use of agentic AI. The list of ten functional layers is neither exhaustive nor definitive. Rethinking how we model and think about public functions is itself a key step in transitioning to an *Agentic State*.

What is at Stake and What is Driving This Whitepaper

Collectively, the world's governments are falling short at delivering public goods. In high-income countries, overall public trust in government and quality of public services are in decline.[2] Emerging economies face a different challenge: the pressure to do more with less and to leapfrog to close the gap with wealthier states.

The human and economic cost of poor governance is staggering: trillions lost in misallocated resources, unmet needs, and institutional failure. Worse still, most governments are structurally brittle and poorly equipped to manage disruption. Their organisations and processes were designed for stability, not for a world of cascading geopolitical, technological, environmental, and social shocks.

Technology alone is no panacea. However, when paired with deep institutional reform, it becomes a powerful force multiplier. What creates public impact is not adopting tools for their own sake but linking technology adoption and transformation to public missions. The difference between governments that have mastered the use of technology and those that have not is not measured in single digit percentages, but in multiples of cost savings, operational efficiency and service outcomes.[3] And that is before factoring in the potential of agentic AI.

Government digital transformation is increasingly becoming a top priority in many countries. As governments undertake modernisation efforts, they must avoid the trap of committing significant resources solely to catch up with the present at a time when agentic AI is triggering a once-in-a-generation paradigm shift in technology, organisation and design. This whitepaper serves as a practical guide to grounding reforms and technology modernisation in the opportunities and challenges of the agentic age.

Factors for Successful Execution

There is no playbook or catalogue of best practices for adopting agentic AI in government. The technology is simply too new and developing too rapidly. Even the most digitally advanced

---

[2] OECD (2023): Trust in government (source)
[3] On this topic, see Ilves, L. (2025): The end of bureaucracy (source)

public administrations are only beginning to experiment. Many AI transformation efforts, as done today, are bound to fail.[4]

Public sector leaders can get a head start by looking to the private sector in four ways:

- **Learn from private sector AI adoption and use cases:** Enterprises are pouring billions into AI adoption and development. Their collective experience in coming years will yield a rich evidence base of best practices, useful lessons and empirical evidence on what works, and more importantly, what doesn't (yet) work. Governments should observe closely and copy what works.

- **Build with the private sector:** The past three years have seen a wave of new products to support enterprise AI adoption. Nearly every step of the AI development and adoption lifecycle has multiple providers offering models, tools, data, much of it open source. Instead of reinventing the wheel, public administrations should seek to build on what is already there and invite enterprises to collaborate with them.

- **Adopt new economic models:** Governments should increasingly treat agentic deployments not just as technical builds, but as performance-based services, paid for per transaction, per outcome delivered, or per marginal cost of serving hard-to-reach groups. This shift in pricing models can help align incentives, control expenditure at scale, and ensure that AI systems deliver public value, not just operational novelty.

- **Operate as a platform for private sector and individual invention:** Agents reduce the technical and skills barriers to accessing and building on APIs, datasets, and digital infrastructure like eID, allowing users to interact with government systems and data using natural language instead of technical interfaces or developer tools. Governments should extend and democratise their existing role as technical and data platforms, making these resources compatible with and useful to third-party AI agents operated by the private sector, civil society and even individuals.

The gap between rapid private sector AI development and slow government adoption also presents an opportunity. In economic sectors where public funding, infrastructure, data or standards are critical (health, education, energy, science, infrastructure, agriculture, construction, defence and public safety to name just a few), those governments that move faster will also create significant opportunities for private innovation, growth and export.

Assumptions, Caveats and Limitations

Assumptions and predictions about the capabilities of agentic AI are grounded in tools that are either already in use or in public development by leading AI companies and research organisations, as well as the initial findings from their adoption in the private sector. While it is

---

[4] Ryseff, J., De Bruhl, B., Newberry, S. (2024): The root causes of failure for artificial intelligence projects and how they can succeed (source)

relatively optimistic about the reliability and performance of evolving technologies, it does not speculate about breakthroughs beyond current capabilities.

The whitepaper also assumes a certain amount of structural continuity. Rather than imagining a radically transformed state or society, it builds on the existing functions of public institutions and the lived experience of today's citizens. It assumes that human biology, psychology and social structures will remain largely unchanged. It is intended as a guide for today's policymakers and practitioners, not as a vision of a transhumanist future.

Version 1.0 of this whitepaper does not cover several adjacent but critical topics in depth:

- A comprehensive societal vision for the agentic age, including the broader economic and social disruptions AI may bring.

- The impact of generative and agentic AI on politics, media, and the public sphere.

- Governance or regulation of AI, including AI safety and ethics.

- International and global collaborative approaches (e.g. standards, guidelines, digital public infrastructure, or interoperability) to pursuing the visions outlined here.

- Forecasts or timelines for technological developments or adoption.

- Environmental, supply chain, sovereignty implications of wide-spread AI use.

This whitepaper takes a horizontal view across core government functions. It is agnostic to specific policy domains (e.g. healthcare, social services, education, or justice), which are natural candidates for follow-on work. And it presents a snapshot in time, a reflection of present technological developments.

1. Service Delivery and User Experience

From fragmented portals to self-composing public services and personal concierges.

a. How It (Doesn't) Work Today

Users of public services, citizens and businesses alike, navigate fragmented portals, websites and forms, triggering digital services with varying levels of automation. For most public services, the user experience (UX) tends to be transactional and brittle. Standard cases follow rigid workflows, while anything outside the norm often results in manual handling and bureaucratic back-and-forth.

Some countries' public authorities have made significant investments into improving government UX over the past decade (such as design systems, modern user interfaces, user testing, product management, proactive services). The results of all this have been mixed. While there have been some great successes, such as the Gov.UK design system, there have also been failures and stalled efforts.

Recently, designing user-centric life events is becoming part of the standard playbook of digital government. This approach organises public services around key moments in people's lives, such as having a child, starting a job, or retiring, rather than around institutional structures. The goal is to deliver seamless, end-to-end experiences that reduce complexity for users.

While effective for capturing broad, predictable stages of life, the 'life events' model misses the granular, messy, and often urgent needs that define real user journeys. For instance, a 'birth of a child' life event may help parents register the birth and apply for leave or benefits. But it fails to adapt to more complex scenarios, such as a single non-citizen mom giving birth in a different jurisdiction, while facing housing insecurity and urgent healthcare needs. These edge cases typically fall outside the scope of predefined service bundles, forcing citizens to navigate disconnected systems on their own.

Generally, the current manual approaches to service design do not scale. Furthermore, good design requires significant upfront investment, particularly when coordination is needed across multiple layers of government and external partners. Labour is the main cost driver here. Even in small and digitally advanced countries like Estonia, revamping services for major life events, such as the birth of a child or business compliance, has cost millions of euros to design, build, and launch. These costs limit how broadly such efforts can be repeated worldwide.

b. A Vision for Agentic Service Delivery and UX

Digital-era UX limits users to interactions and service definitions defined in advance by humans, bottlenecked by the cost and friction of the (re)design process. Generative AI, by contrast, can compose novel interactions and services addressed to the specific needs and limitations of each user.

In contrast to the current, static 'life events' model, agentic AI unlocks the potential to go beyond this one-size-fits-all framework by dynamically composing services tailored to the individual's situation, preferences, and constraints. The widespread use of agents, whether directly by users or on their behalf by public authorities, will enable endlessly customised services at zero marginal cost.

In this new paradigm, agentic public services will be characterised by:

Personalisation and multi-modality: As a first step, service interactions will become more tailored to individual preferences. User interactions can be customised in real time to any language and offered consistently across different modalities, channels and devices (e.g.

browser, app, text message, phone call, video avatar, AR/VR headset, brain-computer interface). Tone and emotion can be adjusted to circumstances and cognitive styles (warm and effusive conversation for one person, austere recitations of rules and processes for another). Multimodality will support universal coverage (e.g. monitoring detects a user struggling partway through an online benefit application and proactively offers a support call).

Proactivity: Proactive government services today usually rely on fixed rules or triggers, such as sending reminders when a deadline is approaching. By contrast, agentic services will be far more responsive and personalised. For instance, an AI agent could identify individuals who would benefit from a new training programme and contact them directly. Over time, the system could learn which types of messages work best for different people and adapt its approach accordingly.

