Digital Government Outlook 2026

From Foundations to Transformational Impact

Digital Government Outlook 2026

FROM FOUNDATIONS TO TRANSFORMATIONAL IMPACT

OECD
BETTER POLICIES FOR BETTER LIVES

This work was approved and declassified by the Public Governance Committee on 8 June 2026.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Please cite this publication as:
OECD (2026), *Digital Government Outlook 2026: From Foundations to Transformational Impact*, OECD Publishing, Paris, https://doi.org/10.1787/0496b2bc-en.

ISBN 978-92-64-97814-0 (print)
ISBN 978-92-64-88028-3 (PDF)
ISBN 978-92-64-44851-3 (HTML)

Photo credits: Cover © Digineer Station/Shutterstock.com. Executive summary © Digineer Station/Shutterstock.com.
Chapter 1 © puhhha/Shutterstock.com. Chapter 2 © Digineer Station/Shutterstock.com. Chapter 3 © Andrey_Popov/Shutterstock.com.
Chapter 4 © Digineer Station/Shutterstock.com. Chapter 5 © Digineer Station/Shutterstock.com.

Corrigenda to OECD publications may be found at: https://www.oecd.org/en/publications/support/corrigenda.html.

Foreword

Governments are under increasing pressure to deliver faster, be more responsive and ensure reliable human-centred public services, while operating under tight fiscal constraints. The rapid advance of artificial intelligence (AI) reinforces this imperative, opening opportunities as quickly as it raises governance challenges. Yet many public sector systems have struggled to keep pace.

Digital technologies and data are no longer optional tools for reform; they are essential to ensuring public sector performance, resilience and trust. OECD Member countries have made significant progress in building the foundations of digital government, guided by the OECD Recommendations on Digital Government Strategies (2014), on Enhancing Access to and Sharing of Data (2021), on the Governance of Digital Identity (2023), and on Human-Centred Public Administrative Services (2024).

However, the challenge is no longer just to build these foundations, but to complete the systemic digital transformation of the state that will deliver real impact for people and businesses. The move away from siloed, project-based digitalisation is under way, but governments need to go further in embedding whole-of-government approaches that prioritise user needs, data-driven policymaking and platform-based delivery models.

The next phase of digital government therefore requires a strong focus on delivery. Consistent with more mature digital governments, this means embedding digital, data and technology into everyday public sector operations – from budgeting and regulation to service design, procurement and policymaking – while adopting more iterative, agile and collaborative ways of working. It also requires aligning governance frameworks, skills and digital investments with the goal of achieving measurable improvements in outcomes for people and businesses.

This report – the first OECD *Digital Government Outlook* – provides a comprehensive and forward-looking assessment across 36 OECD Members and 8 accession candidate countries. Building on the findings of the 2025 OECD Digital Government Index and the Open, Useful and Re-usable Data (OURdata) Index, it examines both the advances made and gaps that remain and sets out the priorities for governments to translate digital ambition into tangible impact.

Acknowledgements

The OECD *Digital Government Outlook 2026* is the work of the Directorate for Public Governance (GOV), under the leadership of Elsa Pilichowski, Director. It was prepared by GOV's Government Performance and Indicators Division (GIP), under the direction of Gillian Dorner, GOV's Deputy Director, and Valerie Frey, Acting Head of Division, and with the supervision of Marco Daglio, Senior Strategy Advisor.

The Outlook was co-ordinated by Felipe González-Zapata. The chapters were drafted by Jamie Berryhill, Chloe Chadwick, Marco Daglio, Cecilia Emilsson, Felipe González-Zapata, Julian Olsen, Seong Ju Park, Mario Restuccia, Kenjiro Taniguchi, James Teague, Tony Tripp, and Ricardo Zapata, and benefited from the feedback and inputs from Gillian Dorner, Valerie Frey, Arnault Pretet, and Conor Das-Doyle. Marco Beltrán-Navarro provided data management and analysis assistance. Administrative support was provided by Imogen Ryan, Polyxeni Stappa and Jocelene Bonneau. Justin Kavanagh, Thibaut Gigou and Sarah Babay provided communications and dissemination assistance. The report benefitted from editorial support from Andrea Uhrhammer and Misha Pinchakov and was prepared for publication and laid out by Meral Gedik.

The country notes which accompany the report were co-ordinated and prepared by Ricardo Zapata and Mario Restuccia with the support of María Stephanía Guzmán and Marco Beltrán-Navarro. The country notes benefitted from the input of Thibaut Gigou and Meral Gedik.

The draft report received comments from Members of the OECD Public Governance Committee (PGC), as well as the OECD Working Party of Senior Digital Government Officials (E-Leaders). Feedback was provided by colleagues from GOV divisions including Public Budgeting and Management (PMB), Infrastructure and Public Procurement (IPP), Global Partnerships, Inclusion and Justice (GPIJ) and Anti-Corruption, Integrity and Open Government (ACIOG). More broadly in the OECD, the directorates for Science, Technology and Innovation (STI) and Development Co-operation (DCD) also provided valuable input and comments.

The Digital Government Outlook project, including the Digital Government Index and the Open, Useful and Re-usable Data Index, is based on the long-standing work of the OECD on digital government. It has benefitted from the continuous support and expertise of the OECD Working Party of Senior Digital Government Officials (E-Leaders) and its Expert Group on Open Government Data. The OECD is grateful for their contributions, as well as the financial support for this project provided by the governments of Israel, Slovenia, United Kingdom and Brazil.

Table of contents

FIGURES

TABLES

BOXES


Data Monagement
LOADING
Target Market
Marketing and soles
Business analytics tools
30% 55% 65% 80%
Financial Plan
Target Customer
Marketing and soles
Service or Product Line
Financial Plan
Target Cus
Target Cus
68227
15251
64214
66187
20825
76610
70
100
2022
2023
2024
Cost reduction
Quality management
Futurstial Growth

Executive summary

Governments are operating in an increasingly demanding environment of rapid change, shaped by economic uncertainty, demographic pressures, rising public expectations, and rapid technological change such as the advance of artificial intelligence (AI). At the same time, fiscal constraints, an ageing civil service and burdensome internal processes limit governments' ability to respond effectively.

The effective use of digital technologies and data offers a critical pathway to address many of these pressures. However, public trust in their governments' use of data and new technology remains fragile: only 52% of people across 30 OECD countries trust their government to use their personal data for "legitimate purposes". This highlights that progress in digital government depends not only on technology, but also on strong governance, skilled workforces and credible safeguards.

This first OECD *Digital Government Outlook* assesses progress in digital government across OECD Member and accession candidate countries and identifies where further effort is needed, drawing on the results of the 2025 Digital Government Index and the Open, Useful, and Re-usable Data Index.

The Outlook shows that, since the last stocktaking in 2023, governments have made significant progress in building the foundations of digital government, including shared infrastructure, interoperable systems and open data frameworks. **The challenge now is to move beyond these foundations to deliver transformational impact for people and businesses.** This includes filling important gaps in several areas, including institutional capabilities, governance mechanisms and workforce skills.

The Outlook highlights four priority areas for the next phase of digital government:

Moving from foundations to widely adopted interoperable systems and broader data sharing

OECD countries have made real progress in building digital foundations in government. Core, interoperable systems such as data-sharing platforms, digital identity, single digital gateways and cloud infrastructure are now widely available. These foundations make it easier for different parts of government to work together, respond rapidly and operate more efficiently. The challenge now is to ensure these systems are more widely adopted and used effectively across institutions to deliver visible benefits, including simpler and more efficient interactions between people and government. This means, for example, making digital identity easy to use and trustworthy so that more people adopt it, as well as increasing the quality and sharing of government-held data so that they can be effectively reused. Privacy and security standards are nearly universal across the OECD, but the operational data-management practices needed to ensure data quality, interoperability and trusted sharing are yet to follow at the same pace. Today, only 63% of public institutions across OECD countries, on average, are sharing data within government through their national data interoperability system, which are a critical component of a proactive and responsive government. Making better use of existing foundations will also support the trustworthy use of AI and help governments provide more joined-up, human-centred public services.

Strengthening investment and skills to deliver impact

OECD countries are making steady progress in how they plan and fund digital transformation. Most now assess digital projects before they start, provide dedicated funding for digital technologies and offer clear guidance on how to procure them. These steps matter, but much of the potential impact remains unrealised. Governments that fund digital projects in stages, learning from and building on what works, are better able to adapt to new technologies, redirect resources to high-impact areas and avoid locking in costly mistakes. Stronger evaluation is likewise essential: only one in four countries systematically assess whether completed digital projects delivered the results they promised. Closing this gap would help governments learn from experience, improve future decisions and show taxpayers that public money is being used well. Digital skills in the public sector are just as critical, yet only six OECD countries have a dedicated strategy for developing digital skills among civil servants. Without the right people in place, governments struggle to oversee the responsible use of AI, manage complex relationships with technology suppliers and sustain digital reforms over the long term. A more strategic approach to digital talent is therefore a basic condition for turning digital investment into lasting public value.

Scaling the adoption of trustworthy AI in government

In almost every OECD country, AI is already being used in at least one area of government, and most have established dedicated strategies, oversight bodies and training programmes to support its adoption. This marks an important shift from experimentation to early integration and puts governments on a solid footing for the next phase. The priority now is to create the conditions that allow AI to provide reliable results at scale. More targeted training is needed for specific roles in public services and policymaking, where readiness remains low. More practical support for AI procurement – currently available in just over half of OECD countries – would help governments better manage suppliers, clarify data ownership and control long-term costs. Reinforcing safeguards before and after systems are deployed, alongside open algorithm registers, can strengthen transparency and accountability, which are essential for public trust. Most critically, governments need to invest in measuring results: with only 28% of countries systematically assessing the impact of AI use, many lack the evidence needed to distinguish promising pilots from solutions that are ready to be deployed across the public sector.

Delivering more joined-up and user-centred public services

OECD countries have made solid progress in establishing whole-of-government service standards, involving users more consistently and investing in digital service delivery. These efforts provide a strong foundation; however, to ensure they lead to better, more reliable experiences for people and businesses, governments need to apply service standards to routine decisions such as budget approvals and service redesign processes. Only 28% of OECD countries systematically measure the burdens services impose on users, suggesting user engagement should be expanded to reach those who face the greatest barriers. The results of user engagement should feed into continuous improvement: strengthening feedback loops is essential to understand what works, identify obstacles early and make user-centred improvements a routine practice rather than a one-off initiative. Digital government authorities also play a critical role in improving co-ordination across agencies and ministries by connecting service channels and sharing individuals' data securely, sparing users from having to provide the same information repeatedly. Better linked data can enable more proactive services that anticipate needs before people have to ask, further reducing time, effort and frustration.

1 Digital governments at a turning point

Governments today face a growing disconnect between rising expectations for speed, adaptability and responsiveness, and institutional systems that have not kept pace. Digital technologies and data are no longer optional enablers; they have become core infrastructure for governments seeking to address today's policy and service delivery challenges. Yet the 2025 OECD Digital Government Index and OURdata Index show that while progress is real, it remains concentrated in strategies, frameworks and enabling conditions, rather than in their consistent operational application. Governments have invested in many of the right foundations, but these often fail to function as an integrated system. Weak data governance limits coherence and reuse; digital public infrastructure is deployed but underused; investment, procurement and workforce systems remain too rigid for iterative digital delivery; artificial intelligence (AI) is advancing faster than the trust mechanisms needed to steward it; and services remain too reactive and fragmented to reach people in a simple and proactive way. This chapter sets out the evidence behind this diagnosis, identifies the main challenges preventing governments from moving from policy design to operational delivery, and proposes the actions needed to close the gap between digital ambition and strong public sector performance.

1.1. Digital government in a fast-changing world

Efficient and adaptive governments remain essential. Around the world, governments operate in a context of rapid change and disruption, driving increasingly dynamic and uncertain policy environments. Governments simultaneously navigate geopolitical tension, economic volatility, demographic pressure, environmental challenges and rapid technological change. In such an environment, resilience is not only about responding to crisis. It requires governments to anticipate and to adjust quickly, learn continuously and reconfigure their institutions' methods and processes at pace to protect people from evolving risks and ensure that services remain relevant to their needs.

People expect government to deliver solutions to increasingly complex and fast-moving challenges. These expectations are shaped by many factors, including people's direct experience of public services and by their perceptions of how government responds to high-stakes, cross-cutting policy issues that affect long-term well-being. The 2024 OECD Survey on the Drivers of Trust in Public Institutions shows that people have limited confidence in governments' capacity to address complex policy issues involving multiple trade-offs: while 77% of people believe adapting to automation and new technologies should be a high national priority, only 41% trust their government to regulate them appropriately. This is further compounded by a frenetic and fragmented information eco-system. Together, these dynamics make it more difficult for governments to communicate clearly and mobilise collective action in times of uncertainty.

Against this backdrop, the effective, coherent and trustworthy use of digital technologies and data is foundational for an efficient and adaptive government. Digital transformation enables governments to anticipate risks earlier, co-ordinate complex interventions and respond at pace. But technology alone is not enough. It also requires strong digital governance, robust data stewardship, a skilled and adaptable workforce and legal and ethical frameworks that safeguard trust. These elements form the core infrastructure of a public sector capable of better joining up government institutions, navigating uncertainty, delivering high-quality services and strengthening confidence in the digital age.

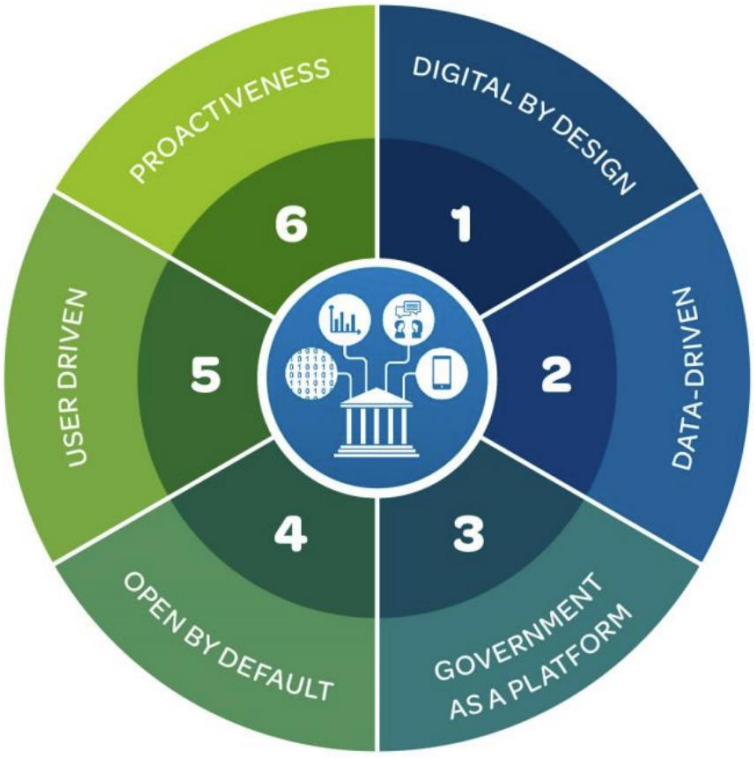
However, many governments face structural constraints that limit their agility to respond to this changing environment and expectations. Tight budgets, obsolete rules and regulations, rigid processes, and fragmented institutional responsibilities slow decision-making and weaken co-ordination. While digital government strategies have grown more ambitious in recent years, governance and delivery mechanisms have not always kept pace. As a result, governments increasingly find themselves caught between rising expectations for speed, adaptability and responsiveness, and institutional systems not designed for rapid, co-ordinated action. This gap is the central challenge for governments today.

1.2. Measuring progress to turn digital maturity into government performance

Closing the gap between rising expectations and institutional capacity requires more than technology adoption. It demands a fundamental re-engineering of how governments organise, govern and invest in their digital capabilities. Layered processes, rigid rules and fragmented systems have made many governments structurally slow. Connecting data, modernising systems and adopting more agile ways of working can make governments faster, more efficient and more responsive without sacrificing quality and accountability. The next phase of digital government reform requires governments to change how they organise, govern and invest in digital capability, with greater focus on embedding delivery capacity across institutions rather than expanding policy frameworks

The OECD Digital Government Policy Framework (DGPF) provides a structured, evidence-based approach to this challenge (OECD, 2020[1]). Building on the OECD Recommendation on Digital Government Strategies, the DGPF identifies six dimensions of digital maturity that governments must develop to deliver a coherent, human-centred and whole-of-government transformation (Figure 1.1). They are: (1) Digital by design; (2) Data-driven public sector; (3) Government as a platform; (4) Open by default; (5) User-driven; and (6) Proactiveness.

Figure 1.1. The OECD Digital Government Policy Framework



Source: (OECD, 2020[1]).

Digital by design means embedding digital thinking into the design of policies, processes and services from the outset, rather than adding technology onto legacy structures. It acts as a strategic lever across the public sector, creating the conditions for the other dimensions to take root. A government that is *digital by design* reconfigures how it operates at the source, rather than managing workarounds.

A data-driven public sector puts data at the centre of decision-making, service design and public accountability. Governments that systematically govern, share and use data can anticipate needs, reduce duplication and tailor services more precisely. This dimension is foundational to both efficiency and the capacity to absorb and respond to shocks.

Government as a platform shifts the model from siloed delivery to shared infrastructure: common building blocks, interoperability standards and reusable components that allow agencies to co-ordinate without rebuilding from scratch. This directly addresses the fragmentation that widens the gap between institutional capacity and what people and businesses expect.

Open by default moves governments away from closed, top-down decision-making towards transparency, data openness and collaborative engagement with people, civil society and the private sector. It enables governments to draw on broader knowledge and resources, and to build the trust that underpins legitimacy in the digital age.

A *user-driven* government centres the design and delivery of policies and services around the actual needs of people, addressing the digital divide and ensuring that digital transformation works for all. It requires systematic engagement with users across policy and service lifecycles, moving beyond formal consultation to continuous feedback.

Proactiveness goes further. It captures governments' capacity to anticipate users' needs and deliver services before they are explicitly requested, using the once-only principle and data analytics, AI and predictive tools to shift from reactive to anticipatory government.

To understand how countries are putting these six dimensions into practice, the Digital Government Policy Framework examines each one through four transversal

facets that mirror the stages of the policy cycle: *strategic approach, policy levers, implementation* and *monitoring*. The policy cycle lens therefore offers a more targeted and actionable understanding of where reforms stand and, crucially, where intervention is most needed to turn digital maturity into tangible improvements in government performance.