Ideally, AI-driven public services should help close social and economic gaps. Unlike human systems, AI Agents can apply inclusive rules more consistently, taking into account things like different levels of digital skills, disabilities, cultural backgrounds, or income. With the right safeguards, they can also be designed to detect and correct unfair patterns as they go.

Agents can also unlock a form of public sector cross-selling. In contrast to the private sector, which routinely leverages touchpoints to suggest relevant actions, services, or upgrades, governments typically treat interactions as single-purpose. But agents, operating with contextual awareness and public intent, could prompt citizens toward beneficial next steps: notifying them of available programs they are likely eligible for, inviting participation in local decision-making, or surfacing rights and responsibilities they may not be aware of. A request for a permit could also prompt an offer to update business registry information; a tax filing could be paired with a participatory budgeting invitation. Done well, this kind of value-aligned upselling could enhance inclusion, transparency, and engagement, without becoming intrusive.

Self-composition: Instead of hand-building 10 or 30 standardised life events, public administrations will be able to compose tailored services for each citizen and business. Every life path is unique: a home birth followed by an emergency hospitalisation in a rural municipality is very different from an unmarried refugee giving birth in a city hospital; similarly, the insolvency of a startup founded by a serial founder differs profoundly from a multi-generational family firm going out of business during a recession.

On top of defined rules (i.e. laws and regulations) and resources (i.e. budgets, support thresholds, and reimbursement amounts), agents will be able to compose public, and also private, microservices into seamless, end-to-end offerings. Citizens simply state intent, and agents resolve full service flows dynamically. For example: "I need help after my house was damaged in a storm" could trigger an agent dynamically assembling the relevant services, including filing insurance claims, applying for relief funds, scheduling inspections, by connecting banks, insurers, construction firms and government agencies in one unified process.

c. Key Questions

Is this a continuation or a reset? Does it make sense to continue along the familiar linear path of UX, refining life events one workflow at a time? Or does agentic AI require a radical reset, starting from scratch to avoid perpetuating legacy assumptions?

Who will build the agents, and who will govern them? Multiple models will likely coexist. Governments could develop their own trusted agents on behalf of citizens. Alternatively, users may rely on personal agents built by large platforms such as OpenAI, Google and Apple, or they may run their own. Should governments treat these agents as endpoints, like browsers, or build for direct orchestration?

What happens when only some citizens can afford the best agents, trained on privileged data and optimised through constant feedback? Agentic systems raise critical questions about equity. If only some citizens can afford high-quality agents, will access to public services become unequal? What obligations do governments have to ensure fair access, and what technical or institutional tools could guarantee this? Should governments provide open APIs, agent testing environments, or even baseline public agents to prevent capability capture by private actors?

How do we avoid going too fast or over-promising? What causes early AI deployments to falter [5], and how can governments avoid similar pitfalls in critical public functions?

What developments will help agentic UI and services comply with high legal standards for public services? What can we learn from risk aversion and guardrails (in the form of e.g. filters, templates, or silos) that have limited the usefulness of user-facing public sector Large Language Model (LLM) deployments so far?

2. Internal Workflows

From manual casework to outcome-driven agents with humans on the loop.

a. How It (Doesn't) Work Today

Governments are infamous for their process inefficiencies. Public servants are often their own worst critics: 94 per cent of UK civil servants reported process inefficiencies in a recent survey[6]. Digitisation has often replicated broken, siloed paper processes in digital form, resulting in little

---

[5] On this topic, see the recent developments at Klarna: Fortune (2025): As Klarna flips from AI-first to hiring people again, a new landmark survey reveals most AI projects fail to deliver (link)

[6] Appian (2025): New Data Shows UK Public Sector Burdened with 30.6 Million Hours of Extra Work Every Week (source)

more than the 'PDFication' of bureaucracy, without meaningful automation, time savings or user benefit.

Many internal workflows are resistant to traditional, deterministic business process automation (BPA). They often require human judgment, discretion, or contextual reasoning, e.g. eligibility decisions, exception handling, or prioritisation. Others are constrained by incomplete or inconsistent data, with critical inputs scattered across legacy registries, PDF attachments, or unstructured case notes. These limitations make end-to-end automation difficult and often impractical when using conventional tools.

b. A Vision for Agentic Internal Workflows

Generative AI is already being used to augment the internal tasks of bureaucracy, from drafting and analysis to reporting, document processing, and coding. Benefits are even greater when AI assistants can pull on in-house proprietary data. As in any enterprise, this will allow civil servants to work more efficiently and productively across a wide range of responsibilities.

But AI agents' potential goes beyond individual productivity. AI agents can help fix broken internal workflows and government back office processes, working around inefficiencies without the need to achieve perfect data integration or process standardisation. Their capabilities include:

Working with imperfect and unstructured data: Governments often hold vast amounts of critical information in non-standardised formats, such as scanned PDFs, legacy databases with inconsistent schemas, handwritten notes, or free-text case files. AI agents can be trained to interpret and reason over unstructured, heterogeneous data, reducing the need for large-scale pre-processing or data cleansing.

Automating for outcomes: Agentic government will come into its own as teams of AI agents become more capable of delivering on specific, measurable objectives, enabling them to contribute to achieve high-level outcomes. These agents will orchestrate complex workflows, intelligently breaking down high-level goals into smaller, executable tasks. They will autonomously interact with diverse systems, data sources, and APIs, coordinating across organisational silos. Crucially, they will monitor progress against defined metrics and adapt their approach to stay aligned with the target outcome.

Navigating complexity and intentions: Public sector workflows often involve a degree of discretion, interpretation of complex regulations, or handling numerous edge cases, these are scenarios where rigid, rule-based automation typically fails. Outcome-focused agents offer a new model. Rather than following fixed processes, these agents can be designed to understand policy intent, navigate procedural variations, and apply nuanced judgment to a wider range of situations, with only the most complex or novel cases escalated to human experts. This adaptability is crucial in domains where achieving universal process standardisation is unrealistic.

For instance, agents designed to automate for outcomes while navigating complexity and policy intent might be tasked to:

- *Approve 90 percent of construction permits within ten days while rigorously enforcing zoning and climate standards.*
  An agent assigned this task would orchestrate the full workflow, from document ingestion and rules-checking to issuing the draft permit, all while adjusting its approach on the fly to meet performance metrics.

- *Issue new business licences in real time, contributing to a 75 per cent reduction in new business setup times.*
  Here, the agent would coordinate API calls, verify documentation, reconcile data, and send notifications.

- *Process routine benefit claims with over 97 percent accuracy and generate automated, plain-language explanations for decisions.*
  The agent would handle end-to-end adjudication, flag outliers, and track its clarity and accuracy metrics over time.

Instead of manually pushing cases, civil servants shift to supervisory roles, managing exceptions, overseeing high-value decisions, and defining or refining the outcome metrics that guide automated agents handling routine eligibility checks, approvals, and adjudications.

This shift would also bring important secondary benefits: In areas historically susceptible to corruption or rent seeking, fully logged, agentic decisions aligned with fair and transparent outcomes reduces opportunities for discretionary abuse. At the same time, workflows driven by outcome-based agents can continuously learn and optimise for efficiency, compliance, and fairness based on their performance against the target metrics.

c. Key Questions

Which workflow earns the 'first-pilot' slot, and why? How do we balance high pain points, data readiness, and political capital when choosing the inaugural end-to-end agent deployment?

How should the safety net work at scale? What confidence thresholds, break-glass rules, and escalation paths keep humans responsibly in charge without stalling efficiency gains or inflating costs?

What kind of changes to management practices are needed for the shift to an AI-native operating model? Leaders will need to orchestrate hybrid human-AI teams and focus on their combined effectiveness.

What are the canonical Key Performance Indicators (KPIs) and quantifiable goals for an agentic government? What are the right metrics to measure success in agentic government — in terms of domain-specific outcomes and operational performance, such as time-to-service, cost per transaction, public trust in digital services, and compliance lag (the time between a law's passage and its full implementation)?