Developing maturity across all six dimensions involves navigating trade-offs. Efficiency pushes governments towards consolidation, standardisation and leaner processes; resilience requires redundancy, fallback channels and the capacity to absorb shocks. Investment models and workforce strategies must also keep pace: flexible, staged funding allows governments to test, learn and scale iteratively, while multidisciplinary teams and continuous professional development build the capabilities that technology alone cannot substitute.

Many of the challenges governments face, such as pandemics, environmental disasters and geopolitical shocks, are increasingly cross-border and cross-sector in nature, compounding the gap that no single government can close alone. Shared digital standards, interoperable data infrastructures and cross-border digital credentials reduce duplication and enable whole-of-government responses under strain. Instruments such as eIDAS 2.0 and the European Digital Wallet support trusted access within and across borders. Partnerships with the private sector, academia and civil society further expand capacity for collaborative responses to transnational risks.

Measuring digital government maturity is thus essential to understand how countries can strengthen their digital capabilities and what may be impeding them to turn developments into greater government performance. Furthermore, benchmarking digital capabilities helps policymakers see where the building blocks of digital government are in place, identify strengths to build on, and pinpoint where weak implementation is leaving governments stuck and in need of greater investment or political attention. To support this, the OECD has developed two complementary indexes that together provide a comprehensive picture of digital government performance: the Digital Government Index (DGI) and the Open, Useful, and Re-usable Data Index (OURdata). Together, these indexes benchmark the enabling foundations for a coherent and human-centred government digital transformation across OECD Member and accession countries (Box 1.1).

Despite progress across countries, implementation remains uneven. Governments with frameworks but without sustained capability, shared platforms or assurance mechanisms struggle to translate intent into delivery at the pace and scale needed. Progress depends on translating digital ambition into institutional transformation, supported by operating models, incentives and accountability arrangements that enable sustained adoption and use. The remainder of this chapter examines where countries stand across each of the six dimensions, and what it will take to move from digital ambition to institutional transformation.

Box 1.1. Measuring Digital Government: The OECD's Digital Government Index and Open, Useful and Re-usable Data Index

The **Digital Government Index (DGI)** assesses the enabling foundations for digital transformation across the six dimensions of the Digital Government Policy Framework (DGPF). It measures government actions on a wide range of critical enablers to strategically leverage digital technologies and data in government: governance and investments management, digital infrastructure, digital skills, data governance and sharing, artificial intelligence in government, and service design and delivery. It collects 155 datapoints per each participant country.

Progress across each dimension is assessed through four transversal facets that reflect successive stages of the policy cycle: *strategic approach* (the extent to which governments have coherent vision and direction); *policy levers* (the extent to which right mandates, legal frameworks and tools are in place); *implementation* (the extent to which these are embedded in operational practice); and *monitoring* (the extent to which governments evaluate results and learn). This four-stage lens is central to understanding not just how far governments have come, but where in the reform process progress has stalled.

The **Open, Useful and Re-usable Data (OURdata) Index** provides a specific benchmark on the robustness of open government data policies, examining the extent to which open government data (including high-value datasets) are available, accessible, as well as the degree governments proactively support their reuse. It collects 670 datapoints per each participant country. Selected datapoints are included in the calculation of the DGI, dimensions *Data-driven public sector* and *Open by default*.

What makes these two indexes distinctive is that they go beyond checking whether comprehensive digital government policies exist on paper, or government services are offered by digital means. They assess whether governments have the capability to implement those policies coherently across the public sector, from initial design through to final delivery. Therefore, they are essential instruments for OECD Member and partner countries to design their digital government strategies, benchmark progress, prioritise efforts and, overall, build more solid digital government capabilities.

Methodological process

Both indexes are the product of collaborative work with OECD Member countries through the Working Party of Senior Digital Government Officials (E-Leaders) to establish rigorous, transparent, and coherent measures, with their methodology approved by the Working Party and declassified by the OECD Public Governance Committee (PGC).

The data presented in this report draws on the OECD Survey on Digital Government 3.0, which informs the DGI; and on the OECD Survey on Open Government Data 6.0, which informs the OURdata Index. Both surveys were collected in the first half of 2025, covering policies and initiatives in place between 1 January 2023 and 31 December 2024.

Survey respondents were high-level digital government officials designated by each participating country, and a glossary of terms was provided to ensure consistent interpretation across jurisdictions. Once the data collection period closed, all country responses underwent a detailed, multi-round validation process. A first round reviewed responses for internal consistency and verified that answers and supporting evidence corresponded to the respective question. A second round ensured transversal consistency across survey sections and themes, identifying contradictions or gaps between related questions. Throughout this process, the OECD engaged bilaterally with country respondents to clarify ambiguities, request additional evidence and resolve discrepancies.

Following validation, each participating country formally reviewed and approved the final dataset before it was used to calculate the composite indices and inform the analysis presented in this report. This approval step ensures that the data accurately reflects each country's situation during the reference period and establishes a shared commitment to the integrity of the dataset.

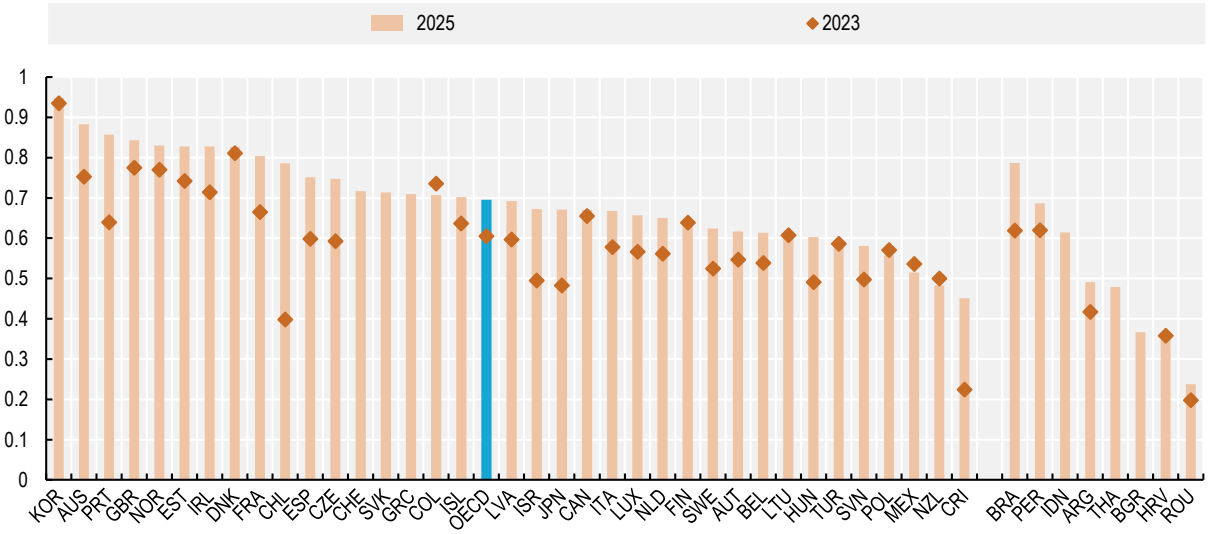
Further methodological details, including the weighting scheme, aggregation method and statistical robustness tests, are presented in OECD working paper with composite results (2026[2]).

Source: OECD (2026[2]).

1.3. The state of digital government: real progress made, more still needed

This report is based on the results and insights from the 2025 Digital Government Index (DGI) and the Open, Useful and Re-usable Data (OURdata) Index. The DGI analysis comprises 36 OECD countries and 8 accession candidate countries (Argentina, Brazil, Bulgaria, Croatia, Indonesia, Peru, Thailand and Romania), while the OURdata Index presents the same cohort except Denmark and Hungary. The headline results confirm real but uneven progress. The 2025 DGI average rose from 0.61 (out of 1) in 2023 to 0.70 in 2025 This represents a 14% increase, with all but 7 OECD countries improving their scores since 2023 (Figure 1.2). The OURdata Index increased more modestly, from 0.48 to 0.53 (Figure 1.4). Accession countries trail behind: their DGI average of 0.50 is 0.20 points below the OECD average, and their OURdata average of 0.46 is 0.07 lower. These results show that most OECD governments are now closer to the frontier of digital maturity than away from it, but the pace and depth of change remain insufficient to close the gap between institutional capacity and what people and complex policy challenges demand.

Figure 1.2. OECD Digital Government Index results



Note: 2025 data not available for Germany or the United States. 2025 data cover 1 January 2023 to 31 December 2024. 2023 data not available for Germany, Greece, Slovak Republic, Switzerland or the United States. Data for Indonesia and Thailand cover 1 January 2022 to 31 December 2023. See Annex Table 1.A.1 for detailed country scores.
Source: OECD (2026[2]; 2024[3]; OECD/ADB, 2025[4]).

StatLink https://stat.link/32clen

Progress across the six DGI dimensions is uneven and, when examined through the four transversal facets, reveals a structured pattern. The largest gains were recorded in *Data-driven public sector* (from 0.63 to 0.74, the biggest improvement of any dimension), *User-driven* (from 0.61 to 0.71) and *Proactiveness* (from 0.57 to 0.67). These gains reflect stronger data-governance frameworks, wider use of service design and user testing approaches, and a moderate expansion of the governance and use of AI in government.

Progress has been more limited in *Digital by design* (from 0.68 to 0.75), *Government as a platform* (from 0.62 to 0.71) and *Open by default* (from 0.53 to 0.59). The smaller gains in these three dimensions are partly because countries had already built solid foundations, particularly in governance and cybersecurity, rather than because they have stopped making progress. Key areas such as digital investment governance and monitoring of digital strategies remain weak and have not kept pace with improvements elsewhere in these dimensions.

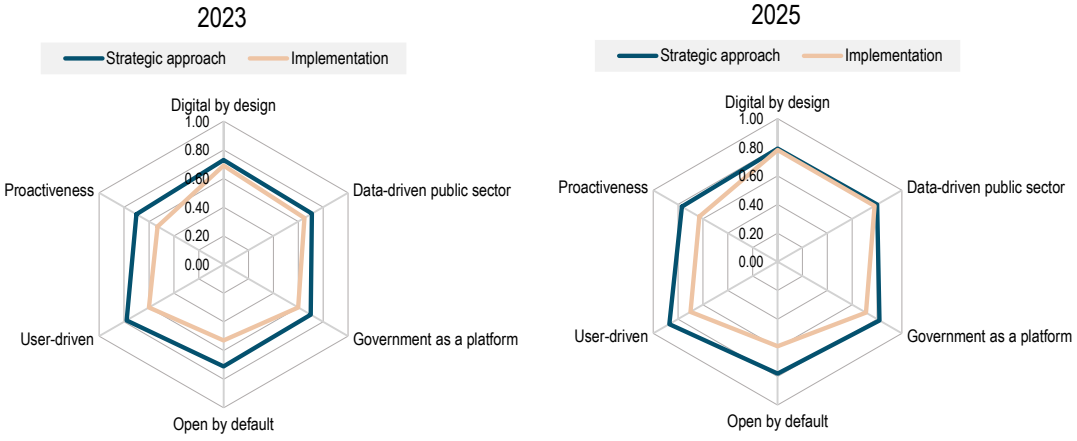
Open by default results are the most concerning: it recorded the smallest gain of any dimension (from 0.53 to 0.59) and remains the lowest-scoring overall. Progress was driven largely by modest advances in algorithmic transparency guidelines and open-source software policies, while the availability and accessibility of high-

value open datasets, the elements that carry the greatest weight in this dimension, improved only marginally. This matters beyond the dimension itself: limited performance in open government data constrains governments' ability to use data for real-time co-ordination, public accountability and innovation across the whole of government.

The four transversal facets that reflect successive stages of the policy cycle *(strategic approach, policy levers, implementation and monitoring)*, and which are tracked across the DGI dimensions, reveal varying degrees of progress. Across all six dimensions, scores for all facets increased compared to 2023 (Annex Table 1.A.2). However, they continue to demonstrate the gap between strategy and implementation (Figure 1.3). Scores for *strategic approach* (from 0.77 to 0.87) and *policy levers* (from 0.64 to 0.80) continue to exceed those for *implementation* (from 0.59 to 0.78) and *monitoring* (from 0.45 to 0.65) - the stages at which policy intent must translate into operational practice.

Figure 1.3. OECD countries show stronger performance and progress when setting the strategic direction for digital government, but still lag behind in their implementation

Selected transversal facets scores across the six dimensions of the DGI, OECD average, 2023 and 2025



Note: for full list of transversal facets values, see Annex Table 1.A.2.
Source: Authors' based on OECD Survey on Digital Government 3.0 (2025), OECD (2026[2]) and OECD (2023[5]).

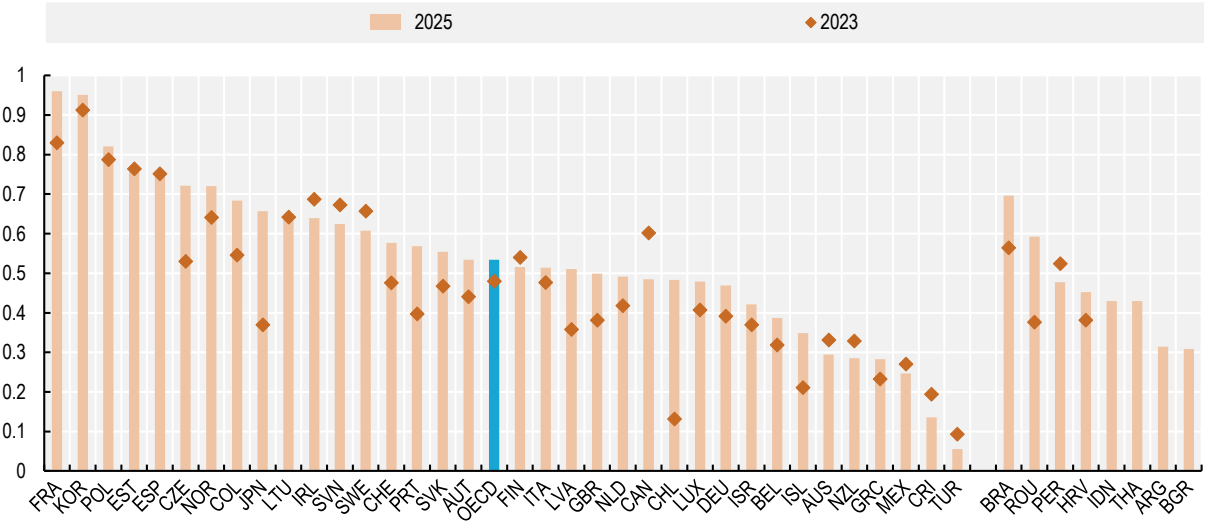
StatLink https://stat.link/iw0rk4

The results indicate a persistent gap between strategic ambition and implementation, particularly where monitoring lags policy direction. In *Data-driven public sector*, for instance, the strategic approach score reached 0.80 and policy levers 0.74, while monitoring remained at 0.45, essentially unchanged from 2023. A similar pattern holds in *Digital by design*, where policy levers reached 0.80 but monitoring remained at 0.55, and in *Proactiveness*, where despite notable gains in policy levers and implementation, monitoring stayed flat at 0.53. This gap between design and delivery was present in 2023 and has not materially closed, confirming that progress is stronger in establishing formal frameworks and enabling mechanisms than in embedding them into the day-to-day operations, workflows and accountability systems that determine how well digital government performs. Taken together, the evidence shows that the primary barrier to closing the gap is no longer the absence of strategy or policy frameworks, but the failure to translate them consistently into operational practice at scale.

The OURdata results further reinforce this diagnosis (Figure 1.4). OECD countries perform better in *Data availability* (driven by wider publication of high-value datasets, particularly in education, government finances and justice, the full list of datasets is presented in the annex) and *Data accessibility* (supported by the EU Open Data Directive requirements) than in *Government support for data reuse* – the pillar where performance remains weakest. On average, 57% of high-value datasets are available as open data and 67% are accessible through central portals, but only 49% offer

application programming interface (API) access. Progress in stakeholder engagement and impact assessment has been modest, confirming that while governments are making data more visible, they are less successful in making it systematically useful for learning, innovation and the creation of public value.

Figure 1.4. OECD OURdata Index results



Note: 2025 data not available for Denmark, Hungary, or the United States. 2023 data not available for Hungary or the United States, and not included for Denmark. 2025 data cover 1 January 2023 to 31 December 2024. Data for Indonesia and Thailand cover 1 January 2022 to 31 December 2023.
Source: OECD (2026[2]; 2023[5]; OECD/ADB, 2025[4]).

StatLink https://stat.link/gxjb7a

Taken together, the indices portray a public sector more digitally mature than in 2023, but still insufficiently coherent, adaptive or operationally integrated to close the gaps identified in the previous section. Governments must not only advance individual dimensions of digital government but also ensure that established foundations shape how they operate, co-ordinate and deliver in practice. The next challenge is not only to continue progressing within each dimension, but to close the distance between existing foundations and how governments operate, co-ordinate and deliver in practice. The following sections explore the barriers contributing to this gap and the actions governments can take to translate digital maturity into system-level performance.

1.4. Key challenges to moving from policy design to implementation and use

Building on the general and dimension results of the DGI and OURdata Index, this section examines five challenges that explain why the gap between digital ambition and institutional performance persists, and why closing it requires more than adding new components to an already crowded landscape.

1.4.1. Limited data governance prevents unlocking the value of data

Data is central to governments' ability to act coherently, reduce duplication, anticipate needs and build the conditions for trustworthy AI. The 2025 DGI results show that governments have made genuine progress in treating data as a strategic asset: 94% have data strategies and 92% report metadata standards, reflecting a broad commitment to governing data across the public sector. The use of data for core government functions is also strong with 94% of countries using data for policy monitoring and evaluation, and 92% to anticipate and plan interventions. These are not trivial achievements; they represent a substantial shift from the fragmented, siloed approaches that characterised public sector data management a decade ago.

However, progress has been uneven across the policy cycle. Monitoring of data strategies remain limited, with only 62% of countries reporting that they track results. Data quality management is also incomplete, with only 64% of countries having formal standards for data quality assessment. The gap is sharpest in understanding how services actually perform: just 44% of countries reported having government-wide initiatives to analyse service usage patterns, limiting governments' ability to learn from what people experience and improve services iteratively. Governments will realise limited benefits from stronger data arrangements unless they apply data consistently to service design, delivery and evaluation, not only to planning and oversight.