At what point do we consider the agent's output to be a legitimate public act? In many bureaucracies, proxies (e.g., interns, staffers, accountants) already complete official work that is formally signed by a responsible civil servant. But agentic workflows blur this distinction. What mechanisms will governments need to ensure delegated legitimacy, such as agentic power-of-attorney models, and how should they define when, how, and under what conditions an AI-generated action is considered authoritative and binding?

How to avoid unnecessary overheads? At what point does human-in-the-loop become not a safeguard but an unnecessary overhead, and a costly reflex that undermines agentic efficiency without adding real value? Are there domains where insisting on human review should itself be justified?

Should the 'right to a human' be absolute? Or should it come with trade-offs, such as longer adjudication times or a threshold cost, to avoid overuse that could erode the viability of automated systems?

3. Data Governance, Management, and Operations

An operational asset for agents and a strategic asset for society as a whole.

a. How It (Doesn't) Work Today

Managing information has long been a core function of government. Accurate, timely and well-governed data is essential for effective public services delivery and the government's decision-making processes leading to better policies.

Data is also one of the government's core platform offerings. The public sector plays a critical societal role in organising, certifying and making accessible the information that modern societies and economies need. This is exemplified by institutions such as public libraries, statistics bureaus, property and business registries, copyright offices and open data repositories.

Governments have struggled to keep pace with the exponential growth and complexity of *Big Data*, which makes up the vast, diverse and rapidly flowing streams of information that underpin

modern AI. Most governments have focused on managing structured register data (i.e. *small data*), the immense potential of *Big Data* has largely remained untapped.

Even when the technical foundations are in place, many governments fail to make meaningful use of their data assets, held back by gaps in leadership, skills and mindset. In the UK, for instance, 45 percent of public sector organisations still lacked a formal data strategy in 2023, while 73 percent kept their most valuable data on-premises, thereby limiting access and integration.[7]

b. A Vision for a Data Layer Supporting Agentic Government

Over the past decade, AI has reshaped our understanding of what is considered 'high-value' data. By enabling AI agents, all data becomes high-value. Information hidden in unstructured data becomes analysable and actionable. Viewed in aggregate, a nation's data merits treatment as a core strategic asset and national infrastructure on par with health, education, transport, or energy.

Enabling agentic government requires a fundamental update in how the public sector governs and uses data:

Storage, computation and interoperable sharing: For both training and operational purposes, public administrations must secure real-time machine access to vast, diverse data pools, including records, documents, images, sensor streams, and logs. Governance measures, including privacy protections and purpose restrictions, are fine-grained, applied not to entire datasets but to individual fields and rows. Access and usage are governed by policies that evaluate each specific query and use case.

Ecosystem-level data fabric: This allows AI agents to integrate public data with consented private sector data. For instance, combining real-time log data across government entities and critical infrastructure could enable earlier detection of coordinated cyber attacks. These real-time data flows are the lifeblood of these agentic workflows, enabling live insights and responsive services to be offered both by public and private actors.

Identity: Unique, standardised identifiers for individuals, locations, legal entities, and physical assets help AI agents develop a holistic and accurate understanding of the entities they interact with. Such an identity framework also ensures the 'once-only' principle can be effectively extended to AI-driven interactions.

Metadata: Rich, machine-readable metadata provides essential context for each data asset. This extends beyond basic descriptions to include clear usage policies, data quality indicators, and a complete audit trail (so-called *lineage*) of how data has been generated and transformed. This makes AI-driven government decisions explainable, auditable, and trustworthy.

---

[7] Source: Hewlett Packard Enterprise (2023): House of data - public sector data strategy report 2023 (link)

Agent infrastructure: Beyond individual data elements like identity and metadata, enabling an effective agentic government requires so-called *Agent Infrastructure*[8]: the technical backbone governing how AI agents interact with their environment, each other, and human institutions. Such infrastructure must support 'attribution', i.e. linking agent actions to responsible entities, shape agent interactions to be safe and efficient, and provide mechanisms to detect and remedy harms.

Openness: An 'open by default, closed by exception' stance should guide data policy. Public datasets, metadata, logs, source code, models, training data, and even weights should be made available wherever possible. This allows citizens, businesses, and oversight bodies to understand how AI systems inform government decisions, fostering public trust and democratic legitimacy. Widespread openness further accelerates innovation by enabling academia, private companies, and civic technologists to build upon government AI work.

Data commons: Governments can host the creation and stewardship of high-value, curated (multi)national training datasets to support responsible AI developments. These include collections of local-language text (e.g. public documents, service interactions, or educational materials), annotated public health images, depersonalised legal or administrative texts, and satellite imagery. These should be permissively licensed for use by academia, domestic AI vendors, and public sector innovators, with guardrails in place to protect privacy and prevent misuse.

Two cross-cutting practices are essential to make all this work:

1) Data Product and service management: Every major public dataset (such as core registries, key operational data streams, or critical unstructured information) should be treated as a distinct data product or service, with a designated public steward, public quality standards (e.g. for freshness, accuracy, and bias), and automated reliability monitoring. This ensures government agents operate trusted, well-governed inputs.

2) Agents as data scientists: AI agents can augment the government's limited data science capacity by autonomously analysing patterns, generating insights, and surfacing anomalies, helping to overcome the scarcity of human data scientists.

One frontier role for public sector agents is acting as *data fiduciaries* for individuals — not merely querying data but maintaining dynamic personal models that help citizens interact with the state. Just as banks maintain financial models for creditworthiness, public agents could maintain administrative models of eligibility, preference, and risk, continually updated with consent, and used to streamline interactions with public systems. This shifts the burden of data navigation away from citizens and toward agentic intermediaries operating under fiduciary obligation.

---

[8] Source: Chan et al. (2025): Infrastructure for AI Agents (link)

What the Private Sector is Doing with Data

Embed computation next to data rather than shipping data out.

Data governance and use in enterprise settings are rapidly growing more sophisticated and complex. Here is a snapshot of tools and practices currently gaining broad traction:

Data as a product and data contracts: Beyond just being a resource, data assets are managed like commercial products. Each 'data product' (e.g. a specific dataset or real-time stream) has a designated owner, a publicly defined schema, and service level agreements (SLA) detailing its quality, freshness, and reliability. 'Data contracts' formalise these terms between data producers and consumers, with automated tests ensuring compliance.

Real-Time API fabrics and event streaming: The paradigm has shifted from slow, periodic batch data transfers to live 'event streams' and API-first architectures. This enables AI agents, applications, and analytical systems to access and react to data instantly. Technologies like *zero-copy sharing* allow secure, live access to data across organisational boundaries without costly and risky physical duplication.

In-platform governance with automated lineage and policy: Modern data platforms embed governance directly into their architecture. *Data lineage* (tracking the origin, transformations, and usage of data at a granular level) is captured automatically. Access controls, privacy rules and usage policies are enforced programmatically and continuously, making compliance auditable by design rather than an external check.

Privacy-enhancing technologies (PETs) for secure collaboration: To collaborate on sensitive data without compromising privacy or commercial confidentiality, enterprises use PETs. *Secure Data Clean Rooms*, for example, provide controlled environments where multiple parties can pool and analyse their data (or run AI models on it) without any participant seeing another's raw data. An example could be researchers running analytical code where sensitive census microdata lives, receiving only aggregate, anonymised results. *Federated Learning* allows AI models to be trained on decentralised datasets (e.g. across different hospitals, or company branches) by sending the model to the data, learning locally, and then aggregating insights centrally without exposing the source data. Other PETs, like *differential privacy* and *homomorphic encryption*, are also gaining traction.

Curated corpora and synthetic data for generative AI: Enterprises strategically invest in creating high-quality, specialised datasets, or *corpora* (e.g. internal documents, customer interactions, research notes) to finetune foundation models for their specific industry and tasks. They also increasingly use Generative AI itself to create realistic synthetic data when real-world data is scarce, sensitive, or imbalanced.

c. Key Questions

Where do we draw the privacy–utility line in an agentic world? As AI agents learn and act in real time, how should we govern access to sensitive data? What determines whether a dataset should be open, restricted to clean-room environments, or closed altogether, and who defines the rules of use at the speed of automation?

When do you build on what you have vs. when do you start over? Should governments incrementally adapt legacy data infrastructure, or is now the moment for deeper re-engineering? What is the tipping point between patching what exists and building what is truly needed for AI agents at scale?

Why have so many previous data strategies failed to stick politically? Despite countless initiatives, data often remains an afterthought in digital transformation. What makes it so hard to mobilise leadership around foundational data work?

How do we prevent openness from becoming a vulnerability? 'Open by default' is a powerful norm — but how do we prevent malicious use of openly accessible logs, models, or weights?

Which types of data sharing maximise third party innovation? What is needed for this, terms of content, format, and delivery infrastructure?

4. Crisis Response and Resilience

From legacy responses to agentic readiness in an era of polycrisis.

a. How It (Doesn't) Work Today

When *force majeure* hits, whom do you turn to? Responding to large-scale emergencies is one of the original tasks of government and remains a core function in every policy area, from defence and public safety to financial markets and public health. Yet today's emergency systems are struggling to keep pace. Most governments still rely on siloed command structures, manually updated dashboards, and *human-in-the-loop*-focused decision-making. Coordination across agencies is slow. Real-time data often does not exist. When it does, it is fragmented across systems, underused, or too complex to process and act on quickly.

This would be challenging in any environment, but especially so given today's extraordinary complex challenges. We are in an era increasingly characterised by *polycrisis*: interconnected and cascading shocks ranging from pandemics and extreme weather events to cyber-physical attacks, financial instability, disinformation campaigns and even conventional warfare — traditional crisis management models are under strain. Threat actors are already adapting. With AI, they can automate, scale, and personalise attacks at unprecedented speed. Governments,

by contrast, are often still operating with institutional reflexes shaped for a slower, more linear world.

b. A Vision for Agentic State Resilience

In a world increasingly shaped by AI, the best form of preparedness is to excel at using AI. Agentic government means equipping the state with intelligent systems that can anticipate, respond, and adapt across the entire crisis lifecycle: from prevention and preparedness to response, recovery, and continuous learning. In an environment where threat actors are already leveraging AI to disrupt and destabilise, governments must match speed with greater speed, and intelligence with higher intelligence.

Resilient statecraft in an agentic era will depend on the following capabilities:

Predictive early warnings and proactive preparedness: AI systems trained on global and hyperlocal data streams identify precursor signals and provide warnings with actionable lead times. AI agents simulate a near-infinite variety of virtual stress tests. The already overwhelming fire hydrant of data turns into a tsunami. AI is crucial for maintaining a signal-to-noise ratio. Otherwise, meaningful decision-making, resource allocation, prioritisation and cross-agency coordination break down.

Simulation infrastructure: Governments should treat simulation infrastructure as critical public infrastructure. Agentic models can continuously simulate crisis scenarios across domains, producing synthetic datasets that reveal systemic fragilities. More than stress tests, these simulations become generative foresight mechanisms. Similar to how flight simulators improved aviation safety, crisis simulators, if public and participatory, could preempt cascading failures in everything from climate to supply chains.

Hyper-aware AI-orchestrated first response: When a crisis begins to unfold, AI initiates the first steps in crisis response before *human-in-the-loop* structures have time to react. What is already happening today in technical domains like automated distributed denial-of-service (DDoS) attack mitigation will be increasingly used for complex tasks. This ranges from raising alert levels and dispatching repair teams to fielding inbound help requests and managing initial public communication. These agents will work alongside increasingly autonomous physical systems such as drones and robots, forming the backbone of a responsive, adaptive crisis infrastructure.

Coordinated machine-speed response: Governments will not be the only actors fielding AI agents. Private firms, NGOs, and even individuals may deploy agents to assist or intervene in emergencies. At best, this enables the entire ecosystem to respond at machine speed. At worst, uncoordinated agents will work at cross-purposes and undermine a coherence response. Avoiding this scenario will require new technical and institutional protocols for agent alignment, coordination, and conflict resolution.

Human-on-the-loop: Human oversight will increasingly move from making decisions to supervising them. This shift may feel uncomfortable, but those who let machines take the first step, especially in fast-moving situations, will gain an edge, with mental capacity freed up for critical thinking under pressure.

c. Key Questions

How do we harden information supply chains and models against adversaries and outages? What safeguards detect spoofed and poisoned data or autonomy? And how do agentic systems respond when networks degrade or go dark?

What does operational resilience look like at machine speed? Can agents function safely and effectively in degraded environments or under contested conditions, and how do we design for 'graceful fallback'?

Can governments develop a shared doctrine for agentic crisis management? Do we need new playbooks, rules of engagement, or even treaties that define how autonomous systems coordinate in multi-actor emergencies? What would shared operating principles between allied agents, public and private, look like in practice?

How can we prevent agentic lines of defence from escalating crises unnecessarily? For example, how does misclassifying intent or triggering automated countermeasures in response to ambiguous signals not lead to escalation? What governance mechanisms can ensure that autonomous protection does not become a source of provocation or geopolitical miscalculation?

5. Compliance and Reporting

Continuous compliance that preserves confidentiality and supports lighter regulation.

a. How It (Doesn't) Work Today

Across most countries, the number one demand from businesses is clear: reduce bureaucracy and administrative burden. The cost of compliance and reporting is enormous and, for example in the European Union, amounts to as much as 3.5 percent of GDP.[9] It weighs heavily on small businesses and large corporations alike.

Furthermore, the entire compliance, certification, and reporting apparatus is outdated and poorly suited to its intended purpose. Periodic inspections and static documentation offer, at

---

[9] Source: European Commission (2006): Measuring administrative costs and reducing administrative burdens in the European Union (link)

best, a limited snapshot of compliance at a single point in time, often incentivising box-ticking rather than meaningful adherence. A certification may only tell us a company was compliant on one day, two years ago. Even well intended 'risk-based approaches' are only partially successful, introducing complexity and legal uncertainty as to whether a given company's measures meet requirements.

The system is not working for regulators either: They face information overload from reporting requirements. Financial supervisors, for example, must sift through thousands of transactions or reports hoping to spot anomalies, which is a needle-in-haystack exercise. In many cases, violations are uncovered through whistleblowers or random audits, not through a systematic screening.

Let's be clear: the purpose of these rules and regulations are not in question. From clean air and water to safe workplaces and stable markets, the public interest rationale is strong. These rules correct for market failures and protect people. The real problem lies not in the regulatory intent, but in its execution.

b. A Vision for Agentic Compliance and Reporting

Compliance monitoring and reporting is one of the most obvious cases for agentic AI. When let loose on the real-time internal data of any enterprise, an AI agent can outperform human compliance officers on every of the following dimension:

Thoroughness: Agents can examine the full picture of enterprise data, gigabits per second streams, to discover risks. Unlike existing solutions for algorithmic monitoring and fraud and risk detection solutions, it can also formulate novel hypotheses and expand its input data as needed.

Managing complexity: AI can act as compliance copilots. They can ingest new rules and regulations, map them to enterprise systems, and highlight where necessary changes, exceptions or trade-offs are needed.

Real-time validation: Instead of depending on quarterly reports or scheduled inspections, a statement of conformity becomes a live reflection of the present. Compliance is no longer a retrospective snapshot; it is an active, up-to-date status.

Minimal disclosure, maximal assurance: Most government regulators do not need full internal datasets — they just need to know whether a company is compliant. A well-governed AI compliance agent, running on a verifiable, tamper-resistant algorithm, could issue YES/NO compliance attestations without transmitting sensitive internal data. In this model, reporting becomes proof, not just paperwork.

Cost-reduction: All the above measures save time and will be increasingly automatable, feeding into cost-reductions for both companies and regulators alike.

On a broader level, agentic compliance will enable **emergent ecosystem benefits**. Many regulations are built with significant safety margins to compensate for imperfect compliance. With more precise, real-time monitoring and verifiable reporting, regulators could cautiously recalibrate requirements toward socially optimal levels. In the long run, we can envision a situation where compliance in domains like health, safety, financial, environmental, cybersecurity, and ethics become a component of overall quality management, with less, not more, internal information crossing organisational boundaries.

c. Key Questions

What lessons can we take from early AI use in fraud detection? Machine learning has been used in financial supervision and anomaly detection for years. What worked, and what failed, in those efforts that can inform the next generation of agentic compliance systems?