Open government data shows a similar pattern. Publication requirements and accessibility have advanced: 94% of OECD countries now require public sector institutions to publish open data, and accessibility through central portals is relatively high. But the mechanisms that turn data into public value remain weak. Only 49% of high-value datasets across OECD countries offer API access (a key enabler of reuse), and impact assessment of open data is limited: just 31% of countries evaluate its economic impact, 26% its public sector impact, and only 11% its social impact. Governments are making data visible without making it useful. Without stronger support for reuse and more systemic measurement of outcomes, open government data remain an example of formal availability without practical utility.

1.4.2. Adoption of digital public infrastructure lags behind its rollout

OECD countries have invested substantially in shared digital building blocks - digital identity, data-sharing systems, digital notifications, cloud infrastructure and single digital gateways. The rollout is real, but existence does not automatically produce public value nor integration.

Digital identity governance is largely in place: 92% of countries have a digital identity strategy and nearly all have designated a responsible body. Yet service coverage and actual use remain uneven. 69% report that more than half of their online services can be accessed using digital identity, and population uptake of digital identity ranges from over 90% in nine countries to below 50% in twelve. Furthermore, other systems are highly prevalent across OECD countries, such as data interoperability systems available in 83% of OECD countries, their impact depends on being actively used, which requires human-centred approaches, incentives, compliance and sustained investment that many governments have not yet put in place. Other enabling components such as digital post and digital payments are still absent in many countries.

The result is that many governments have the components for acting as a platform without realising the benefits of doing so. Governments face the greater challenge of driving consistent adoption, integration and effective use across government, as fragmented implementation, uneven uptake and variable interoperability can continue to limit the benefits of shared platforms and data assets. This gap between availability and actual use typically reflects three connected problems: fragmented governance, where no single institution has the mandate or incentive to drive uptake across government; limited requirements for service providers to use shared infrastructure; and insufficient practical support - technical guidance, onboarding support and hands-on assistance - to make common building blocks the default choice. This matters directly for the public. Where digital identity adoption is limited, where interoperability remains thin, and where shared infrastructure is incomplete, governments cannot provide the seamless, joined-up experience people expect and likely struggle to maintain continuity of services when disruptions occur.

1.4.3. Investment, procurement and skills are not yet fully aligned for digital delivery

Governments have strengthened central steering and planning for digital transformation, but the systems that govern investment, procurement and workforce remain better suited to managing compliance than to driving delivery. *Ex ante* assessment is widespread, with 89% of OECD countries having mechanisms to plan and estimate spending on digital government, but ex-post evaluation is rare: only 25% conduct ex-post cost-benefit analysis of digital projects. This means governments are approving digital investments without systematically learning whether they work in practice or delivering intended results.

Procurement guidance has improved, with 89% of OECD countries having dedicated central procurement guidelines for digital and ICT projects, but the use of agile and innovation-oriented mechanisms remains

moderate; only 55% of countries report using procurement approaches suited to iterative digital delivery. Instead, governments are still struggling to manage fast-changing and data-intensive technologies through static budgets, rigid approval cycles and compliance-oriented controls designed for a different era.

The same rigidity appears in digital talent and skills. Governments are increasingly aware of capability gaps (72% of countries have conducted digital skills-needs assessments) and have expanded training and recruitment efforts. But these remain fragmented and disconnected from long-term workforce planning: only 17% of countries have a dedicated public-sector digital skills strategy. Without sustained investment in people, governments cannot maintain the internal capability needed to exercise sustain strategic control over technology choices, manage vendors effectively or learn from implementation over time. Investment systems that do not learn, and workforces that are not planned, keep governments dependent on external providers and unable to build the institutional memory that sustained digital transformation requires. Together, these barriers limit progress toward more adaptive, evidence-based operating models that support lasting efficiency and resilience.

1.4.4. AI adoption is advancing faster than governments' capacity to govern it

AI adoption across OECD governments is accelerating, but the safeguards and operational conditions needed to use it safely and at scale are not keeping pace. The strategic foundations are largely in place: nearly all OECD countries have an AI-in-government strategy, 83% have at least one institution responsible for governing AI in the public sector, and AI is now used in at least one area of government in 97% of OECD countries, with strongest uptake in internal processes and public services.

However, the gap between strategy and operational governance is significant. Only 58% of countries provide central support for procuring AI goods and services. Data readiness, interoperability and transparency arrangements, the conditions that make AI trustworthy and scalable, remain underdeveloped in many contexts. Most strikingly, only 28% of OECD countries report conducting any financial or non-financial assessment of the impact of government AI use cases. Governments are adopting AI without systematically evaluating whether it is working as intended. Many have moved from strategy to experimentation, but not from experimentation to durable, government-wide implementation.

This matters beyond AI itself. AI can support productivity, responsiveness and proactivity, but only when built on reliable data, clear accountability and trusted operating arrangements. Where these conditions are absent, AI risks remaining confined to isolated pilots and delivering narrow efficiency gains rather than enabling a genuine shift in government capacity to anticipate, co-ordinate and deliver. The barrier is not ambition or early adoption, it is the limited capacity to govern and deploy AI systems in a way that is trustworthy, measurable and scalable across government.

1.4.5. Services are still too reactive and fragmented to deliver government as one system

Public services are still largely organised around institutional structures rather than people's needs. Many countries have made real progress: service standards are present in 89% of OECD countries, and co-design tools are widely available. But making standards consequential in practice is harder than establishing them. Formal requirements to apply service standards at both central/federal and sub-national levels exist in only 44% of countries, and the practical support mechanisms needed to apply them consistently are weaker than the standards themselves. User engagement, while improving, remains insufficiently systematic: the targeted inclusion of groups facing higher access barriers is lower than general co-design activity, and the use of testing methods such as design thinking sessions, focus groups and consultation platforms remain limited.

Measurement of service performance is also weak. Most governments lack the system-wide tools to coherently identify where users drop out, where service journeys break down or where administrative burdens accumulate. Without this feedback, it is difficult to improve services systematically or to demonstrate the value of digital investment to decision-makers and people alike.

The deeper problem is that services remain reactive. People and businesses must still know what to request, when to apply and where to go. The once-only principle, intensive use of data and AI-enabled anticipation, the mechanisms that would allow government to reach out

rather than wait to be contacted, remain unevenly implemented. The barrier is not the absence of digital channels but the failure to connect them into a coherent, people-centred system that acts on what government already knows.

1.4.6. Moving away from fragmentation to achieve system-level performance

A common thread runs through all five challenges: governments do not lack individual initiatives, policy instruments or digital components. What they lack is the institutional coherence to make these elements reinforce each other. These include data systems that cannot be shared, infrastructure that is built but not adopted, investments that are approved but not evaluated, AI that is deployed but not governed, and services that are designed but not connected. Each of these is a symptom of the same underlying condition. The barriers are not independent of each other: weak data foundations undermine interoperability; fragmented infrastructure limits service integration; rigid investment systems slow the iteration needed to close capability gaps; and without trust mechanisms, AI cannot scale. The parts are mostly there. The challenge now is making them work as a system, and that requires a different kind of reform effort from the one that built the foundations in the first place.

1.5. Realising the full potential of digital government

The five barriers identified in Section 1.4 share a common root: digital government reforms have been more successful at building foundations than at making them work together in practice. Closing the gap between digital ambition and institutional performance is therefore not primarily a question of adding new strategies or components, as most governments already have enough of both. It requires a different kind of effort: connecting what exists, embedding it into how governments operate, and sustaining the organisational conditions needed to learn and adapt over time. The following sub-sections set out four areas where more deliberate and systemic action is needed.

1.5.1. Moving from building digital public infrastructure to driving its use

Critical building blocks like data-sharing systems, digital identity, cloud infrastructure, common registries and service platforms remain underused and insufficiently embedded in daily operations of public institutions. The priority now is more systematic use of what already exists.

This requires designing shared digital components so that reuse is the path of least resistance for users and service providers. When agencies can draw on common digital identity systems, shared data pipelines and standardised service components rather than building their own, they create the conditions for genuinely joined-up government, reduced duplication and more efficient service delivery. Estonia's approach to digital public infrastructure illustrates what becomes possible when shared infrastructure is actively governed, mandated and maintained over time. Its X-tee data exchange platform, which public sector organisations are legally required to use and which is estimated to save Estonians 844 years of collective work time annually, while digital identity has saved up to 2% of GDP (OECD, 2024[6]).

Reuse does not happen automatically. It requires clear governance including common rules, co-ordination mechanisms and data-sharing agreements that give institutions both the obligation and the practical support to use shared infrastructure. It also requires funding models that cover not just the initial build but the ongoing costs of maintaining, updating and expanding common components over time and across agencies. Infrastructure that is built once and left to atrophy quickly becomes a barrier rather than an enabler.

User trust is an equally important condition for adoption. As governments expand digital identity systems and data-sharing capabilities, users need meaningful agency over how their personal data are processed, used and shared. Finland's Suomi.fi data exchange layer, built on the same architecture as Estonia's system and legally mandated for use by all public sector organisations, combines compulsory adoption with strong data protection safeguards, including clear information about what type of data is shared and for what purpose. This demonstrates that mandating use of shared infrastructure and protecting people's rights over their personal data are complementary rather than competing

objectives. Digital identity systems and wallets that allow users to control and selectively share their credentials, within and across borders, are an important mechanism for building this trust. Where users feel in control, adoption follows; where they are not, even well-designed infrastructure goes unused.

These foundations also determine how far governments can go with AI. Moving AI from isolated pilots to scaled, trusted use depends on reliable data, interoperable systems and repeatable assurance processes. Governments that treat strong digital infrastructure as a precondition for AI deployment, rather than something to be sorted out later, are better placed to realise AI's potential without creating new systemic risks. This need becomes even more pressing as governments harness AI systems to be more proactive.

1.5.2. Making governance and investment fit for digital delivery

The 2025 DGI shows that governance of digital government skews heavily towards planning: strategies are strong, mandates are clearer than before, and ex-ante assessment is widespread. What remains weak is the capacity to iterate, evaluate and adapt once delivery begins. Fixing this requires changes to how governments govern, fund and build capability for digital transformation, not just how they plan it.

Governance models need to embed feedback as a routine function rather than an occasional exercise. This means creating structured mechanisms, including regular reviews, user feedback loops, cross-agency learning forums, that allow strategies to adjust course based on evidence rather than waiting for a formal evaluation at the end of a project cycle. It also means opening governance to external perspectives: governance models and advisory arrangements that bring in industry, civil society and academic expertise help keep digital government strategies grounded in what is technically feasible and socially legitimate.

Institutional structures matter, too. Fragmented central oversight, where digital strategy, delivery support and emerging technology governance sit in separate organisations, weakens the coherence between policy intent and operational practice. The United Kingdom addressed this directly in January 2025 by consolidating its Government Digital Service, Central Digital and Data Office and AI incubator into a single Digital Centre of Government, with a mandate spanning strategy, delivery support and AI governance across departments, an approach designed to reduce the distance between central direction and day-to-day delivery.

Investment approaches need to match the iterative nature of digital work. Large, upfront programme budgets with fixed specifications are poorly suited to technologies that evolve rapidly and whose requirements become clearer through use. Governments that are shifting to modular, staged funding, releasing resources in tranches tied to demonstrated progress rather than upfront commitments, are better able to stop what is not working, scale what works well and avoid locking in costly mistakes. Australia's Digital and ICT Investment Oversight Framework (IOF), which requires major digital projects to pass through staged gateway reviews before receiving further funding, illustrates how investment governance can be structured to promote learning and reduce the risk of large-scale failure. Equally important is closing the evaluation loop: without systematic assessment of whether digital investments have delivered their intended results, governments cannot learn from experience or make the case for continued investment.

Decisions about whether to build, buy or partner for digital capabilities are among the most consequential governments make, yet many governments lack the internal expertise to make these decisions well. Governments that invest in this institutional capability, developing the skills to assess vendor proposals critically, manage contracts actively and understand the long-term implications of technology choices, are less exposed to lock-in, better placed to switch providers when needed and more able to maintain strategic control over their own digital infrastructure.

Ultimately, none of this work without skilled public servants. Expanding training and recruitment is necessary but not sufficient: only 17% of countries have a dedicated public-sector digital skills strategy, and without one, capability-building efforts remain fragmented and reactive. Korea's digital government talent development programme, part of the country's Human Resources Development System, illustrates how workforce planning and digital delivery can be systematically connected by combining a dedicated skills framework with structured career pathways for digital roles across the public sector. Governments need workforce plans that develop the cross-disciplinary skills,

combining policy, service design, data and technology, that digital delivery requires, and that create career pathways attractive enough to retain talent over time. Public servants who understand both the policy intent and the technical realities of digital systems are the most important enabler of the shift from digital foundations to digital performance. Many governments expand training and recruitment but do so outside a long-term workforce plan.

1.5.3. Building trust into AI in government from the outset

The OECD Trust Survey shows that people do not yet sufficiently trust governments' handling of emerging technologies, AI or personal data. The 2025 DGI offers some justification for these concerns: transparency, algorithmic accountability and impact assessment remain among the weakest areas of digital government performance across OECD countries.

This challenge is intensifying as AI becomes more deeply embedded in government. Conventional AI tools that generate content or recommendations already raise questions of accountability and bias. Agentic AI systems – which can place and execute sequences of actions across government tools and workflows, on behalf of users or public servants – raise the stakes further (Box 1.2). They offer the prospect of more proactive, integrated and responsive public services, but they also may also raise the stakes regarding clear oversight mechanisms, traceable decision trails, meaningful accountability, traceability and user control and the ability to pause, reverse or challenge automated actions. Governments that take account of these considerations from the outset will be better positioned to scale agentic AI responsibly.

Box 1.2. Exploring agentic artificial intelligence (AI) in government

AI agents are systems that can perceive and act upon their environment with a degree of autonomy, using tools as needed to achieve specific goals and adapt to changing inputs and contexts. Agentic AI generally refers to systems composed of multiple co-ordinated AI agents that can break down tasks, collaborate and pursue more complex objectives over time with limited human intervention. While generative AI (GenAI) systems *answer*, agentic AI systems *act*.

This distinction is important for government because the implications shift from what an AI system says to what it does. Conventional machine learning (ML) or GenAI tools may support analysis, drafting or interaction. By contrast, agentic AI systems may retrieve information across databases, trigger workflow steps, route cases, initiate transactions or update records within defined permissions. This creates opportunities to reduce administrative burden, improve responsiveness and simplify services, but it also raises the bar for legality, accountability, traceability and human oversight. Governments therefore need to govern not only the model, but also the action space granted to the system, the approval points in the workflow, and the mechanisms for oversight and redress.

An early public sector example is Estonia's Bürokratt, an early-stage interoperable network of government AI solutions that, from the user's perspective, functions as a single channel and unified gateway to government services. In the envisioned (and early) user experience, a user can request a complex service such as ordering a new passport, and an AI agent orchestrates the interaction across the relevant authority. The broader aim is to move service complexity into the background through system-to-system interaction while allowing the user to validate key actions where needed.

The OECD Working Party of Senior Digital Government Officials (E-Leaders) is exploring how governments can use agentic AI responsibly, including its public sector use cases, readiness requirements, and the enablers, guardrails and engagement needed for trustworthy adoption.

Source: (OECD, 2026[7]; OECD, forthcoming[8]).

Transparency is a foundational element for deploying and using AI in government. Governments should proactively disclose information about the algorithms they deploy, including their purpose, the data they use and the safeguards in place to prevent bias or error. The Netherlands' Algorithm & AI Register, developed in direct response to public concerns over the use of a faulty algorithm by the Dutch Tax Office and now covering over 600 algorithms across nearly 200 public organisations, offers a recent and well-documented model for institutionalising algorithmic transparency at scale. Publishing algorithm registers, strengthening open data practices and records gives users meaningful visibility and control over the use of their personal data are concrete steps that reinforce public confidence. The same principle applies to how governments govern and share personal data more broadly: informing people on the use of their data, and developing digital identity systems and wallets that give users genuine control over their credentials, rather than simply digitising existing processes, are a practical expression of transparent design.

Alongside transparency, independent assurance builds confidence that digital transformation is safe, fair and working as intended. This means embedding ethical frameworks and risk management processes throughout the lifecycle of digital systems – not only at the point of deployment – and establishing oversight mechanisms with the independence and technical capacity to hold governments to account. Modular and staged approaches to digital delivery support this: by breaking large programmes into smaller, evaluable components, governments can demonstrate progress, surface problems early and maintain accountability throughout. The 28% of OECD countries that currently assess the impact of government AI use cases represent a floor, not a ceiling. Systematic impact assessment should become a standard expectation, not an exception.

1.5.4. Delivering public services as one coherent system

Governments have invested heavily in individual service improvements. The next step is to connect these into service journeys that work across institutional boundaries, so that people experience government as a single, coherent system rather than a series of separate organisations each requiring its own interaction. This is less a technical challenge than a governance one: it requires deliberate choices about how services are designed, how data flows between institutions and how performance is measured and held to account.

The foundations for this shift are increasingly in place. Digital identity, data interoperability and the once-only principle – whereby governments collect information from users once and reuse it across services rather than asking for it repeatedly – make genuinely integrated, multi-agency service journeys technically feasible at scale. Denmark's digital public infrastructure, including MitID and NemLogin digital identity ecosystem and data-sharing systems, have enabled a range of life-event based services, covering everything from birth registration to business start-up, that pull together information across agencies without requiring users to re-submit data they have already provided. What is needed now is the governance and operational discipline to apply them consistently. Service standards, co-design methods and user testing are increasingly widespread, but the next step is to embed them in everyday delivery, decision-making and improvement routines. Strengthening these mechanisms through clearer mandates, better guidance and more systematic measurement of user experience is essential to turning isolated service improvements into system-wide change.

AI, and agentic AI in particular, offers significant potential to accelerate this shift. In a public-sector context, agentic AI can help navigate complex, multi-agency processes on user's behalf, identifying relevant entitlements, assembling information across systems, completing routine steps within defined limits and prompting users ahead of key deadlines or life events. Over time, this could move much of the complexity of interacting with government into the background, making services feel more proactive, connected and responsive. But realising this potential depends on the same foundations that underpins integrated service delivery more broadly: interoperable systems, trusted digital identity, clear records of automated actions, and meaningful points at which user can review, challenge or override what the system has done. AI amplifies the value of strong foundations, and the risk of weak ones.

Services also need to be designed for continuity and cross-border use. Continuity means maintaining service access when circumstances change or demand surges, through multi-channel delivery, fallback mechanisms and the ability for users to move between channels without losing progress or repeating steps. Cross-border

operation means allowing people, businesses and goods that move across borders to access services in other jurisdictions as seamlessly as they do at home. This requires interoperable digital identity systems, trusted data-sharing frameworks and mutual recognition of digital credentials. Both are expressions of the same principle: services designed around people's actual situations, not around the organisational convenience of individual institutions.

1.6. Setting up the Digital Government Outlook

The analysis in this chapter presents the central challenge the rest of this Outlook addresses: governments have built real digital foundations, but have not yet translated them into consistent, system-level performance. The OECD *Digital Government Outlook* provides a comprehensive, forward-looking assessment of digital government policies across 36 OECD Members and 8 accession candidate countries. Drawing on the results of the 2025 OECD Digital Government Index and the Open, Useful and Re-usable Data (OURdata) Index, it evaluates progress and persistent gaps across key areas of digital transformation, identifying what governments need to do to move from digital ambition to public sector performance in an environment of rapid technological change, fiscal constraints and limited public trust.

The Outlook is structured around this overview chapter and four thematic chapters covering key areas of digital government policy:

- Chapter 2 examines how OECD countries build and use digital infrastructure and data as foundations for more effective and future-ready government. It reviews progress and gaps in rolling out digital public infrastructure, expanding the use of digital identity, and implementing data strategies and data-management practices.
- Chapter 3 explores how countries develop the governance and organisational capacity needed to manage digital transformation. It examines developments and challenges in steering digital government, managing investments, and building the digital talent and skills to prepare the public workforce needed to deliver it.
- Chapter 4 presents how countries govern and adopt AI in government. Following the report *Governing with AI*, it provides a quantitative overview of the enablers governments have put in place to ensure trustworthy use, and progress towards more user-centred and responsive AI-enabled services.
- Chapter 5 examines how countries are building human-centred and proactive public administrative services in the digital age. It explores how governments organise, steer and improve services so that people experience government as reliable, joined-up and easy to navigate.

The cross-country analysis presented in this Outlook is accompanied by country notes for each participating OECD Member and accession candidate country, setting out the state of play and identifying strengths and areas for improvement on critical aspects of digital government policy.

Annex 1.A. OECD Digital Government Index scores

Annex Table 1.A.1. 2025 OECD Digital Government Index composite scores

Country	Digital by Design	Data-driven public sector	Government as a Platform	Open by Default	User-Driven	Proactiveness	Composite score
OECD	0.75	0.74	0.71	0.59	0.71	0.67	0.70
AUS	1.00	0.88	0.91	0.67	0.95	0.88	0.88
AUT	0.78	0.63	0.77	0.46	0.53	0.52	0.62
BEL	0.70	0.52	0.69	0.36	0.71	0.69	0.61
CAN	0.76	0.59	0.54	0.74	0.80	0.59	0.67
CHE	0.85	0.75	0.78	0.65	0.76	0.51	0.72
CHL	0.86	0.87	0.71	0.56	0.90	0.81	0.79
COL	0.68	0.87	0.52	0.77	0.70	0.70	0.71
CRI	0.60	0.43	0.38	0.32	0.55	0.42	0.45
CZE	0.71	0.94	0.78	0.72	0.64	0.68	0.75
DNK	0.88	0.83	0.92	0.81	0.72	0.79	0.83
ESP	0.82	0.82	0.74	0.63	0.73	0.78	0.75
EST	0.71	0.93	0.81	0.87	0.72	0.92	0.83
FIN	0.69	0.75	0.70	0.42	0.66	0.59	0.63
FRA	0.79	0.92	0.77	0.87	0.67	0.80	0.80
GBR	0.96	0.92	0.78	0.70	0.93	0.79	0.84
GRC	0.74	0.66	0.75	0.63	0.77	0.70	0.71
HUN	0.60	0.75	0.55	0.49	0.70	0.52	0.60
IRL	0.91	0.77	0.88	0.69	0.85	0.86	0.83
ISL	0.79	0.61	0.73	0.50	0.85	0.73	0.70
ISR	0.71	0.71	0.68	0.60	0.81	0.52	0.67
ITA	0.74	0.77	0.68	0.73	0.69	0.39	0.67
JPN	0.79	0.70	0.77	0.39	0.69	0.68	0.67
KOR	0.98	1.00	0.92	0.94	0.91	0.94	0.95
LTU	0.60	0.88	0.58	0.56	0.53	0.49	0.61
LUX	0.72	0.71	0.71	0.41	0.60	0.79	0.66
LVA	0.78	0.71	0.77	0.54	0.61	0.75	0.69
MEX	0.59	0.54	0.60	0.52	0.47	0.38	0.51
NLD	0.75	0.67	0.68	0.60	0.56	0.64	0.65
NOR	0.78	0.91	0.81	0.68	0.88	0.92	0.83
NZL	0.58	0.56	0.52	0.31	0.34	0.59	0.48
POL	0.64	0.51	0.61	0.54	0.59	0.46	0.56
PRT	0.96	0.76	0.93	0.65	0.94	0.91	0.86
SVK	0.73	0.72	0.73	0.7269	0.75	0.63	0.71
SVN	0.65	0.62	0.64	0.46	0.57	0.54	0.58
SWE	0.62	0.87	0.65	0.53	0.63	0.44	0.62
TUR	0.61	0.58	0.66	0.25	0.69	0.69	0.58
ARG	0.62	0.45	0.55	0.60	0.32	0.42	0.49
BGR	0.57	0.43	0.41	0.36	0.28	0.14	0.37
BRA	0.78	0.75	0.81	0.74	0.84	0.80	0.79

Country	Digital by Design	Data-driven public sector	Government as a Platform	Open by Default	User-Driven	Proactiveness	Composite score
HRV	0.46	0.58	0.41	0.23	0.34	0.06	0.35
PER	0.79	0.86	0.57	0.67	0.82	0.40	0.69
ROU	0.49	0.37	0.14	0.27	0.1	0.06	0.24

Note: 2025 data is not available for Germany and the United States. It covers the period from 1 January 2023 to 31 December 2024.
Source: (OECD, 2026[2]).

Annex Table 1.A.2. Dimensions of the DGI across four transversal facets

OECD average, 2023 and 2025

Dimension	Strategic approach		Policy levers		Implementation		Monitoring	
	2023	2025	2023	2025	2023	2025	2023	2025
Digital by design	0.73	0.79	0.71	0.8	0.69	0.78	0.53	0.55
Data-driven public sector	0.71	0.8	0.62	0.74	0.65	0.78	0.44	0.45
Government as a platform	0.70	0.82	0.58	0.67	0.60	0.71	0.56	0.56
Open by default	0.71	0.78	0.53	0.64	0.53	0.59	0.39	0.41
User-driven	0.78	0.87	0.53	0.64	0.60	0.70	0.55	0.65
Proactiveness	0.70	0.77	0.63	0.77	0.53	0.63	0.45	0.53

Note: The transversal facets assess performance across the stages of the public policy cycle.
Source: (OECD, 2026[2]; OECD, 2024[3]).

Annex 1.B. OECD Open, Useful and Re-usable Data (OURdata) Index scores

Annex Table 1.B.1. 2025 OECD OURdata Index composite scores

Country	Pillar 1. Data availability	Pillar 2. Data accessibility	Pillar 3. Government support to data re-use	Composite score
OECD	0.53	0.67	0.40	0.53
AUS	0.43	0.26	0.19	0.29
AUT	0.42	0.77	0.41	0.53
BEL	0.30	0.58	0.28	0.39
CAN	0.58	0.55	0.33	0.48
CHE	0.46	0.69	0.58	0.58
CHL	0.59	0.45	0.41	0.48
COL	0.71	0.60	0.75	0.68
CRI	0.07	0.33	0.00	0.14
CZE	0.74	0.76	0.66	0.72
DEU	0.45	0.65	0.30	0.47
ESP	0.59	0.77	0.91	0.76
EST	0.74	0.87	0.67	0.76
FIN	0.65	0.70	0.19	0.52
FRA	0.90	0.98	1.00	0.96
GBR	0.67	0.55	0.28	0.50
GRC	0.29	0.54	0.01	0.28
IRL	0.61	0.72	0.59	0.64
ISL	0.42	0.46	0.17	0.35
ISR	0.42	0.57	0.28	0.42
ITA	0.54	0.68	0.32	0.51
JPN	0.55	0.77	0.65	0.66
KOR	0.90	0.97	0.98	0.95
LTU	0.60	0.88	0.45	0.64
LUX	0.34	0.87	0.22	0.48
LVA	0.48	0.78	0.27	0.51
MEX	0.29	0.45	0.00	0.25
NLD	0.51	0.86	0.11	0.49
NOR	0.66	0.88	0.62	0.72
NZL	0.28	0.47	0.11	0.29
POL	0.75	0.91	0.81	0.82
PRT	0.49	0.82	0.40	0.57
SVK	0.51	0.76	0.39	0.55
SVN	0.58	0.82	0.48	0.62
SWE	0.75	0.82	0.25	0.61
TUR	0.11	0.00	0.06	0.06
ARG	0.33	0.42	0.19	0.31
BGR	0.25	0.63	0.04	0.31
BRA	0.78	0.74	0.57	0.70
HRV	0.44	0.67	0.24	0.45
PER	0.52	0.34	0.58	0.48
ROU	0.41	0.85	0.52	0.59

Note: 2025 data is not available for Denmark, Hungary, and the United States. It covers the period from 1 January 2023 to 31 December 2024.
Source: (OECD, 2026[2]).

Annex Table 1.B.2. 2025 OECD OURdata Index sub-pillar scores

Country	1.1	1.2	1.3	2.1	2.2	2.3	3.1	3.2	3.3
OECD	0.69	0.32	0.57	0.82	0.50	0.70	0.35	0.49	0.37
AUS	0.52	0.24	0.54	0.00	0.12	0.65	0.04	0.38	0.17
AUT	0.60	0.10	0.57	1.00	0.40	0.90	0.18	0.90	0.17
BEL	0.42	0.08	0.40	1.00	0.06	0.67	0.17	0.19	0.50
CAN	0.79	0.32	0.62	0.67	0.25	0.72	0.34	0.66	0.00
CHE	0.53	0.33	0.52	0.75	0.56	0.75	0.37	0.79	0.58
CHL	0.65	0.55	0.57	0.00	0.83	0.52	0.43	0.54	0.25
COL	0.86	0.63	0.63	0.25	0.58	0.96	0.58	1.00	0.67
CRI	0.22	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00
CZE	0.81	0.75	0.67	1.00	0.47	0.81	0.49	0.92	0.58
DEU	0.87	0.05	0.44	1.00	0.23	0.73	0.15	0.51	0.25
ESP	0.85	0.30	0.60	1.00	0.58	0.72	0.77	0.97	1.00
EST	0.95	0.44	0.84	1.00	0.77	0.85	0.63	0.55	0.83
FIN	0.75	0.38	0.83	0.83	0.57	0.70	0.24	0.00	0.33
FRA	1.00	0.83	0.86	1.00	1.00	0.95	1.00	1.00	1.00
GBR	0.92	0.35	0.75	0.50	0.46	0.68	0.41	0.42	0.00
GRC	0.66	0.17	0.05	1.00	0.00	0.63	0.04	0.00	0.00
IRL	0.87	0.36	0.60	1.00	0.42	0.75	0.60	0.67	0.50
ISL	0.52	0.11	0.62	0.83	0.00	0.55	0.18	0.16	0.17
ISR	0.60	0.13	0.53	0.83	0.13	0.75	0.20	0.63	0.00
ITA	0.87	0.29	0.46	1.00	0.44	0.61	0.23	0.72	0.00
JPN	0.63	0.28	0.75	0.75	1.00	0.56	0.62	0.82	0.50
KOR	0.94	0.86	0.90	1.00	1.00	0.92	0.93	1.00	1.00
LTU	0.73	0.42	0.65	1.00	0.75	0.88	0.26	0.42	0.67
LUX	0.48	0.05	0.51	1.00	0.88	0.74	0.04	0.13	0.50
LVA	0.66	0.18	0.59	1.00	0.58	0.78	0.32	0.17	0.33
MEX	0.60	0.05	0.24	0.83	0.00	0.50	0.00	0.00	0.00
NLD	0.56	0.18	0.78	1.00	0.71	0.88	0.15	0.00	0.17
NOR	0.83	0.38	0.77	0.92	0.83	0.88	0.57	0.71	0.58
NZL	0.47	0.13	0.23	0.38	0.46	0.58	0.00	0.00	0.33
POL	0.93	0.65	0.66	1.00	1.00	0.73	0.92	0.75	0.75
PRT	0.52	0.36	0.59	1.00	0.77	0.69	0.43	0.43	0.33
SVK	0.72	0.26	0.55	1.00	0.58	0.71	0.34	0.32	0.50
SVN	0.74	0.32	0.67	1.00	0.60	0.85	0.29	0.90	0.25
SWE	0.79	0.63	0.84	1.00	0.55	0.90	0.30	0.46	0.00
TUR	0.25	0.08	0.00	0.00	0.00	0.00	0.00	0.17	0.00
ARG	0.58	0.08	0.33	0.58	0.00	0.67	0.35	0.23	0.00
BGR	0.52	0.00	0.24	0.83	0.41	0.65	0.00	0.13	0.00
BRA	0.85	0.76	0.72	0.83	0.77	0.61	0.61	0.94	0.17
HRV	0.58	0.45	0.28	1.00	0.47	0.55	0.07	0.50	0.17
PER	0.83	0.22	0.50	0.42	0.00	0.60	0.51	0.72	0.50
ROU	0.55	0.42	0.26	1.00	0.83	0.72	0.60	0.61	0.33

Note: 2025 data is not available for Denmark, Hungary, and the United States. It covers the period from 1 January 2023 to 31 December 2024. Sub-pillar names are Content of the open by default policy (1.1), Stakeholder engagement for data release (1.2), Implementation (availability of high-value datasets) (1.3), Content of the free and open access to data policy (2.1), Stakeholder engagement for data quality and completeness (2.2), Implementation (accessibility of high-value datasets) (2.3), Data promotion initiatives and partnerships (3.1), Data literacy programmes in government (3.2), Monitoring impact (3.3).
Source: (OECD, 2026[2]).

Annex Table 1.B.3. List of high-value datasets assessed in the OECD OURdata Index

Category	Dataset
Companies and company ownership	Company register
	Company ownership
Earth observation and environment	Orthoimagery
	Satellite imagery
	Land cover
	Land use
	Geology
	Water bodies
	Water treatment plants
	Water supply networks
	Mineral resources
	Renewable energy resources
	Fossil fuel resources
	Air quality
	Water quality
	Noise pollution
	Protected areas
	Natural risk zones
	Forestry
	Agriculture
	Food security
	Fishing
	Hunting
	Energy consumption by end-users
Geospatial	Addresses
	Elevation
	Buildings
	Administrative units
	Geographical names
	Cadastral parcels
Meteorology	Meteorological observations
	Historical meteorological observations
	Weather forecasts
	Climatological observations
	Climate change predictions
	Climatological reference data
Mobility	Road transport networks
	Rail transport networks
	Water transport networks
	Public transport timetables
	Real-time traffic information
	Motor vehicle registrations
Statistics	Census and demographic indicators
	Vital statistics
	Economic indicators
	Connectivity
	Wealth
Government finances and accountability	Public procurement: Planning
	Public procurement: Call for tender

	Public procurement: Awards
	Public procurement: Contracts
	Public procurement: Implementation
	Detailed government budget
	Detailed government spending
	Election results
	Salaries of individual senior civil servants
	Government contact points
	International aid
	Hospitality and gifts
	Aggregated data on lobbying on public decision making
	Assets declarations of top-two-tiers of public employees
	Interest declarations of top-two-tiers of public employees
	Emergency and disaster relief
Crime and justice	Draft legislation
	Laws and statues
	Members of parliament
	Judicial decisions
	Crime statistics
	Gender-based violence
Education	List of schools
	Location of educational facilities
	School performance
	Skills statistics
	Digital skills statistics
Health and social welfare	Medical prescriptions
	Levels of access to health care
	Health visitor data
	Location of healthcare facilities
	Health statistics
	Health insurance
	Social benefits
	Housing

Note: The categories of high value datasets are determined by the OECD and primarily based on the G8 Open Data Charter. Datasets are only considered available if they are free of charge, machine-readable and provided with an open license, following the OECD definition of open data from the Recommendation on Enhancing Access to and Sharing of Data.
Source: (OECD, 2023[5]).

REFERENCES

OECD (2026), "Digital Government Index and Open, Useful and Re-usable Data Index: 2025 Results and Key Findings", *OECD Working Papers on Public Governance*, No. 90, OECD Publishing, Paris, https://doi.org/10.1787/6347ec74-en. [2]

OECD (2026), "The agentic AI landscape and its conceptual foundations", *OECD Artificial Intelligence Papers*, No. 56, OECD Publishing, Paris, https://doi.org/10.1787/396cf758-en. [7]

OECD (2024), "2023 OECD Digital Government Index: Results and key findings", *OECD Public Governance Policy Papers*, No. 44, OECD Publishing, Paris, https://doi.org/10.1787/1a89ed5e-en. [3]

OECD (2024), "Digital public infrastructure for digital governments", *OECD Public Governance Policy Papers*, No. 68, OECD Publishing, Paris, https://doi.org/10.1787/ff525dc8-en. [6]

OECD (2023), "2023 OECD Open, Useful and Re-usable data (OURdata) Index: Results and key findings", *OECD Public Governance Policy Papers*, No. 43, OECD Publishing, Paris, https://doi.org/10.1787/a37f51c3-en. [5]

OECD (2020), *"The OECD Digital Government Policy Framework: Six dimensions of a digital government"*, OECD Public Governance Policy Papers, No. 2, OECD Publishing, Paris, https://doi.org/10.1787/f64fed2a-en. [1]

OECD (forthcoming), *Governing with [Agentic] Artificial Intelligence*, OECD Publishing, Paris. [8]

OECD/ADB (2025), *Government at a Glance: Southeast Asia 2025*, OECD Publishing, Paris, https://doi.org/10.1787/bc89cb32-en. [4]


Data analytics
Diagnostic Analytics
Descriptive Analytics
2022
2023
2024
2025
100%

2 Strengthening digital public infrastructure and data governance

Strong digital foundations – shared digital public infrastructure (DPI), well-governed data and connected systems – enable governments to deliver services reliably, reduce duplication and keep pace with changing needs. OECD evidence confirms real and accelerating progress: data-sharing systems, digital notifications, digital identity and single digital gateways are in place across most OECD countries. Yet availability has not automatically translated into impact. Many services still cannot be delivered fully digitally from start to finish, because key components are missing or not yet consistently used across policy functions and levels of government. Extending adoption of (widely available) digital identity, particularly among users who face barriers of trust, usability and access, remains a challenge. Strategies and standards for data governance are common, but data quality management, reuse at scale, and impact measurement still lag. And even where the right foundations exist, they only deliver when systems can connect and exchange information reliably across organisations, levels of government and (increasingly) borders. This chapter reviews progress and gaps across the foundations: shared digital infrastructure, digital identity and data governance, interoperability, and the resilience and sustainability of government systems.