How do we design compliance agents that are both universal and contestable? What standards for audit trails, appeals, and oversight are needed to ensure that small businesses and multinationals alike trust the system? And that regulators can enforce decisions with confidence and due process?

Where should we draw the line on automated enforcement? If AI agents can issue fines or trigger legal action in real time, what safeguards are needed to prevent runaway enforcement or unjust penalties? What role should human oversight play in preserving legitimacy?

How can governments lead by example? How might the public sector apply agentic compliance tools internally, for monitoring procurement, ethics, or anti-corruption rules, before asking others to follow suit?

6. Policy and Rulemaking

From static rulebooks to living policies, continuously monitored and adapted by AI agents.

a. How It (Doesn't) Work Today

Lawmaking and regulatory rule-making typically operate on slow, reactive cycles. Policies are drafted, debated, decided upon, and only then implemented. Once enacted, they often remain static for long periods, even as conditions change. Updating them usually requires new legislation or a full regulatory process, which are both costly and time-consuming. As a result, many regulatory actors understandably prefer stability over adaptability.

This rigidity leads to critical mismatches. Benefits formulas and tax codes lag behind economic realities; environmental thresholds may fail to reflect the latest scientific data. When law adjustments are made, they are usually based on retrospective data, political compromise, or expert judgment, rather than real-time feedback.

b. A Vision for Agentic Policymaking

In a world where agentic AI is fully embedded in government, the very fabric of governance can change. Laws, currently static code written once and amended rarely, can develop into a far more dynamic living system, continuously interpreted, tested, and refined by agents operating within clearly defined public mandates.

The idea of 'law as code' is not new, but an agentic government will have the capability to rewrite laws as easily as agents rewrite code. AI agents can simulate complex systems, run policy scenarios, test and red team alternative designs at staggering volume and speed; where quantum computing will unlock a further leap. Moreover, AI can course-correct 'at runtime', detecting drift, bias, and systemic failures.

This opens the door to far more dynamic systems of regulation and legislation, where broad societal goals are set by humans (legislators), while specific rules, thresholds and requirements are adjusted dynamically by agents with limited or no human intervention. Much of the current content of laws and regulations (and the time-consuming process of legislation) could be replaced by mandates for agents to achieve outcomes.

This shift will be most profound in areas where public and private sector agents can collaborate and negotiate. In regulatory areas such as environmental protection or financial services, public agents embodying public mandates and goals could negotiate with private agents in sophisticated, real-time markets for risk, emissions, or compliance. A city, for instance, might task its agent with minimising the total financial cost of reducing particulate pollution below health-critical thresholds, while a financial regulator might permit firms to offer higher-risk products, provided that systemic risk remains within acceptable bounds.

Agentic policymaking challenges contemporary notions of inclusion and participatory decision making, but need not be less democratic. Rather than operating solely through top-down regulatory adjustments, agentic policy systems could also learn from citizen signals. Feedback loops, such as appeals, time-to-resolution metrics, or even emotion detection in digital interactions, could become inputs for agent-guided policy refinement. In this model, the boundary between policy implementation and adjustment becomes porous: agents adjust rules not only based on macro-level KPIs but also from bottom-up input and friction indicators.

Realising this vision will require governments to update legal and governance frameworks to ensure continuous, transparent oversight of agentic services and rules. Key elements of such a framework might include:

- **Chain-of-thought logging**: Every agent decision must be traceable back to reasoning steps.

- **Fallback mechanisms**: High-risk decisions must allow human contestation or override at runtime.

- **Identity binding**: Every agent must be legally linked to a responsible person or institution.

- **Public outcome metrics**: Services must report fairness, error rates, and service quality over time, not only at launch.

c. Key Questions

Where can governments safely begin experimenting with dynamic, AI-assisted policy adjustment? While full automation of policymaking is not the starting point, what are the most appropriate early-use cases for AI-assisted adaptation? Could executive agencies, which already operate below the level of legislative decision-making, serve as testbeds?

What kind of (democratic) oversight preserves legitimacy? What combination of public dashboards, citizens' juries, or parliamentary committees legitimises continuous parameter updates?

How do we test and rollback self-adjusting rules? What simulation standards, validation thresholds, and legal rollback procedures apply when a digital-twin-driven change misfires?

How do we harmonise agent-driven policy across borders? When neighbouring jurisdictions adopt at different tempos, how do we prevent regulatory arbitrage yet respect sovereignty?

If evidence-based policymaking and 'law as code' have struggled to gain traction, what makes agentic policymaking different to succeed? Why should we expect it to succeed where those earlier efforts have struggled to take hold?

7. Leadership

The skills and behaviours of outcome-driven government leaders who will build agentic states.

a. How It (Doesn't) Work Today

For three decades, digital transformation has reshaped leadership expectations and operational norms in high-performing enterprises. But a governance gap persists: Many governments are still a generation behind with their leadership practices. Civil service and political leadership alike struggle to adapt to the digital world around them.

Two intertwined challenges stand out in the current situation:

First, political and administrative leaders continue to treat technology and digital systems as siloed support functions. Data and even AI are seen as technical or back-office concerns, disconnected from the core public service mission and strategic objectives. In some cases, digital illiteracy is not just tolerated but effectively rewarded, both in senior civil service appointments and at the ballot box.

Second, governments have been slow to adopt broader leadership and management best practices that have become standard in high-performing organisations, a trend often highlighted in analyses by organisations like the OECD and public sector consultancies. These best practices include rigorous data-informed decision-making, disciplined performance management based on meaningful metrics for both process and outcome, and agile methodologies focused on iterative value delivery, and a relentless focus on clearly defined outcomes.

This foundational leadership and management deficit contributes to a misalignment between technological capabilities and government priorities, and perpetuates organisational dysfunctionalities.

b. A Vision for Outcome-Driven, Agentic-Powered Leadership

The surge in generative and agentic AI means that expectations of leadership change and become more demanding: Enterprise leaders are increasingly expected to navigate AI's potential to reshape entire business models, manage hybrid human-AI teams at scale, govern systems with emergent properties, and drive innovation at an accelerated pace. We should expect no less of government leaders. This fundamental shift does not exempt government leaders.

Leaders understand that agentic AI reframes how the state must conceive of itself. As systems that reason, act, and learn autonomously begin to take on core functions, public sector leaders must confront foundational choices about where the state should act, and how.

In this paradigm, leadership is no longer just about delivery. It is about designing the posture of the state. In this regards, leaders must be conscious of the new key questions they need to address:

- **Investing or divesting:** Scarce resources, including compute, talent, and institutional focus, must be intentionally directed toward public goals where automation can deliver the greatest value. Not all functions should be scaled equally; prioritisation becomes a strategic act.

- **Regulator or deregulator:** Rules are no longer only enforced, they are encoded. Leaders must determine how policies are embedded into systems, and under what conditions those systems can adapt dynamically based on performance, confidence levels, or local variation

- **Central orchestrator or federated enabler:** Leaders must decide which powers remain centrally coordinated and where to enable autonomy — whether through local institutions, regulated non-state actors, or even citizen-controlled agents. These structural decisions will define how flexible, resilient, and trusted the *Agentic State* becomes.

These are not merely technical or organisational decisions. They are acts of public judgment and political design. The challenge is how to lead like an *Agentic State*: to govern with clarity, constraint, and intentional absence. This means designing not only for effectiveness, but for discretion, knowing when not to act, when to yield, and how to create space for autonomy without losing legitimacy.

In this era, key strategic imperatives for government leaders will include:

Defining public value and strategic intent: Leaders should define clear societal outcomes and public value in a way that can be handed over to AI agents, while also recognising when automation has failed. This process begins with a personal commitment to learning about AI.

Ensuring ethical, democratic, and accountable governance: Leaders should establish and enforce robust ethical frameworks for all public sector behaviour, both human and AI, rooted in democratic values, human rights, and public trust. They mandate transparency, fairness, human oversight, and clear accountability mechanisms for all AI deployments, while also 'working in the open' to build transparency and public trust.

Leading people and organisations through transformation: The human dimension remains ever more critical to leadership. It requires all the leadership traits that bring critical judgment, creativity, empathy, and risk-taking to the forefront in human teams.