Key messages

- **Rollout of digital public infrastructure (DPI) is accelerating, while gaps in end-to-end delivery remains.** The core shared systems - data-sharing platforms, digital notifications and single digital gateways - are now in place across OECD countries, and three quarters of countries also have digital post and digital payment platforms. However, gaps remain: where these components are absent, services cannot be delivered fully digitally, and users must move between digital and non-digital channels, limiting seamless service journeys.
- **Digital identity governance is largely established, and the priority now is extending adoption.** Most countries have strategies and clear institutional responsibilities, and nearly seven in ten allow the majority of online services to be accessed using a secure digital identity. Reaching the remaining countries – and deepening uptake among users – require sustained attention to trust, usability and inclusive design.
- **Data governance is advancing, but translating high-level commitments into operational practice remains the main challenge.** All OECD countries have data strategies and clear objectives, yet implementation and impact measurement lag. Strengthening data-quality standards, enabling reuse across and beyond the public sector, and measuring outcomes are the next priorities – and are also preconditions for trustworthy artificial intelligence (AI) and effective data-driven government.
- **DPI and data policies only deliver results when systems can connect and work reliably.** Systems need to work together across organisations and levels of government so that data can flow and services can be joined-up – yet, on average, only 63% of public institutions are connected to their national data interoperability system across OECD countries. Cloud technologies have become standard government infrastructure, and open-source software, when backed by clear rules, active stewardship and sustained funding, can reduce dependence on single suppliers, increase transparency, and make it easier to share digital solutions across governments and borders.

2.1. Introduction

Digital public infrastructure (DPI) and data are the foundations on which modern government is built. DPI refers to the shared systems - such as digital identity, notification services, and data sharing platforms – that public institutions use in common to deliver services, exchange information and carry out their functions (OECD, 2024[1]). When these systems are well designed and well governed, they can enable government to work as a single coherent system rather than a collection of disconnected organisations. They reduce duplication, cut costs, and make it easier for government institutions to share information and co-ordinate their work. They also help governments adapt as needs change, keep services running reliably under pressure, and maintain operations when things go wrong.

Data flows through this infrastructure and creates public value. When data are governed responsibly – with clear rules about how it is collected, secured, shared and used – they can improve decision-making, simplify administrative processes and make services more responsive. For people and businesses, this can mean fewer requests to provide the same information repeatedly to different authorities (OECD, 2025[2]). For governments, effective data use supports better-targeted policies, stronger oversight of what is working (and what is not), and more efficient use of resources – with potential positive implications for cost savings.

Realising the full benefits of DPI and data requires treating them as shared public assets for all of government – not one-off technology projects. In practice, this means designing and managing them for reuse across the public sector and uptake by users if applicable; setting clear rules about who is responsible for what; and funding them as long-term national capabilities. These foundations are also critical for the trustworthy use of artificial intelligence (AI) in government where the quality, availability and governance of data determine whether AI can be trusted and scaled.

Governments build digital foundations to achieve four outcomes: 1) improving and sustaining reliable service delivery; 2) driving efficiency by reducing duplication and enabling shared use; 3) strengthening trust through secure identity systems and responsible data practices; and 4) enabling innovation while maintaining appropriate safeguards. These outcomes depend on four building blocks that this chapter examines in sequence:

- **The availability of core shared systems** such as digital identity, data sharing platforms, payment systems, notifications and service gateways that form the basic toolkit of digital government.
- **Governance arrangements** refer to the rules, responsibilities and accountability mechanisms that turn policy intentions into reliable practice. This covers both digital identify governance and data governance.
- **Interoperability** is the ability of systems to connect and exchange information across organisations, levels of government, and borders, so that data flows where it is needed.
- **Resilience and sustainability** refer to the choices that determine whether digital infrastructure can be maintained, adapted and kept secure over time, including the use of cloud technologies and open-source software.

This chapter follows these four building blocks in sequence, highlighting where progress is strongest and where gaps in adoption, governance, standards and evaluation still limit what digital infrastructure and data can deliver.

To support governments in building these foundations and achieving broader goals, the OECD Recommendations on Digital Government Strategies (2014), Enhancing Access to and Sharing of Data (2021), Governance of Digital Identity (2023) and on Human-centred Public Administrative Services (2024) highlight how secure and scalable digital infrastructure must be combined with robust data governance to deliver modern government (OECD, 2014[3]; OECD, 2021[4]; OECD, 2023[5]; OECD, 2024[6]). These Recommendations offer core guiding principles that inform this report.

2.2. Rollout of digital public infrastructure has accelerated across OECD countries

2.2.1. What counts as DPI and why it matters for outcomes

DPI refers to a set of shared, secure, and interoperable digital systems designed to support access to public and private services at scale. Rather than each government agency building its own separate tools, DPI provides common building blocks that any institution can use, reducing duplication lowering costs and making it easier for services to work together (OECD, 2024[1]; OECD, 2024[6]). DPI systems include:

- **Digital identity** systems allow people and organisations to prove who they are when accessing services online – securely, efficiently and increasingly across borders. They include ways of logging in, signing documents digitally and, in more advanced cases, storing and sharing verified digital credentials through a digital wallet.
- **Digital payment** systems enable governments to send and receive payments with people and businesses – for example, paying benefits faster, collecting fees more easily or tracking transactions more reliably.
- **Core registries** are authoritative, official records that serve as the single trusted source for key information – such as population records, business registers, address and land ownership data. They underpin many government processes by ensuring that all government institutions work from the same reliable information.
- **Data sharing** systems enable governments organisations to exchange information with each other, and in some cases with the private sector and civil society, under appropriate safeguards. They make it possible to apply the once-only principle – collecting information from a person or business once and reusing it across services, rather than different providers/government institutions asking users for the same details repeatedly.
- **Digital post** systems provide a secure channel through which official communication can be sent and received digitally, replacing physical mail for important or sensitive correspondence.

- **Digital notifications** are systems that allow public institutions to send messages – by emails, text or post – to keep people and business informed about their interactions with government.
- **Single digital gateways** facilitate the discovery and access of government services, reducing the need for individual solutions and platforms.

Individual institutions have long maintained their own digital systems operating in siloes, with limited incentives to transit towards more integrated approaches. The concept of DPI reflects a shift in ambition and scope: these components are designed to be used across ministries, levels of government, and in certain domains across the wider economy. This shared approach reduces fragmentation, lowers the cost of transactions and makes it possible to deliver genuinely joined-up services. For example, when someone experience a major life event – the birth of a child, starting a business or moving home – DPI can allow their information to flow automatically across relevant government institutions, so they interact with government once rather than many times. What in the past to require multiple separate transactions can become a single, joined-up process.

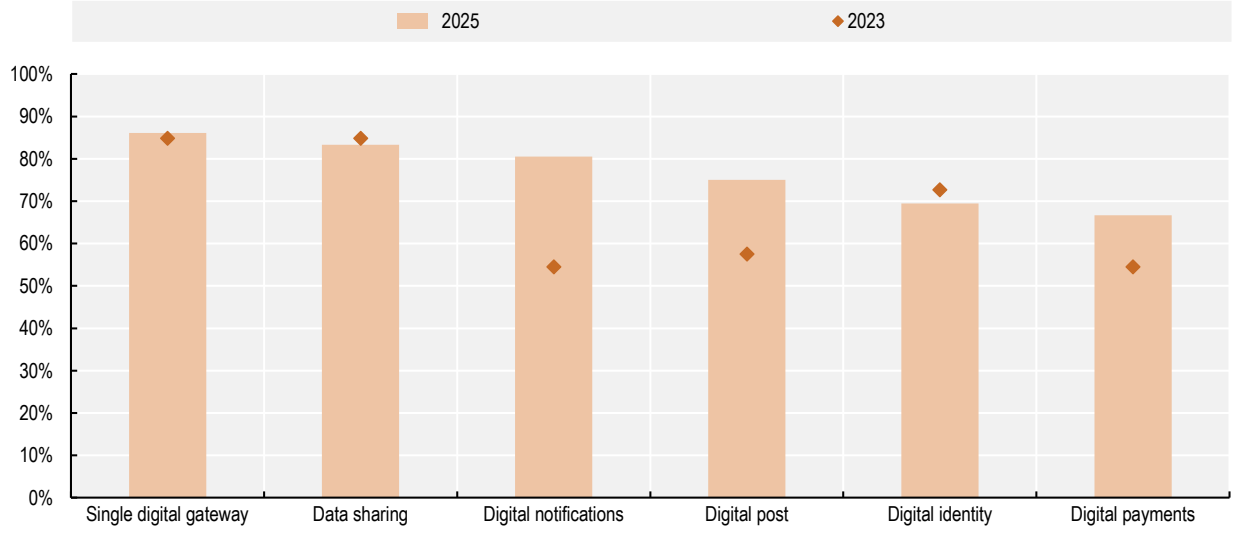
2.2.2. Progress and gaps: most building blocks are in place, but end-to-end delivery remains incomplete

OECD countries have made significant progress in deploying shared digital building blocks, particularly data-sharing systems and digital notifications. However, gaps in some components – notably digital post and digital payments – still prevent many services from being delivered fully digital from start to finish.

Evidence from the *Government as a platform* dimension of the OECD Digital Government Index (DGI) shows that, on average, 74% of core DPI components are now in place across OECD countries (Figure 2.1). Whole-of-government data-sharing and digital notification systems are now a standard, with over 80% of OECD countries having implemented both. Digital notifications are increasingly used to communicate proactively and reliably with people and businesses, supporting faster and more efficient service delivery.

Figure 2.1. The adoption of DPI systems has grown across OECD countries, particularly in the areas of digital notifications and digital post

Percentage of OECD countries adopting digital public infrastructure systems, 2023 and 2025



Note: Data not available for Germany or the United States. Single digital gateway: availability of a catalogue of services accessible to users. Data sharing: availability of a data interoperability system. Digital identity: at least 50% of national online public services can be accessed through a digital identity solution with two-factor authentication. Refer to Annex Table 2.A.1 for comprehensive OECD and Accession country data.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/8inaty

Progress is also noticeable, though more varied, for other components. Digital post and digital payment platforms are available in 27 out of 36 OECD countries (75%), reflecting steady expansion of the digital service toolkit. Where they exist, digital post solutions provide a secure channel for official communications and are often integrated into broader service platforms (OECD, 2024[1]) (Chapter 5). In many countries, digital post and notification services functionalities are built into single digital gateways – unified entry points where people can receive official communications, complete transactions and track their interactions with government in one place. This integration makes services simpler and more consistent for users, reduces administrative burdens and strengthen trust (Box 2.1). However, the fact that around one in four OECD countries still lacks digital post or payment capability points to an ongoing gap in the completeness of digital public infrastructure, and limits how far service delivery can be transformed in those countries.

Box 2.1. Digital public infrastructure in practice

Digital public infrastructure can enhance governments in several ways: by reducing duplication and cost; by enabling government institutions to work together more seamlessly; by making services more accessible and inclusive; and by supporting reliable and continuous delivery even when demand surges or disruptions occur.

Digital notifications - Canada and Italy

Canada's GCNotify allows federal public servants to send emails and text messages to individuals, free of charge. It connects easily to other services through a standard interface and its underlying code is publicly available for others to reuse – an approach modelled on the United Kingdom's GOV.UK Notify.

Italy's SEND platform is the national system for issuing and receiving legally valid notifications from public administrations. It centralises official communications, allows institutions to connect through standard interfaces, and lets people choose how they receive notifications. By maintaining up-to-date contact details and managing the full delivery process, SEND reduces uncertainty, lowers costs and simplifies workflows.

Single digital gateways - Belgium

Belgium's MyGov.be mobile app brings together access to official documents and certificates from federal, regional and local authorities in one place. It includes a unified digital post service, a secure digital wallet for storing government-issued documents, and a digital identity function for logging in to public services. The app consolidates multiple channels into a single, consistent experience and aligns with EU initiatives on European digital identity wallets.

Digital post - Sweden

In Sweden, people and businesses receive official communications from public authorities through a secure digital mailbox, using electronic identification to log in. The Mina meddelanden messaging service is operated by the Agency for Digital Government (DIGG), while the mailboxes themselves are offered by a range of public and private providers. People receive messages only from the public authorities they interact with, keeping the service manageable and relevant.

Digital payments – United Kingdom

GOV.UK Pay is a free payment service available for use by? public-sector organisations in the United Kingdom. It has no set-up fees or monthly charges and require no procurement process, making it straightforward for service teams to adopt. It allows organisations to replace offline payment methods quickly, providing a secure and accessible payment experience hosted on GOV.UK.

Source: (OECD, 2024[7])

2.3. Governance of digital identity is not yet leading to wider uptake

Most OECD countries have established governance arrangements for digital identity, but the integration of digital identity across services and its uptake by users remain uneven. The evidence shows that technology is not the bottleneck: trust, usability and inclusive design are what determine whether digital identity systems are adopted at scale.

A well-designed digital identity system delivers clear benefits. For individuals, it provides a simpler and more secure way to access services. For businesses, it reduces the cost and complexity of verifying who they are dealing with. Beyond these immediate advantages, digital identity is central to making digital government work reliably over time. By providing a trusted, consistent way for users to authenticate across institutions, it allows services to work steadily as processes evolve, new channels emerge, or technologies change. Where digital identity is not widely adopted, it becomes much harder to introduce new service models securely and at scale.

As set out in the OECD Recommendation on the Governance of Digital Identity, trusted and interoperable digital identity systems rely on solid governance arrangements (Box 2.2). Clear mandates, shared standards, robust security requirements and clear accountability ensure that digital identity protects users while remaining flexible enough to support new service models and adapt to future changes.

Box 2.2. Key principles for governing digital identity

The OECD Recommendation on the Governance of Digital Identity provides a framework for building identity systems that are effective, usable, secure and trusted. Its key provisions ask governments to:

- Design and implement digital identity systems that respond to the needs of users and service providers.
- Prioritise access for all and minimise barriers
- Take a strategic approach and define clear roles and responsibilities across the digital identity system.
- Protect privacy and prioritise security to ensure trust in digital identity systems.
- Align legal and regulatory frameworks, and invest in interoperability.

Source: (OECD, 2023[5])

2.3.1. Digital identity strategies are in place but their reach varies

OECD countries have made significant progress in strengthening the governance and strategic direction of digital identity. Nearly all (except Slovak Republic) have a designated government body responsible for setting the strategic direction for digital identity. This near-universal assignment of responsibility marks an important shift away from fragmented, project-based efforts toward more coherent, long-term stewardship.

However, the scope of these mandates varies considerably. Nine out of 36 OECD countries (25%) limit the mandate of this body to the public sector, treating digital identity primarily as a tool for accessing government services. In contrast, 26 out of 36 OECD countries (72%) extend the mandate to the broader digital economy, positioning digital identity as an enabler of secure interactions across public and private sectors. This broader approach treats digital identity not just as an administrative infrastructure but as a driver of digital trust, economic participation and innovation.

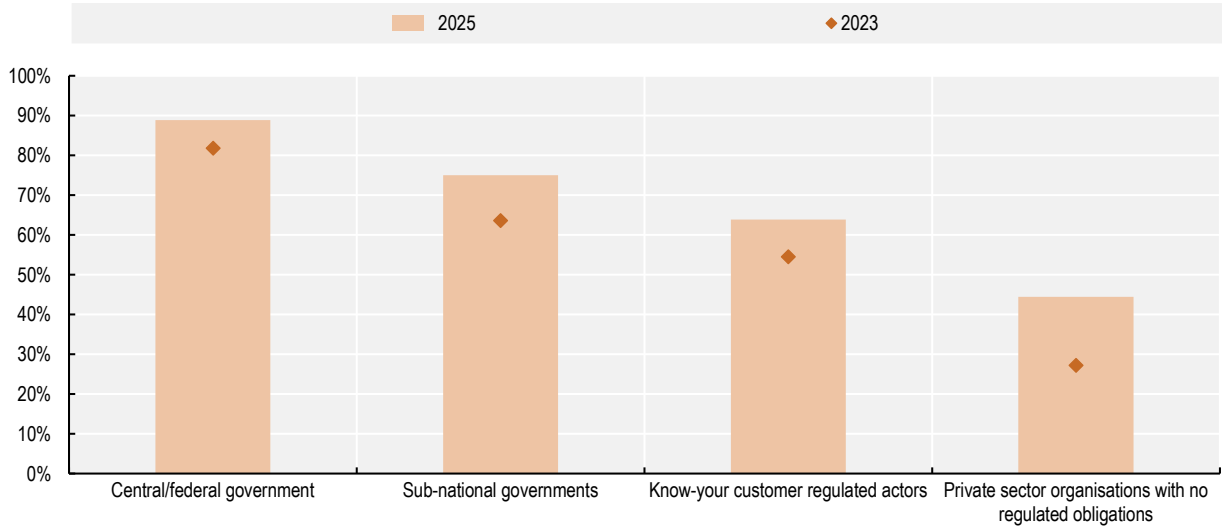
Strategic planning has also advanced: 33 out of 36 OECD countries (92%) have a government digital identity strategy, up from 82% in 2023. Almost all include provisions for use by central or federal government institutions, providing a common baseline across service portfolios.

The reach of these strategies beyond central government is more uneven. 27 out of 36 OECD countries (75%) include subnational governments in

their strategic frameworks, and 23 out of 36 countries (64%) explicitly address sectors with strong identify verification requirements, such as banking and the financial sector. This reflects growing recognition that shared identity infrastructure can reduce fraud, ease compliance and simplify how people access regulated services.

Figure 2.2. Actors included as service providers by the National Digital Identity Strategy

Percentage of OECD countries reporting types of actors included in national digital identify strategy as service providers, 2023 and 2025



Note: Data not available for Germany or the United States. Refer to Annex Table 2.A.3 for comprehensive OECD and Accession country data. Know-your-customer (KYC) refers to the process by which organisations verify the identity of individuals before providing them with a service — such as opening a bank account, accessing a government benefit, or signing a contract.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/rvg4wm

Extension into the broader private sector – retail, e-commerce and other sectors without specific regulatory requirements – remains limited, with only 16 out of 36 OECD countries (44%) including such provisions. This partly reflects legitimate caution: regulatory uncertainty, privacy concerns, questions about liability and uncertainty about whether systems are mature enough for wider use are all reasonable considerations. Addressing them will require sustained efforts to improve interoperability, foster trust, clarify liability frameworks, and ensure systems are robust enough to support a wider range of service models (Box 2.3).

Box 2.3. How OECD countries are governing digital identity

Denmark manages its digital identity solution (MitID) through a public-private partnership between government entities and the financial sector. The partnership behind MitID consists of the Agency for Digital Government, representing the state, the Danish regions and municipalities, and the country's financial institutions, represented by their industry association, Finance Denmark. This shared governance model has enabled MitID to function as a common national digital identity solution across both the public and private sectors. The solution is a central part of the country's digital infrastructure, supporting secure access to government services, banking, and a wide range of digital services on private platforms in Denmark.

Estonia provides a state-issued digital identity to every citizen, co-managed by the Information System Authority (RIA) and the Police and Border Guard Board (PPA). Since 2001, uptake has been driven significantly by private

sector adoption for business-to-business and business-to-consumer transactions. The Estonian experience shows the value of building a shared identity model with the private sector to encourage widespread use by citizens.

Italy has developed several complementary digital identity tools, all managed by public bodies. SPID is a federated system allowing people to access public and private services using credentials issued by approved providers. The electronic identity card (CIE) is a mandatory government-issued card with both physical and digital authentication capabilities. In 2024, Italy launched the IT-Wallet, its implementation of the EU Digital Identity Wallet, fully integrated into the government's IO app.

Source: (OECD, 2024[8]; MitID, n.d.[9]; Estonian Business and Innovation Agency, n.d.[10]; Government of Italy, n.d.[11]),

2.3.2. Digital identity coverage is growing, though adoption varies across countries and users

Progress in digital identity strategies and governance has translated into broad availability of digital identity systems across OECD countries (Figure 2.1), and this is increasingly reflected in service coverage. Nearly seven in ten OECD countries (25 out 36, 69%) report that more than half of their online public services can be accessed using digital identity – a significant achievement that reflects sustained investment in digital identity infrastructure. Many of these countries have reached this level through widely adopted national solutions that covers a broad range of services. Among OECD accession candidate countries, Brazil and Croatia have made particular progress in implementing such solutions at scale. Sustaining this momentum and extending it to the remaining countries will require continued attention to incentives for service providers to integrate digital identity, clearer governance frameworks and more consistent adoption across service portfolios.

User uptake – meaning the share of the population that actually uses digital identity – varies widely. In nine countries (Belgium, Chile, Denmark, Finland, Iceland, Korea, the Netherlands, Norway and Sweden) more than 90% of the population uses digital identity. In fifteen countries, uptake varies between 90% and 50% of eligible population, and in the other twelve countries, fewer than half use it. These disparities show that making digital identity available across services is necessary but not sufficient. Sustained effort is also needed to build user trust, design and develop systems that are easy to use, address barriers for people who struggle with digital services, and ensure that high-quality non-digital channels remain available, so no one is left behind.

OECD countries use a range of methods to verify users' identity, rather than relying on a single approach (Annex Table 2.A.2). Username and password (without an additional verification step) remain the most widely available solution, used in 27 out of 36 OECD countries (75%). It continues to play a role as a low-cost, familiar entry point for services that require a lower level of security.

More secured methods requiring a second verification step are increasingly common. Text-message-based verification is available in only 17 out of 36 OECD countries (47%) and email-based verification in 12 out of 36 countries (33%), though concerns about their vulnerability to fraud and phishing have led several more advanced countries to move beyond these in favour of app-based or other stronger methods. App-based verification is now available in 26 out of 36 OECD countries (72%), and smartcard-based verification in 24 out of 36 countries (67%). Australia's myGov, for instance, now supports passkeys – a newer more secure method that replaces password by using a unique digital key stored on the user's device, which cannot be stolen through phishing.

Overall, OECD countries are strengthening their identity verification systems, but many are still in transition period, balancing the need for security against the importance of keeping systems accessible, affordable and easy to use.

2.4. Data governance continues to see a gap between strong strategies and weaker delivery

Nearly all OECD countries recognise data as a strategic asset and have put strategies and objectives in place. The

remaining challenge is operational: strengthening data quality, removing barriers to data sharing and re-use, and measuring how data use is delivering impact.

Data governance covers the rules and responsibilities that determine how data are collected, managed, accessed, shared and used across government. It provides the stable foundation that allows systems to work reliably as technologies, organisations and requirements change. When data governance is coherent, institutions can share and re-use data consistently, adapt processes without disrupting services, and maintain continuity when regulations or service models evolve.

This matters across all government functions. In public procurement, consistent and well-managed data supports performance monitoring, oversight and the detection of irregularities. In justice and integrity systems, well-governed data can help prioritise intervention, support protective decisions, identify corruption risks and support accountability (OECD, 2025[12]; Hlacs and Wells, 2025[13]; OECD, 2024[14]; Byrom, Piccinin-Barbieri and Wells, 2024[15]; OECD, 2025[16]). Across all functions, the OECD evidence is clear: data alone does not create value. Value comes from governing data strategically and responsibly – establishing the shared rules, safeguards and collaborative arrangements that make data sharing and re-use possible. Without these conditions, data tends to remain fragmented or under-used, and governments lose the ability to anticipate needs, co-ordinate action, and deliver outcomes that serve the public interest.

The OECD Recommendation on Enhancing Access to and Sharing of Data sets out principles for maximising the benefits of data while protecting the rights and legitimate interests of individuals and businesses (see Box 2.4 and (OECD, 2021[4])). Evidence from the *Data-driven public sector* (DDPS) dimension of the 2025 DGI shows strong governance frameworks on paper – strategies, mandates and standards are widespread – but systematic data use, quality management and routine monitoring still lag. Bridging this gap means moving from having frameworks to applying them in daily practice: enforcing common standards, improving data quality, building skills for responsible data use, and embedding evaluation so governments can measure the impact of data practices.

Box 2.4. What a truly data-driven public sector looks like

A data-driven public sector uses data consistently to improve decisions, design and deliver better services, measure outcomes and strengthen accountability. The central challenge is not only technical; governments also need the right governance, skills, incentives, and ways of working that make data use effective across the whole-of-government.

A truly data-driven public sector:

- treats data as a strategic asset, understands its value and measures its impact;
- reduces barriers to managing, sharing and re-using data across the public sector;
- uses data to improve policies and services, from design and delivery to monitoring and evaluation;
- enables re-use and openness, supporting publication of open data and data use across the public sector and beyond, where appropriate.

The **OECD Recommendation on Enhancing Access to and Sharing of Data** aims to maximise the benefits of data access and sharing while protecting rights and other legitimate interests. It frames data access and sharing as a foundation for addressing societal challenges; improving evidence-informed policymaking and service delivery; strengthening transparency and trust, and enabling people and businesses to create value.

The Recommendation has three practical pillars:

1. **Reinforce trust.** Strengthen stakeholder engagement, adopt a strategic, whole-of-government approach, improve transparency and ensure responsible governance throughout the data value cycle.

2. **Stimulate investment and incentives.** Establish sustainable models and the conditions needed to support data access and sharing.
3. **Foster effective and responsible sharing and use.** Enable trusted cross-border data flows; improve data findability, accessibility, interoperability and re-usability; and build capacity for responsible data use.

Source: (OECD, 2019[17]; OECD, 2021[4]).

2.4.1. Public-sector data strategies are common and implementation is strengthening

A strategic approach to data governance in the public sector is well-established across OECD countries, and implementation is progressively catching up with ambition. Evidence from the 2025 DGI shows that 34 of 36 countries (94%) have a public-sector data strategy, indicating widespread recognition of data as a strategic asset. Strategic framing is generally strong: 97% set an overall vision and all include explicit goals (see Box 2.5 for some examples). Implementation-oriented elements are also solid: most strategies identify responsible actors (88%) and outline how goals should be achieved (94%). More than six in ten countries (62%) have also put in place mechanisms to monitor results - reflecting growing recognition that strategies need to be tracked to deliver impact. Strengthening monitoring across the remaining countries, and deepening how results are measured and acted upon more broadly, represents the next step in maturing data governance from policy commitment to sustained operational practice. Furthermore, evaluation mechanisms to assess if data strategies are delivering intended results would contribute to closing feedback loops and adjusting future priorities, resource allocation, and implementation approaches based on evidence of what works.

Box 2.5. Dedicated public-sector data strategies: Chile and Poland

Chile's Data Strategy for State Administration sets out a vision for a data-driven public sector that delivers proactive and efficient services. It establishes a coherent governance framework, including a Strategic Data Council, designated data leads, and a shared data inventory. It prioritises staff training across central and local government, and sets out a detailed action plan tracked through 2030. Technological priorities include a new open-data portal, a data interoperability network, consent management tools and broader integration of data across services.

Poland's Open Data Programme 2021-2027, led by the Ministry of Digital Affairs, aims to expand the supply and quality of re-usable open data via the national dane.gov.pl portal. Governance is led by an interministerial task force and a network of data openness officers. The programme mandates open data publication with an application programme interface (API)-first approach, in line with EU legislation and technical standards. Metadata interoperability is ensured through the adoption the DCAT Application Profile for data portals in Europe (DCAT-AP), based on the Data Catalogue Vocabulary (DCAT) developed by W3C. Progress is tracked through data-sharing schedules and annual reports, and stakeholders training is provided through the Open Data Academy.

Source: (Republic of Poland, 2021[18]; Secretaría de Gobierno Digital, 2024[19]).

The gap between ambition and execution suggests that in many countries, data strategies risk functioning more as policy statements than as operational tools. A group of countries – Canada, Chile, Estonia, France, Korea, Norway, Portugal, Sweden, Switzerland, Türkiye and the United Kingdom – stand out for integrating all core components, including monitoring. Other countries have formal strategies but show gaps in implementation, accountability or performance tracking. Consistent

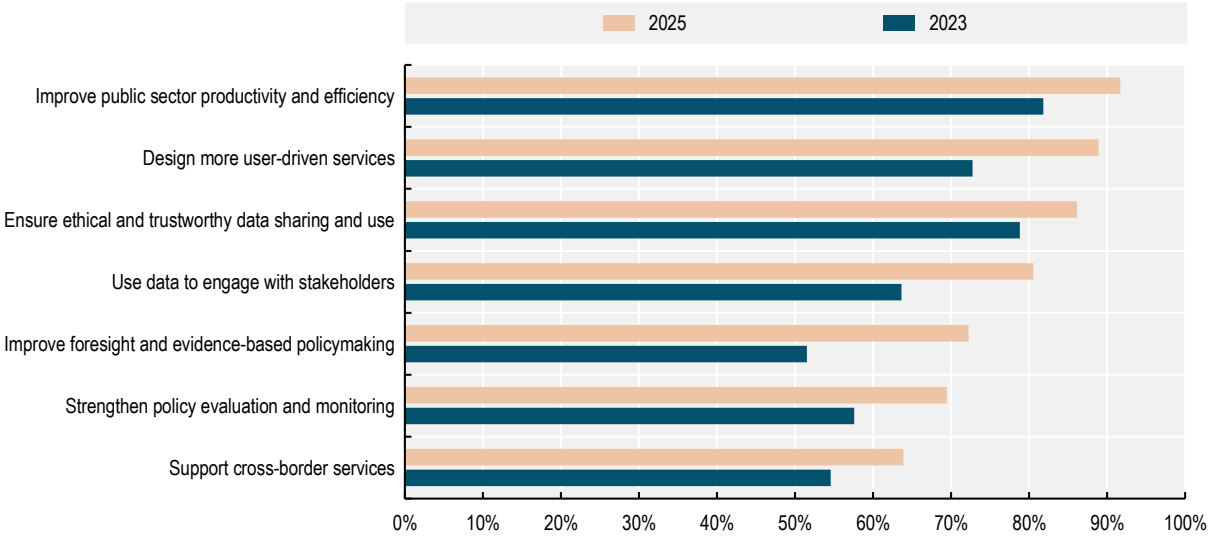
execution remains the next frontier for maturing data governance.

OECD countries' public-sector data strategies are primarily focused on improving internal performance and service delivery, and less toward systemic objectives such as cross border interoperability or long-term evaluation. Every government with a data strategy includes objectives to increase public-sector productivity and efficiency, and 94% explicitly aim to design more user-driven services (Figure 2.3). A similarly high share (91%) prioritises ethical and trustworthy data sharing and use, reflecting growing concerns for privacy.

However, more forward-looking goals are less common: around 68% of countries include goals related to cross-border services, and 74% address strengthening policy evaluation and monitoring. This suggests that, while data strategies are increasingly focused on internal reform, their potential to support longer-term planning, cross-border interoperability and evidence-based governance is not yet fully realised.

Figure 2.3. Government productivity and efficiency as well as user-driven services are the most prevalent goals underpinning public-sector data strategies

Percentage of OECD countries reporting selected goals in their public-sector data strategy, 2023 and 2025



Note: Does not include data for Germany and the United States.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/qcbwl3

2.4.2. Most countries have the basic tools for data management, but quality and coverage vary

Most OECD countries have put core data management tools in place, but their coverage varies across different areas. Standards for metadata (i.e., data describing other data), inventories, quality management and data sharing are crucial for turning high-level ambitions into consistent, scalable practice. They create a common language and set of repeatable processes: metadata standards make datasets findable and shareable; inventories show what data exists and where; quality standards ensure it can be reliably re-used; and sharing standards clarify how data can be accessed and protected. Without these tools, public sector organisations tend to rebuild the same solutions in parallel and collect the same data more than once – adding costs, effort and time, and reducing the reliability of information across government.

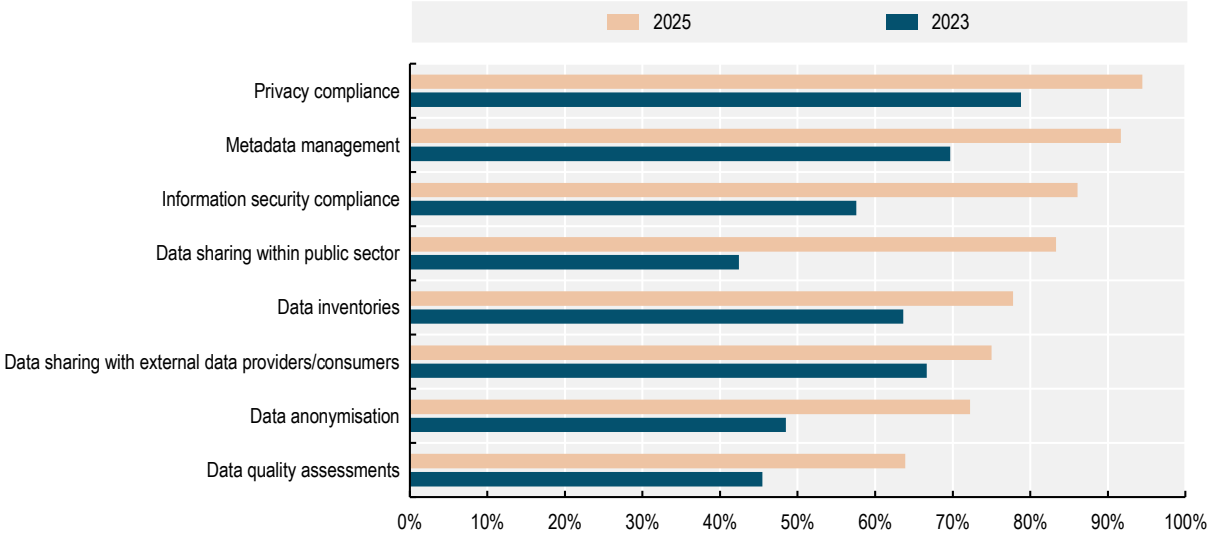
The 2025 DGI shows strong uptake of foundational standards, but with significant variation (Figure 2.4). Metadata management standards are the most widely adopted (33 of 36 countries, 92%), followed by data inventories (28 of 36, 78%) and standards for anonymising data to protect privacy (26 of 36, 72%). Standards supporting data sharing are also relatively widespread: 30 of 36 countries (83%) provide guidance for data sharing within the public sector and 27 of 36 (75%) for sharing with external entities. However, formal standards for assessing data quality are less common, with only 23 of 36 OECD countries (64%) reporting them in place. This pattern suggests that countries have prioritised the structural and legal enablers for data re-use – such as documentation, inventories and sharing arrangements – while more systematic approaches to assessing and improving data quality are still maturing. This matters because poor data quality limits how reliably data can be reused across institutions.

Formal data quality frameworks set criteria for assessing and comparing the quality of data across public bodies – a prerequisite for systematic, high-quality re-use of data across government. 2025 DGI evidence shows that such frameworks exist in countries including Australia, Canada, Chile, Colombia, Korea, Japan, and most Nordic and Western European countries. Among accession candidate countries, Peru reports having such a framework. Where they are absent, the cause may reflect limited capacity, decentralised approaches to data management, or reliance on sector-specific practices rather than government-wide guidance.

Privacy and security requirements are widely recognized, while the development of more detailed operational data management practices take longer to develop. According to the DGI, 34 of 36 countries (94%) have standards for privacy compliance and 31 of 36 (86%) have information security standards – areas in which legal obligations and risk considerations drive adoption. Several countries, including Australia, Canada, Chile, Colombia, Denmark, France, Italy, Japan, Korea, the Netherlands, Norway, Switzerland and the United Kingdom stand out for achieving comprehensive coverage across nearly all data management domains. Other countries have privacy and security standards in place but more limited guidance on data quality, inventories or sharing. Overall, the pattern shows that governments tend to address compliance-driven areas first, while the more operational, practice-oriented tools take longer to mature - limiting how fully data can be used for service integration, policy analysis and long-term operational reliability.