Additionally, effective leadership of agentic AI in the public sector will recognise that AI and humans require complementary but distinct leadership skills:

Agentic AI performs optimally when directed by clear, measurable outcome metrics and unambiguous strategic intent provided by leadership. This is because it has the capacity for autonomous execution and optimisation.

Humans, especially when dealing with complicated change and working with AI, need leaders who can provide emotional intelligence, encourage open and clear communication, and leave room for experimentation, learning from mistakes, and quick iterations within the strategy.

c. Key Questions

What requires political leadership? And where can senior civil servants lead the way?

Which aspects of agentic transformation require elected leaders to set direction and provide democratic legitimacy? Where can senior public executives lead change independently, without waiting for political mandates?

How do we grow a generation of AI-native public leaders? What kind of training, mentorship, and career pathways will equip tomorrow's leaders to steer agentic government, blending technological fluency with public purpose, systems thinking, and ethical reasoning?

How do leaders define strategic intent in a way that AI can act on and humans can rally around? What does it mean to set a 'machine-readable mission'? How do leaders craft goals that are precise enough to guide AI agents, yet inspiring and flexible enough to motivate human teams?

Do we need a new leadership archetype for the agentic AI era? Is it time to replace, or evolve, the role of the government CIO? Should governments appoint Chief AI Officers with the authority to integrate AI across operations, ethics, and strategy?

8. Workforce and Culture

Towards broad tech fluency, elite talent, and high-performance culture.

a. How It (Doesn't) Work Today

The structures, cultures and workforce practices of the public sector have not kept up with the increasing dynamism of modern organisational forms:

Outdated career models and rigid HR structures: Government HR systems often prioritise lifetime careers, rigid job classifications based on credentials rather than agile skills, and slow, bureaucratic hiring processes. This makes it difficult to attract, develop, and retain talent with expertise in cutting-edge digital, data, and AI expertise, who are often undervalued and underpaid compared to the private sector. Career progression for technical specialists outside of traditional managerial tracks is often limited.

Cultural inertia and misaligned incentives: A risk-averse, process-driven culture often stifles the experimentation and iteration that are essential for AI development. Political and bureaucratic incentive structures rarely reward long-term technology transformations.

Structural immobility: Unlike the private sector, where companies face constant competitive pressure to evolve, public sector agencies are infrequently reorganised and almost never eliminated. Institutional legacy accumulates. This allows institutional legacies to accumulate and outdated structures to persist, even when they hinder progress.

Alongside this structural stasis, governments around the world are contending with an aging workforce. In some countries, the average age of civil servants is in the mid-40s or 50s, with a large cohort nearing retirement over the next decade. This demographic shift presents a dual reality: While this opens an opportunity to redesign jobs as they turn over, it also means a lot of senior personnel did not come of age in a digital environment and may lack fluency with modern technologies, let alone AI.

b. A Vision for a Modern, Agent-Empowered Workforce

The future of work in an agentic government is one in which humans and AI collaborate in new and dynamic ways within organisations that are redesigned to be agile, to facilitate continuous learning and to create public value. This vision encompasses several interconnected transformations:

Democratising tech skills: Generative AI is dramatically lowering the skills required to engage directly with data, develop simple applications, and automate routine tasks. Natural language interfaces, AI-assisted coding, and intuitive data analysis tools make data-driven decision-making and rapid prototyping widely accessible.

Attracting elite talent: Alongside democratisation, there is an increased need for highly skilled specialists to design, build, govern, and orchestrate complex core agentic AI systems. Attracting, developing, and retaining this scarce, 'hyper-productive' talent is a critical priority for any organisation, but particularly challenging and expensive for the public sector.

Blended teams of AI and human colleagues: Agentic systems will not only augment, but also significantly transform and, in some cases, automate many existing public sector job roles. The latter is particularly true for those involving routine information processing, content generation, and standardised decision-making. This presents an opportunity for slimmer organisations but also means a massive challenge for retraining and reorganisation. All public servants will need to develop skills in 'working with AI', such as critically evaluating AI outputs, providing effective feedback to AI systems, understanding how to use AI ethically in their context, and collaborating seamlessly with AI teammates.

Transforming organisational forms: As agents take on more complex tasks, the structure and culture or organisations will evolve. While some functions may approach full automation, most will be hybrid, with human-AI teams working side by side. Competence matrices…

AI co-workers and agentic systems, potentially designed with insights from high-performing tech companies, can act as catalysts, encouraging public sector teams toward more agile, data-driven, and startup-like routines and norms. The aim is not to replace present working culture wholesale, but to use AI to accelerate the adoption and reinforcement of high-performance practices, such as rapid iteration, transparent data sharing for decision-making, and continuous feedback loops.

The Automated Firm

Technologist Dwarkesh Patel envisions automated firms[10] - entirely AI-driven organisations that leverage the fundamental advantages of digitally embodied ideas:

Perfect replication: Elite talent and high-performing teams, once developed as AI systems, can be copied infinitely at near-zero marginal cost. This allows for the instant scaling of expertise and proven team configurations. Specialised AI 'workers' can be imbued with deep, amortised knowledge (equivalent to multiple PhDs and decades of experience) and deployed across countless tasks simultaneously. Even complex leadership functions could be replicated, enabling a single strategic vision to permeate an entire organisation with perfect fidelity.

Total knowledge fusion: Unlike human organisations, where knowledge transfer is slow and lossy, AI systems can 'merge' learnings. A central AI could assimilate the experiences and insights from millions of specialised AI instances, achieving a comprehensive, real-time understanding of the entire organisation and its environment. Communication

---

[10] Source: Patel, D. (2025): What fully automated firms will look like (link)

between AI models can occur directly via latent representations, eliminating miscommunication and enabling an incredibly rapid accumulation and application of institutional knowledge.

Unconstrained scaling of capability: The primary constraint on deploying capability shifts from the scarcity of human talent to the availability of computing power. If a particular AI skill or role is valuable, it can be scaled massively. The most critical roles (like strategic decision-making) could justify enormous computational resources, enabling exhaustive analysis and scenario planning far beyond human capacity.

Rapid, precise evolution: AI organisations can overcome the 'sclerosis' that affects human firms. Successful structures, processes, cultural norms, and innovations can be perfectly replicated and propagated. Continuous improvements and adaptations can be deployed instantly across all 'AI employees', allowing the entire organisation to evolve and optimise its performance with a speed and precision analogous to biological evolution on an accelerated timescale.

c. Key Questions

How do we reskill, redeploy, or release staff at the speed of automation, while protecting the human experience of transition? What are realistic throughput goals for upskilling, and how can micro-credentials, transition pathways, and social protections ensure no one is left behind?

What talent strategy (and compensation package) can attract world-class AI engineers without alienating unions or budget-conscious voters? Can purpose, flexibility, and influence offset the public sector's structural limitations on pay and perks? What alternative incentives, from impact visibility to intellectual ownership, can rival private-sector offers?

As AI agents take on more decision-making and information processing, how do we prevent over-reliance and preserve human judgment? How do we maintain the 'cognitive sovereignty' of both public servants and citizens?

How can we navigate professional gatekeeping as AI begins to challenge established roles in fields like education, medicine, and regulation? What strategies are needed to manage political resistance from professional bodies that view agentic systems as a threat to their status or authority? Should governments invest in new models for negotiation and hybrid credentialing to support the integration of AI into traditionally protected domains?

9. Tech Stack

Leapfrogging to tomorrow's enterprise stack.

a. How It (Doesn't) Work Today

Over the past two decades, the ideal government technology stack has emerged: Its building blocks include standardised modules for identity, data exchange, messaging, user interface, payments, and platforms for operating and designing registers and services. All of those blocks run cloud-natively on modern infrastructure.

This stack allows for economies of scale while abstracting technical complexity away from most public bodies, enabling them to develop functional services at a lower cost and with greater speed (consider the India Stack, for example, X-road in Estonia or Ukraine's platform of registers). Increasingly, these building blocks are also being standardised and developed internationally as digital public goods (think of the Nordic Institute for Interoperability Solutions or the GovStack initiative, for example).

The truth is less flattering. Most governments are a decade away from achieving enterprise best practice in the pre-Agentic AI era Some of the gaps are as follows:

- **Infrastructure and operational gap:** Workloads are still hosted on fixed virtual machines (or worse, 1990s servers). Systems are sized for peak usage. Common enterprise IT operations best practices are, such as DevOps rather the exception, whereas private sector DevOps penetration is over 80 percent[11]. Budgeting is typically capital-expenditure heavy and oriented toward maintaining legacy infrastructure[12] rather than developing modern, user-focused applications.

- **Architecture and shared platform gap:** Applications often remain monolithic and agency-specific Integration happens through brittle, point-to-point calls. Few countries have adopted data-sharing platforms like Estonia's X-Road, which enables secure cross-agency data exchange. APIs for essential functions, such as ID, payments, and secure messaging, are rare, meaning cross-agency workflows require custom workarounds.

- **Openness gap:** Open-source codebases for government software, vendor-neutral standards, and discoverable open data (and open APIs for restricted data) remain the exception rather than the norm.

---

[11] Source: SDTimes (2024): Report: As DevOps adoption nears 100 percent, these factors determine maturity (link)
[12] On this topic, consider that US federal agencies spend 80 percent of their USD >100 billion IT budget on legacy maintenance (link)

- **Policy gap:** Laws, policies, and entitlements are generally published as prose rather than in machine-readable formats. Without codified rules, automation, transparency, and trust become harder to scale. Policy registries are not designed to be auditable or consumable by AI agents, limiting the ability to build intelligent, rule-based public services.

Together, these gaps lead to the massive cost overruns and dramatic failures common to nearly all countries' public sector technology infrastructure.

b. A Vision for an Agentic Government Tech Stack

Even as most administrations struggle with foundational IT, the enterprise (and by extension, government) tech stack will need to be redesigned from the ground up to take advantage of the capabilities of agentic AI.

This will entail a rethink (and most likely a re-engineering) of nearly every existing functional layer of the government tech stack:

Schematic view of an agentic government tech stack
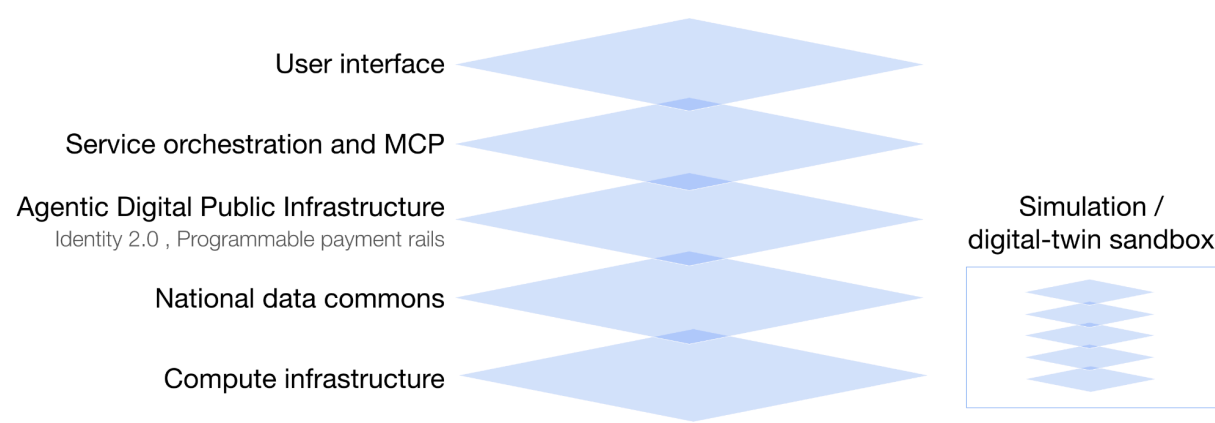
Building blocks for an agentic government tech stack

Building Block	What It Means in Practice	Why Agentic Agents Need It
Compute infrastructure	Serverless and agnostic. A model router picks the best model per task and records cost and energy usage per call.	Keeps inference fast and affordable, and prevents public agencies from buying or renting half-idle hardware.
Simulation or digital-twin sandbox	A live mirror of critical systems where policy tweaks or code updates run safely before hitting production.	Allows for testing rule changes, loading spikes, or cyber-attacks without real-world fallout. Provides evidence before action.

Identity 2.0	A dual identity system: (i) Human: verifiable credentials for people, businesses, and officials. (ii) Machine: cryptographically signed IDs for software agents, delegation tokens spelling out who may act for whom, on which tasks, for how long.	Every agent transaction starts with the question "who am I, on whose behalf, and am I authorised?". Clear, revocable credentials and delegation enable humans to stay in control and allow auditors to trace actions.
Programmable payments rail	Tokenised infrastructure that enables the public sector to support smart contracts, such as escrow and rules-driven payouts, as well as facilitating the straightforward integration of payment APIs.	Lets agents make and receive payments, with no manual finance step required. E.g. pay EUR 0.38/km for verified snow-ploughing routes, or trigger subsidies on verified milestones.
National data commons	A combination of a large-scale *data lake* and a *data mesh*, where all data (from high-value registers to operational logs) are catalogued. There is a retrieval layer for quick calls. Functions to generate for anonymisation and generating synthetic data. Fine-grained data-governance policies track consent, purpose and lineage for every query, while also enabling privacy-preserving machine learning to operate across the entire government data set. Laws, policies and KPIs exist in machine-readable decision tables allowing dynamic rewriting. Each version is tested, signed, and published alongside the legal prose.	Agents learn patterns and answer questions only when they can safely access real-world data. Lineage proves nothing was misused.
Service orchestration and model context protocol (MCP)	Cross-government fabric to orchestrate the interaction between different public and private sector agents, with a machine- readable directory of every API and capability. A workflow engine enables agents to combine tasks in new ways.	Enables 'Lego-brick' composability, allowing agents to rapidly build new life-event flows by snapping tasks together.
User interface	One multimodal shell (chat, voice, web, AR, visual) for accessing the orchestration fabric. It offers accessibility features (speech-to-text, multilingual) as well as an API for agents to appear embedded inside third-party apps.	Government meets users where they already are, whether that is with smart glasses or ERP systems. No more hunting for portals.

There will also be new functional layers, notably for governance:

- **AI evaluation and transparency layer**: Provides user-visible real-time logs, model 'nutrition labels', software bills of materials, and public dashboards showing uptime, decision volumes, and appeal rates. Converts the black box into a glass box, by allowing citizens and auditors to see, question, and correct agent behaviour.

- **Agent registry and governance**: Acts as a control tower for all authorised agents, recording their scope, audit hooks, rollback history, and kill-switches. Includes sandbox, certification, and marketplace functions for third-party agents.

To guide architectural decisions, one can think of the tech stack as comprising three concentric systems, each with a distinct purpose and optimal ownership model:

- **Compute substrate**: This is the foundational horsepower layer: cloud infrastructure, GPU clusters, and scalable data storage. Its role is to provide elastic capacity to train, fine-tune, and run AI agents at speed and scale. The operating model here is market-driven: governments should rent what already exists, prioritising portability and strong SLAs.

- **Agentic Digital Public Infrastructure**: These are the reusable building blocks every agent and service depends on: identity, secure messaging, payment rails, data catalogues, and task-level APIs. These blocks should be co-developed via public–private joint ventures or open-source consortia. Think of an open-source ID wallet, or a cross-border API standard for public service agents.

- **Sovereign governance layer**: This is the crown jewel, the part of the system that encodes law, accountability, and democratic control. It includes rules-as-code, agent registries, audit mechanisms, redress procedures, and kill-switches. Because this layer defines what is legally binding, what agents may act, and how decisions can be contested or rolled back, it must remain under public ownership and stewardship, even if some tools or frameworks are shared across countries or sourced from the market.

c. Key Questions

How can governments commit to long-term architectures when technology standards, tooling, and practices are evolving rapidly? What governance principles or 'minimum bets' ensure flexibility without paralysis?

What straightforward, high-level checks can help CTOs identify infrastructure investments that are incompatible with agentic AI? How should governments audit or phase out platforms that cannot provide task-level, agent-ready interfaces within a defined timeframe? What policy mandates and infrastructure shifts are needed to ensure AI workloads run in elastic, certified cloud environments?