Figure 2.4. Privacy compliance and security are the most adopted data-management standards across OECD countries

Share of OECD countries with noted data management standards or guidelines for public servants, 2023 and 2025



Note: Covers only central/federal government level. Data not available for Germany or the United States. Refer to Annex Table 2.A.4 for comprehensive OECD and Accession country data.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/3m1zds

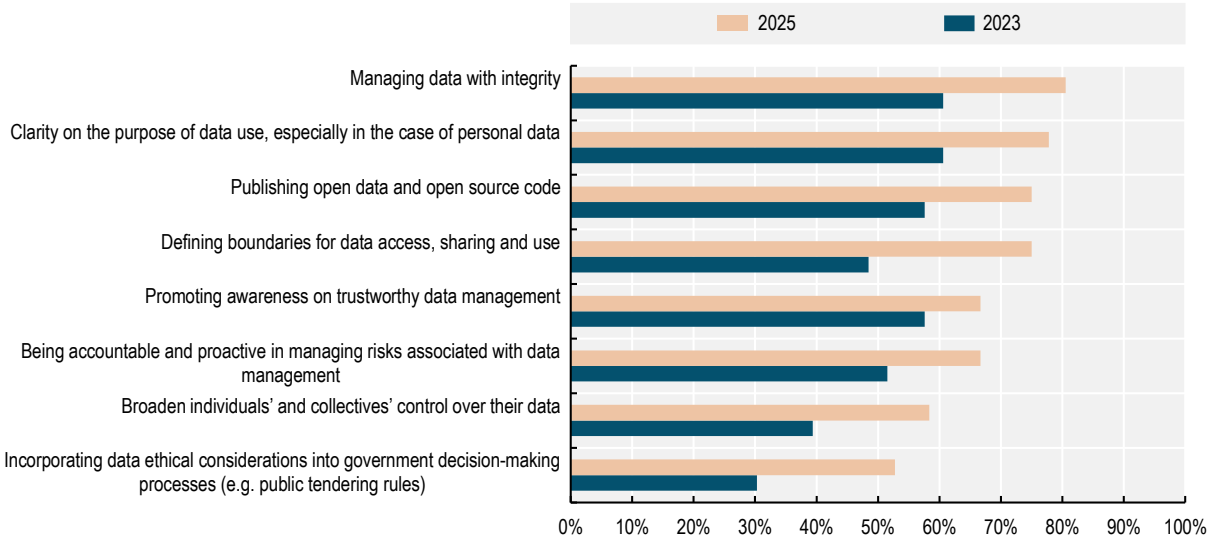
2.4.3. Government are increasingly building ethical data management principles

Public trust in how government handles data are not guaranteed – and once lost, it takes considerable time to rebuild. Guidance on ethical data use governance helps governments set clear boundaries, make decisions transparently, and use data in ways that are lawful, fair and safe. The OECD Trust Survey shows that around 52% of people are confident that public institutions use their personal data for legitimate purposes only. Against this backdrop, an increasing number of governments are adopting a "trust by design" approach – building safeguards into their data systems from the outset.

All OECD countries have a national data-protection authority responsible for enforcing privacy and personal data protection rules, and 30 of 36 (83%) report policy initiatives to promote ethical data management, in line with the OECD Good Practice Principles for Data Ethics in the Public Sector (OECD, 2021[20]). As shown in Figure 2.5, the most commonly implemented principle is managing data with integrity, reported by 29 of 36 OECD countries (80%). Incorporation of ethical data considerations into decision-making processes - such as procurement rules or how third parties handle personal data beyond the requirements of applicable data protection law - is less common, reported by 19 of 36 of OECD countries (53%). This suggests that ethical commitments are broadly established at the level of policy, but embedding them into day-to-day operational practice remains a work in progress.

Figure 2.5. Adoption of ethical data management principles is on the rise across OECD countries

Share of countries adopting selected ethical data management principles by public sector institutions across OECD countries, 2023 and 2025



Note: The figure presents the aggregated responses for OECD countries to the question "Which of the following principles are covered by the [available policy initiative(s) at the central/federal government level to promote ethical management of data across the public sector]?". Data not available for Germany or the United States.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/9ltrqj

2.4.4. Improving open government data availability, but value creation lags

Open government data – government data made freely available for anyone to access, use and share – continues to be a priority across OECD countries, in line with the OECD Recommendation on Enhancing Access to and Sharing of Data, which promotes making data as open as possible and as closed as necessary to protect legitimate interests (OECD, 2021[4]). When governed well, open data can, enable better data sharing across government and beyond, enhance transparency and drive innovation in the provision of public and private sectors based on open datasets. However, these benefits only materialise when open data are easy to find, access and re-use. Without these conditions, open data initiatives risk remaining symbolic – technically available but practically unused (Box 2.6).

OECD countries are improving availability and accessibility of open data, but support for re-use continues to lag. Evidence from the OECD OURdata Index shows progress in legal requirements and publication practices, but stakeholder engagement and impact monitoring remain weak. Almost all OECD countries, require public institutions to make data available as open data, and more than 80% mandate key accessibility conditions including the data to be available free of charge, under an open licence, in a machine-readable format, with standardised metadata, and updated in a timely manner. However, more advanced features that enable data to be used and integrated at scale – such as disaggregated data, Application Programming Interfaces (APIs) and publication through a central portal – are significantly less common. This gap limits how effectively governments, civil society, and businesses can make use of open data.

Box 2.6. Making open data accessible: Examples from Czechia and France

Czechia's National Open Data Catalogue provides a range of ways to explore and download geographic data, in alignment with the EU INSPIRE directive. Many datasets ca be accessed through application programming interfaces (APIs) that allow them to be integrated directly into applications and services to consult maps in a browser, alongside bulk download feeds for full extracts – making the data available for a wide range of purposes.

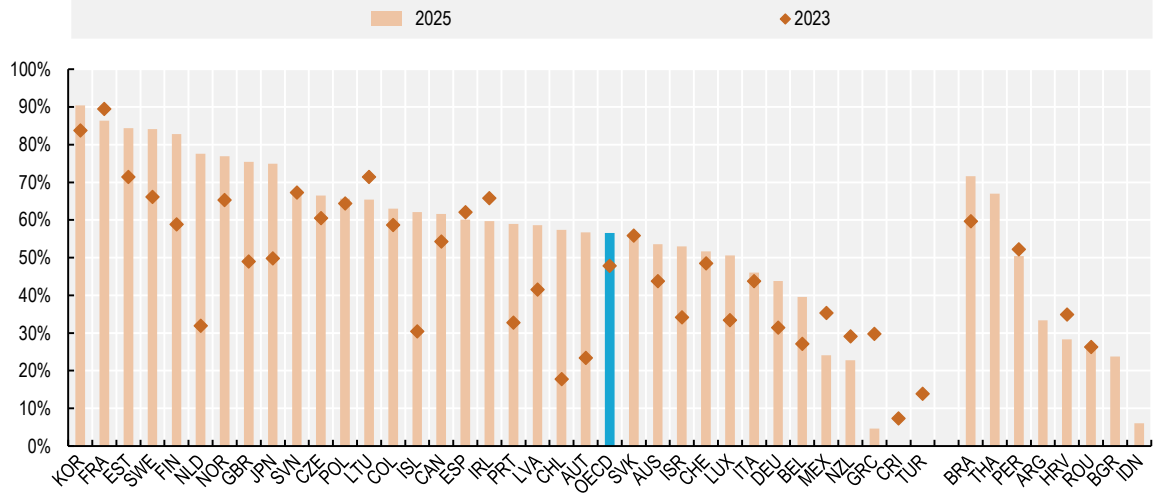
France makes it straightforward to access open government data through programmable interfaces. For tabular datasets published on data.gouv.fr, a built-in API is available to query a table, filter and preview the results directly on the portal without downloading files. The service code is publicly available under an open-source license to encourage reuse.

Source: (Government of the Czech Republic, n.d.[21]; Government of France, n.d.[22]).

Availability of high-value datasets is improving, but overall coverage remains incomplete. According to the 2025 OURdata Index, an average of 57% of high-value datasets across OECD countries are available as open data, up from 47% in the 2023 edition (see Figure 2.6). Availability of high-value datasets varies widely across domains, with persistent gaps in data related to government integrity (see Figure 2.7). OECD countries perform best for geospatial (73% in 2025, up from 67% in 2023) and statistical (74%, up from 67%) data. In contrast, data on companies (34%, up from 31%), government finances and accountability (38%, up from 27%), and health and social welfare (53%, up from 42%) remain significantly under-published. The least commonly published datasets in open data format include hospitality and gifts records (17%), declarations of assets (14%) and interests (9%) by senior public officials, and company ownership information (9%) – areas where stronger transparency could support accountability and public trust. Furthermore, these results are consistent with the limited availability of datasets on declaration of interests and assets, regardless of format, as presented in the OECD Integrity and Anti-Corruption Outlook - with both available in fewer than 33% of OECD countries (OECD, 2026[23]).

Figure 2.6. Availability of open high-value datasets has improved across OECD countries

Average availability of 10 types of high-value datasets as open data per country, 2023 and 2025



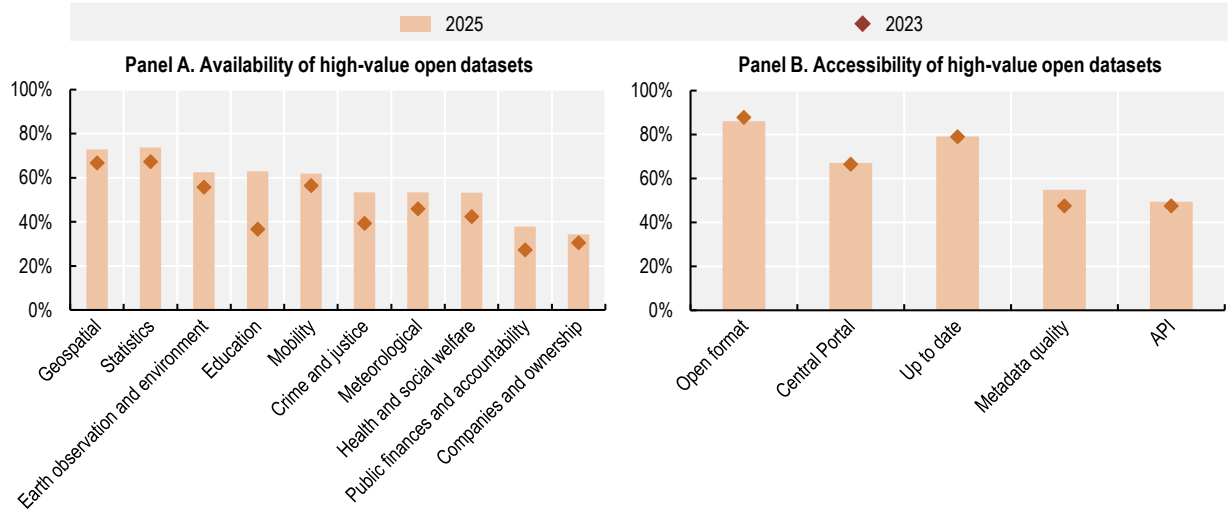
Note: The categories of high-value datasets are determined by the OECD primarily based on the G8 Open Data Charter. Data are considered available if it is machine-readable, free of charge and provided with an open license. 2025 data not available for Denmark, Hungary and the United States. 2023 data not available for Hungary and the United States, while for Denmark it is not included in this chart. 2025 data cover 01 January 2023 to 31 December 2024. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023. Refer to Chapter 1 Annex for the full list of datasets.

Source: OECD Survey on Open Government Data 6.0 (2025) and (OECD, 2023[24]).

StatLink https://stat.link/ce0mwj

Figure 2.7. High-value open datasets are more available and equally accessible in 2025

OECD average, 2023 and 2025



Note: The categories of high-value datasets are determined by the OECD primarily based on the G8 Open Data Charter. Data are considered available if they are machine-readable, free of charge and provided with an open license. 2025 data not available for Denmark, Hungary or the United States. 2023 data not available for Hungary or the United States, while for Denmark it is not included in this chart. 2025 data cover 01 January 2023 to 31 December 2024. Refer to Chapter 1 Annex for the full list of datasets.
Source: OECD Survey on Open Government Data 6.0 (2025) and (OECD, 2023[24]).

StatLink https://stat.link/qncdal

Accessibility is also improving, though important gaps remain. In 2025, an average of 67% of available high-value datasets were accessible through a central/federal open-data portal - a slight increase from 66% in 2023. Access from a central portal, made possible through harvesting mechanisms, improves discoverability and avoids duplication. Metadata quality has also improved, showing broader alignment with standards such as DCAT or DCAT-AP in Europe, which enables harvesting between portals. However, access through APIs – which allow systems and applications to retrieve data automatically – remains limited, with an OECD average of 49% of high-value datasets offering this capability. This restricts more sophisticated or automated forms of data use. Publication in open, non-proprietary formats also declined slightly, which needs to be addressed to ensure data interoperability.

2.4.5. Stakeholder engagement and impact assessment remain underdeveloped

Stakeholder engagement is a common feature of data governance across OECD members, but practices are more limited and less mature when it comes to open data specifically. According to the DGI, 92% of OECD countries have consulted at least one stakeholder group in developing their public sector data strategy, most commonly civil servants. This reflects growing recognition that incorporating people's views often produces better, more trusted outcomes. However, this engagement does not extend consistently to open data, where involvement of external users remains limited.

To make open data genuinely useful, governments need to understand what different users — businesses, civil society organisations, researchers, journalists and citizens, actually need and which datasets would create the most value. Yet only 8 of 35 OECD countries (23%) require regular consultation on open data plans. When engagement does occur, it tends to prioritise internal actors, leaving the people most likely to use the data with limited influence over what gets published and how.

Measuring the impact of open data also remains limited. The average score for impact monitoring in the OURdata Index increased from 0.29 in 2023 to 0.37 in 2025 – a positive trend but from a low base. Only a minority of OECD countries evaluate the economic (11 of 35 countries, 31%), public sector (9 of 35, 26%), or social (4 of 35, 11%) impact of open government data. Without this information it is difficult to prioritise investment in open data, demonstrate its value to decision-makers or identify where efforts are falling short.

These gaps point to a broader pattern: governance structures for data are in place, but the operational practices that turn data into value - systematic engagement with users, targeted release of high-priority datasets and regular measurement of outcomes - are still developing.

2.4.6. Data are used more for oversight than for service improvement, and this matters for AI

Government-wide initiatives on data use are widespread across OECD governments, but its depth varies significantly depending on the function. Data are most consistently used in strategic oversight and planning. According to the DGI, 34 of 36 (94%) OECD countries report having government-wide initiatives to use data for policy monitoring and evaluation, and 33 of 36 (92%) use data to anticipate and plan government interventions. These high levels reflect long-standing administrative routines and well-institutionalised processes in areas such as budgeting, performance management and regulatory oversight, where using data to track results and demonstrate compliance has long been standard practice.

Data use is especially pronounced in public procurement and financial management, where governments have strong incentives – and often legal obligations – to monitor spending, detect irregularities and optimise resource allocation. These are also areas where data tends to be more standardised and easier to analyse (see Section 5.5.2 in Chapter 5).

By contrast, system-wide initiatives to use data to improve how services are designed and delivered are prevalent. While 29 of 36 (80%) OECD countries report having government-wide initiatives to use data for service design and delivery, only 16 of them (44%) analyse how people actually use services. This reflects several practical challenges: service delivery responsibilities are often fragmented across institutions; data standards are inconsistent; feedback loops that capture how people experience services are frequently absent; legacy systems lack capacity to collect or share usage data; service teams often lack dedicated analytical capacity. As a result, the potential for data to improve user experience, enable more proactive service delivery or support workforce planning remains largely untapped.

These patterns matter directly for the use of AI in government (Chapter 4). The OECD (2025[25]) *Governing with AI* report finds that most public-sector AI initiatives remain in exploratory or pilot phases, and that difficulties accessing, sharing and using high-quality data are a common barrier. In areas where data are already well structured, consistently governed and routinely collected, such as tax administration and financial management, AI applications are more likely to be scaled successfully. In areas where data are fragmented, incomplete or unevenly managed, such as service design and delivery, AI deployment tends to be slower. Readiness for AI also depends on whether data can be accessed and used lawfully and are protected by appropriate safeguards. AI development requires balancing the need for large and wide-ranging datasets with compliance with privacy, data protection and intellectual property rules, alongside ensuring traceability and accountability in data use (OECD, 2025[26]). This reinforces a central point: improving data quality, enabling data sharing and supporting reuse are not just good governance practices - they are the precondition for AI to be used reliably and at scale across government.

2.5. Interoperability of data and digital infrastructure is expanding but is still unevenly embedded

Interoperability allows different digital systems to connect, communicate and exchange information with one another. It is what makes it possible for data held by one government agency to be used securely by another, without demanding people provide the same information again. For governments, interoperability determines whether digital infrastructure can actually deliver joined-up services, reduce administrative burdens and enable data to flow where it is needed.

Interoperability requires agreed governance arrangements between actors, clear rules for data sharing, semantic standards, and appropriate technical tools. Without these arrangements, even well-designed systems tend to operate in isolation, and the potential benefits of shared digital infrastructure go unrealised.

2.5.1. Domestic interoperability: Progress is real, but use of shared systems remains uneven

Interoperability is increasingly underpinning the delivery of essential public services and the day-to-day operation of government. When public services are built on interoperable digital systems (Chapter 5), people and businesses do not have to repeatedly provide the same information, can navigate integrated platforms and engage with multiple authorities for what is effectively a single service journey. For governments, high interoperability reduces operational costs, speeds processes and enhances the ability to use data strategically across the public sector. Yet interoperability and linking data to improve benefit and service delivery remain the exception, not the rule, in areas such as social protection (see, for example, Chapter 3 in (OECD, 2024[27]).