What governance and procurement strategies should guide the use of commercial cloud and compute providers, given that compute is a market-based layer? How can governments ensure portability, SLAs, and data protection when renting this foundational infrastructure?

Which public–private collaboration models are best suited for building shared agentic digital public infrastructure, such as identity systems or task-level APIs? How can governments coordinate across sectors and borders for the sake of interoperability?

What safeguards and design principles must apply to the sovereign governance layer, where law, audit, and redress are encoded? How can governments retain full control over this layer while reusing open tooling or cross-national standards?

10. Public Procurement

How Agentic AI redefines how governments buy and what they get.

a. How It (Doesn't) Work Today

Procurement is one of the biggest barriers to the modernisation and improvement of public sector performance. It is often criticised for being slow, inefficient and overly formal. Although it was designed to prevent corruption, promote competition and deliver value for taxpayers, the opposite can sometimes be the result.

Simplistic decision criteria prevent informed buyers from making nuanced or holistic decisions. Newer approaches, such as innovation procurement, outcomes-based contracting and as-a-service models, remain niche. Public administration is struggling with a structural mismatch: on the one hand, traditional budgeting cycles and funding rules favour one-time projects and capital expenditure; on the other hand, cloud-based software works best with flexible, ongoing pricing and contract models.

The procurement of technology-based products and services is particularly hindered by outdated processes, cultural inertia and systemic fragmentation. Tenders often specify legacy solutions rather than functional requirements, effectively locking out innovative solutions often provided by startups. The risk-averse nature of public institutions, the complexity of compliance demands, and the lack of digital expertise among procurement officers mean that it is almost impossible for new technologies to gain a foothold.

b. A Vision for Agent-Driven Outcomes and Procuring Agents

Agentic AI transforms public procurement in two fundamental ways. First, by serving as a core tool to modernise and automate the procurement process itself. And second, by becoming a product governments increasingly need to procure.

Agentic AI *for* the Procurement Process

Throughout the procurement lifecycle, AI agents augment and, in some cases, replace traditional processes. The system becomes faster, more responsive and more transparent, eliminating the bureaucracy and fragmentation. This transformation plays out across the following phases in the procurement process:

- **Needs and problem analysis:** Rather than starting with a predefined solution, agentic systems define procurement needs based on a clear articulation of the underlying problem. By drawing on structured and unstructured data from various agencies, agents can identify inefficiencies, performance gaps or service failures, and present them as procurement opportunities, regardless of specific vendors or technologies.

- **Market scanning and intelligence:** Agents continuously monitor the landscape of suppliers and technological developments, mapping emerging capabilities against the needs of the public sector. This enables them to identify new market entrants and solutions in real time.

- **Cross-departmental coordination:** Agentic systems can detect similar needs across departments, jurisdictions or agencies, and will automatically flag opportunities for joint tenders or consolidated purchasing. This improves volume leverage and reduces duplication.

- **Tender design and matching:** Once a problem has been identified and the market mapped, AI agents will recommend the most appropriate procurement strategy, whether that be a standard open procedure, a dynamic purchasing system, an innovation partnership or an outcome-based contract. They match procurement demand with supply conditions and regulatory pathways in real time.

- **Vendor dialogue and bidding**: AI assistants support government buyers and vendors throughout the tender process. They answer questions to clarify details, generate customised bid templates and help vendors to frame their proposals so that they meet both formal criteria and real needs. This makes it easier for smaller suppliers and newcomers who are unfamiliar with government jargon to participate.

- **Contracting and negotiation:** Agents autonomously conduct procurement discussions and negotiation on behalf of governments. Much like tools used in the private sector,[13] these agents are given clear parameters, such as price ceilings, risk tolerances and

---

[13] On this, see providers like Pactum (link)

service levels, and negotiate directly with supplier agents to reach mutually acceptable terms. The result is faster, cheaper and often more balanced deals with built-in audit trails and far less room for human bias or misconduct.

The procurement *of* Agentic AI

Traditional public procurement still centres on input, such as staff-hours, bespoke software development, buildings, and fleets, However, pockets of *performance-based* and *design-build-operate* contracts do exist in sectors such as highways and energy. What traditional procurement rarely buys is the end-to-end capability that delivers a public service.

Agentic AI changes that calculus. Agents will plan, execute and self-audit entire workflows that currently require human teams (whether in-house or outsourced). Because the *object* of procurement increasingly bundles decision-logic, delivery and assurance in a single service layer, whole tracts of government operations become contestable where they never were before. The result is a rapid shift from paying for tools, software integration or personnel to paying for capabilities and outcomes. This can be for example, "process each building permit within five days at ≥97 percent statutory accuracy," or "answer 95 percent of citizen queries in under 30 seconds with a minimum of 90 percent satisfaction".

Public procurement, at 11-12 percent of global GDP (approx. USD 13 trillion), already constitutes the world's largest market, surpassing the automobile and food industries. However, even this figure represents only one third of public sector expenditure. If even half of routine decision-making and frontline service labour shifts to agentic AI outcome-based contracts, the share of public spending open to procurement could grow from one-third to well over half.

Agentic AI productises internal and external services, alongside novel payment triggers:

- **Frontline service delivery**: Whether In-house or outsourced, staff hours turn into a metered service, enabling any public agency to source capacity on demand. Pay per inquiry solved.

- **Permits and licensing**: Case officers and system monitoring become a decision engine. They are paid per compliant permit issued, with bonuses for low error or noncompliance rates.

- **Monitoring and accountability:** Periodic audits and static dashboards are replaced by always-on risk detection service, with part of the cost paid per incident or violation detected.

- **Policy implementation**: 'Pay and pray' policymaking is replaced by outcome contracts with payment tied to verifiable impact metrics.

This in turn contributes to significant wins:

- **Efficiency and speed:** Faster procurement cycles and quicker time-to-outcome.

- **Value for money:** You only pay when value is delivered), helping bend the cost curve in traditionally low-productivity areas like healthcare, education, and justice.

- **Access to new capabilities:** Even small municipalities or agencies can now 'rent' intelligence, for instance AI services for legal drafting, citizen communication, or service routing, that used to require elite human teams.

- **Flexibility and resilience:** Governments can test, iterate, and replace underperforming services with minimal disruption.

- **Transparency and auditability:** Procurement shifts from paperwork to performance — with live dashboards, KPIs, and full traceability.

As governments leverage agentic AI in both of the above described ways, they can move effectively towards outcomes while maintaining the unique constraints of public services (e.g. universality, ethical and legal safeguards). This unlocks new forms of public-private partnership; delivering public value no longer requires that services be operated or delivered by the public sector itself.

c. Key Questions

How can governments safely begin experimenting with agentic procurement within current legal frameworks? What use cases, such as mini-competitions, outcome sandboxes, or low-value micro-services, offer the highest learning value with the lowest risk?

How do we pay for outcomes delivered by autonomous agents without perverse incentives? What contracting structures ensure alignment between public value and automated performance, especially when human oversight is minimal?

What certification, monitoring and update mechanisms are needed to ensure vendor-supplied agents remain safe and reliable over time? Can governments develop continuous-competition models that keep systems up to date without locking in single providers?

Could a government-owned agent run procurement processes autonomously? If so, what governance guardrails are required to guarantee transparency, fairness, and contestability and to prevent institutional bias or capture?

As procurement becomes more automated, how do we retain strategic control over public priorities? What metrics, audit trails, and decision records are needed to preserve legitimacy when contracts are negotiated at machine speed?

Authors, Contributors and Contact

Authors and Contributors

Lead author	Luukas Ilves, Advisor to the Deputy Prime Minister and Minister of Digital Transformation of Ukraine and former Undersecretary for Digital Transformation and CIO for the Government of Estonia
Contributors	Manuel Kilian, Managing Director, Global Government Technology Centre Berlin
	Tiago C. Peixoto, Senior Digital Specialist - Digital Government Coordinator for the EU and Western Balkans, The World Bank
	Ott Velsberg, Government Chief Data Officer, Republic of Estonia

Contact

Citation:

Ilves, L., with Kilian, M., Peixoto, T., Velsberg, O. (2025). *The Agentic State: How Agentic AI Will Revamp 10 Functional Layers of Government and Public Administration. Version 1.0, May 2025.*