As digital government matures, interoperability is shifting from a narrow technical concern to a core governance issue that shapes how policies are executed and how value is created through data reuse. DPI components only generate value when they are connected and usable across institutions and levels of government. Likewise, data policies that promote access, sharing and re-use depend on common standards, clear interfaces and aligned legal and organisational arrangements. Interoperability is therefore best understood as a system property – something that has to be actively maintained through governance, not achieved once through a technical integration effort.

Building interoperability across government requires moving beyond one-off connections between individual institutions toward shared, reusable building blocks. These include authoritative reference data and registers, shared standards, and interfaces that make data and services accessible across organisational boundaries. Equally important are the governance arrangements that clarify responsibilities for stewardship, verify compliance with standards, and assign operational accountability when multiple institutions rely on shared capabilities. Strengthening these enablers is essential for governments to reduce fragmentation, scale integrated services and support more advanced uses of data such as proactive service delivery, risk-based regulation or AI-driven analytics.

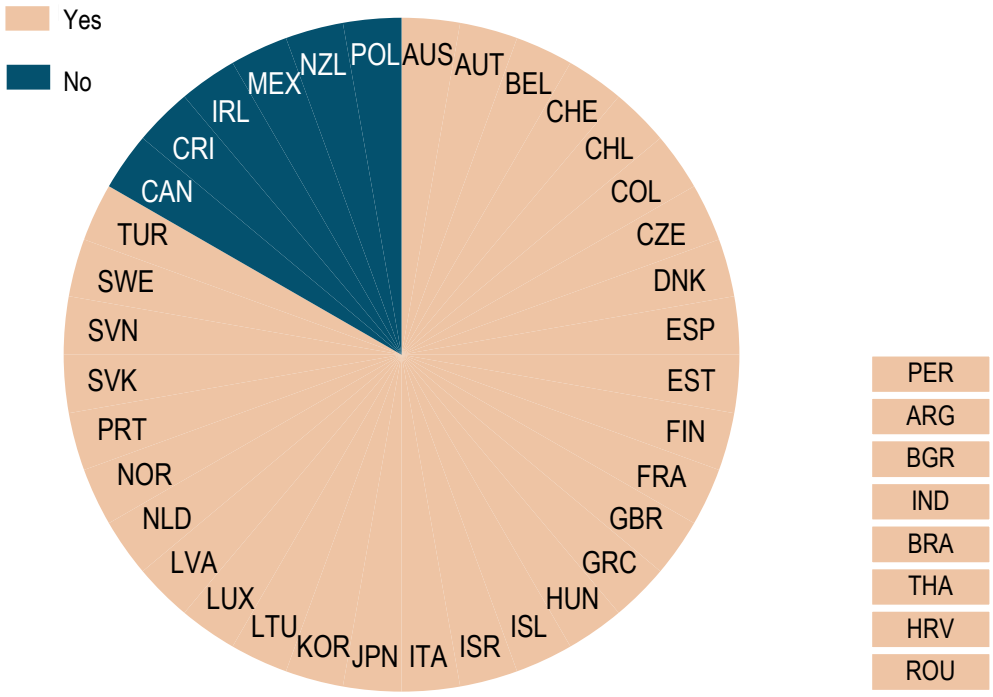
Interoperability systems – the shared technical platforms that allow data to be exchanged across government - are now in place in 30 out of 36 OECD countries (83%) (Figure 2.8). Out of those 30 countries, 23 report widespread usage of the data interoperability system across over 50% of public sector institutions at central government level (63%), while the seven remaining countries report lower usage figures. At subnational government level, the adoption rates of data interoperability systems are even lower.

This shows that the existence of a system is not sufficient to deliver impact, and governments need to put in place incentives for adoption, require compliance with shared standards and ensure sustained investment in maintaining shared components over time. Without these elements, data sharing risks remaining formal rather than functional – technically possible but rarely used, difficult to scale and insufficient to deliver integrated services or reduce administrative burdens. Ensuring that cross-government data sharing is consistent and resilient requires a strategic, long-term governance approach rather than isolated technical solutions.

Furthermore, organisational silos can be one of the most persistent barriers to interoperability and data sharing, and dismantling them requires solid governance and co-ordination arrangements (OECD, 2025[28]; OECD, 2020[29]). Regulatory fragmentation can also hinder data sharing, as governments must navigate overlapping and sometimes conflicting requirements across data protection, cybersecurity, competition and sector-specific frameworks, making cross-regulatory cooperation mechanisms, such as joint sandboxes or digital regulation forums, increasingly important. The efficiency gains that integration promises can also mean the loss institutional relevance or roles, creating incentives to resist the very changes that would make government work better.

Figure 2.8. Eight in ten OECD countries have government-wide data interoperability systems in place

Availability of a data interoperability system, 2025



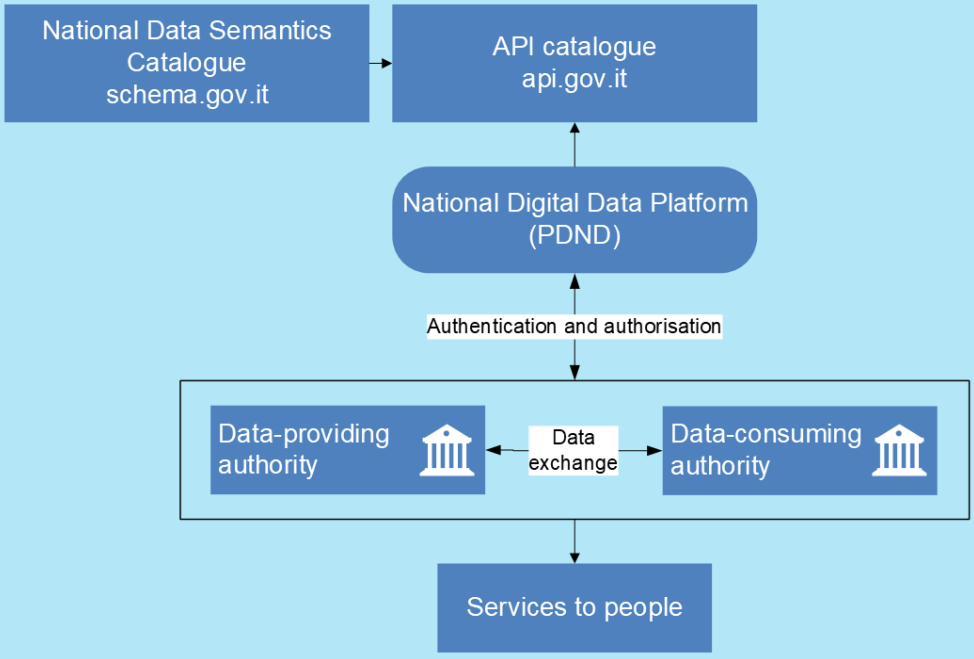
Note: Data not available for Germany and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/h9jq8o

Box 2.7. Implementing data interoperability in Italy and Japan

Italy's National Digital Data Platform (PDND) enables the interoperability of information systems among public and private bodies, implementing the once-only principle. Institutions publish application programming interfaces (APIs) on the api.gov.it catalogue and authorise use based on tokens that create a traceable record of data exchanges. The platform currently connects over 9 000 entities, including central government bodies, subnational governments, universities and private actors. In practice, this means people can have personal pre-filled in forms and eligibility for benefits checked automatically, without needing to submit documents repeatedly.

Figure 2.9. Interoperability of Italian Public Administration



Note: OECD based on Italian government sources
Source: (Government of Italy, n.d.[30])

Japan's Digital Agency manages the Co-operation Network System (NWS) for Personal Information, which allows government institutions to exchange personal data associated with individual identification numbers. This means users can avoid submitting multiple documents – such as certificates of residence or tax records - when completing various administrative procedures. To protect privacy, access to the system is limited to public sector bodies. The system does not store personal information itself; it transmits specific data held separately by individual public organisations, keeping information decentralised.

Source: (Government of Italy, n.d.[30]; Government of Japan, n.d.[31]; OECD, 2024[32]).

2.5.2. Cross-border interoperability: Building the foundations for services that work across borders

Making digital systems work across national borders is significantly more complex than making them work within a single country. Within a country, government institutions typically operate under the same legal framework, follow the same governance rules and share institutional arrangements. Across borders, governments must align across different legal systems, regulatory requirements, and trust models even when they use similar technical standards or digital infrastructure. Technical interoperability alone is not sufficient without legal interoperability, making it essential to align data governance frameworks and engage in international regulatory cooperation to ensure data can flow securely across jurisdictions (OECD, 2023[33]). This makes cross-border interoperability harder to achieve and more sensitive to gaps in governance.

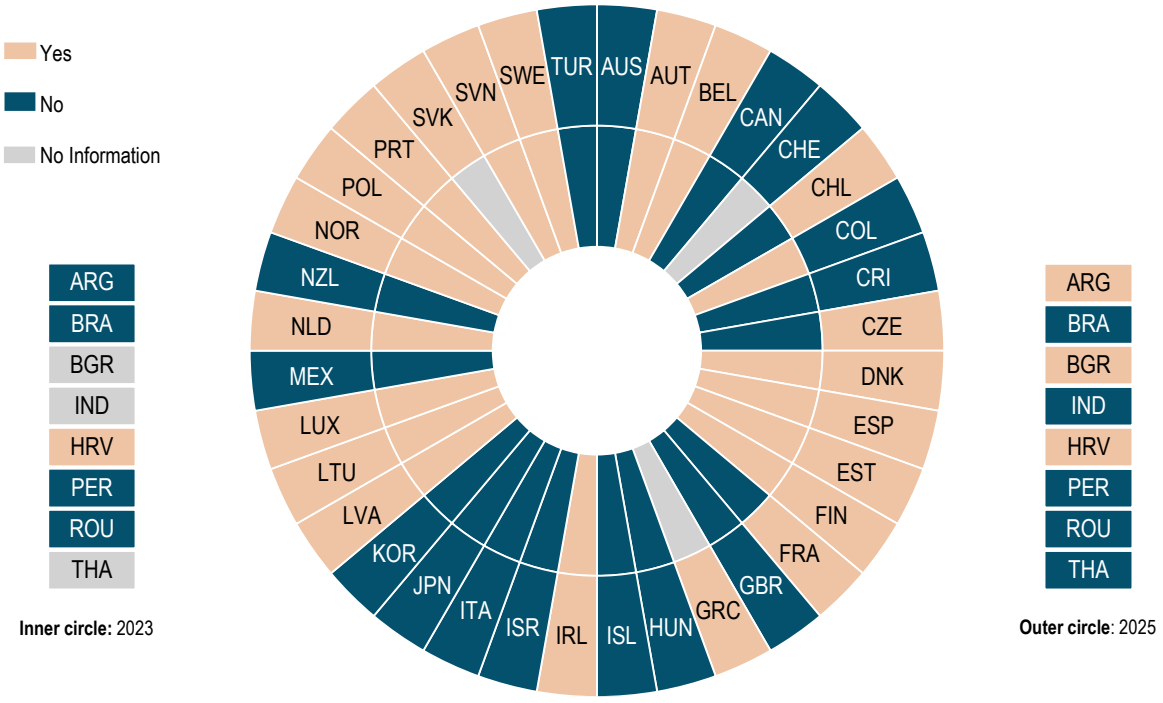
Common technical standards and protocols are a necessary starting point as they make systems technically compatible. But cross-border interoperability ultimately depends on building a shared foundation of institutional trust, mutual recognition of each other's systems, clear liability frameworks, and harmonised protections for privacy, security and personal data.

Digital identity is central to this effort. A trusted, reliable way of identifying and authenticating people and businesses across borders allows governments to exchange data in controlled, verifiable ways, supports the delivery of cross-border services, and underpins emerging policy efforts such as the portability of entitlements, smoother cross-border mobility and international transactions.

Figure 2.10 illustrates the extent to which OECD Members and accession candidate countries have moved from domestic digital identity arrangements toward mechanisms that support cross-border recognition and use. These developments mark early but important steps, largely driven by EU policies to strengthen the cross-border operation of digital identity systems and wallets (Box 2.8). Countries with more mature domestic digital identity systems and clearer governance foundations tend to advance more rapidly, while those with more fragmented identity ecosystems face greater challenges in extending their systems beyond national boundaries. As digital identity matures, its cross-border functionality will increasingly determine governments' ability to deliver seamless services to people who live, work or move across borders.

Figure 2.10. Almost six out of ten OECD countries are providing cross-border digital identity, mostly in OECD-EU countries

Availability of access to public services using foreign digital identity solutions, 2023 and 2025



Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/zg4ftq

Box 2.8. The EU's eIDAS 2.0 and the European Digital Identity Wallet

In May 2024, the European Union adopted Regulation (EU) 2024/1183, known as eIDAS 2.0, establishing the most ambitious cross-border digital identity framework among OECD countries. The regulation requires all 27 EU member states to provide citizens, residents, and businesses with at least one European Digital Identity Wallet (EUDI Wallet) by the end of 2026. The wallet will create a harmonised system where credentials issued in one country = such as driving license or professional qualification - are recognised and usable across all others. The regulation also addresses governance and accountability: member states bear responsibility for failure to comply with their obligations.

The EUDI Wallet goes beyond basic identity verification. It enables users to store and selectively share verified credentials, such as national identity data, driving licences, professional qualifications, health records, and educational diplomas, with both public and private service providers. Built on privacy-by-design principles, the wallet gives individuals control over what information they share and with whom.

Cross-border interoperability is central to the framework. The Architecture and Reference Framework (ARF) establishes common protocols, data formats, and security requirements to ensure wallets function seamlessly across member states. Between 2023 and 2025, four large scale pilots tested real-world cross-border use cases involving over 250 organisations across nearly every EU Member state plus Norway, Iceland, and Ukraine. In December 2025, the first large-scale compatibility testing between national wallet implementations confirmed that cross-border interoperability is technically achievable when common standards are rigorously applied.

Source: (OECD, 2024[8]; OECD, 2025[34]).

As interoperability scales and reliance on shared components grows, the choices governments make about resilience and sustainability – including how they use cloud technologies and open-source software – become increasingly important for continuity, security and the ability to maintain shared infrastructure over time.

2.6. Resilience and sustainability: Cloud technologies and open-source software

As governments rely more heavily on shared digital systems, the choices they make about how those systems are developed, hosted, maintained and updated become increasingly important. Two enablers stand out: cloud technologies and open-source software. Both can strengthen the reliability, flexibility and long-term sustainability of digital government, The value they create depends on the governance choices that surround them: clear rules, sustained funding, the right skills and well-defined responsibilities for maintenance and security.

2.6.1. Cloud technologies: A foundation for reliable and adaptable government

Cloud technologies refer to the delivery of computing resources – such as storage, processing power and software – over a network, on demand. Rathen than owning and running all the underlying infrastructure themselves, organisations can access what they need when they need it, and scale up or down as requirements change.

For governments, cloud technologies have become important tools for making digital services more reliable and adaptable. They provide the capacity to handle surges in demand – for example when large numbers of people access a service at the same time – and support fast recovery when systems go down. Cloud technologies also make it easier to introduce new capabilities, update services and maintain consistent security standards across a complex landscape of government systems. These benefits apply in normal operations as much as in exceptional circumstances: a government that can scale services quickly, recover from failures efficiently and update systems with fit-for-

purpose procurement processes is better placed to serve people reliably day to day, not only in crisis.

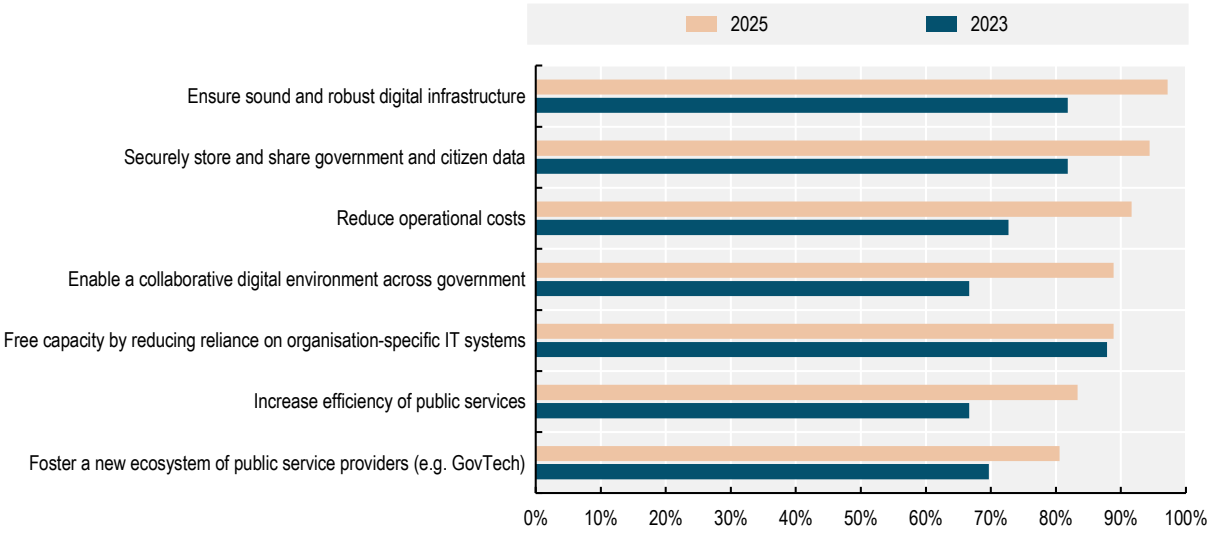
As of 2024, all OECD countries surveyed except Sweden report a strategy to promote cloud technologies adoption in the public sector. The objectives behind these strategies show strong convergence (Figure 2.11). Ensuring robust, secure and continuously available digital infrastructure is the most consistently cited priority, reflecting the central role of cloud technologies in strengthening operational continuity and secure data storage. Governments also highlight the importance of secure data sharing, as cloud environments can support shared platforms and reusable components – foundations for scaling public infrastructure across government institutions.

Cloud technologies' contribution to reliable service delivery is visible across a range of situations. During the COVID-19 pandemic, digital government proved crucial to maintaining continuity of public sector operations and the provision of essential services to individuals and businesses. Similarly, cloud-based back-up and recovery environment allow governments to restore services more quickly after outages or cyber incidents, reducing disruption for users and public servants alike.

Countries also increasingly use cloud computing to modernise ageing IT systems and reduce fragmentation. This includes developing approaches that allow governments to balance scalability of cloud technologies with requirements around data storage location, security and strategic autonomy – sometimes referred to as sovereign cloud models. At the same time, cloud strategies aimed to improve efficiency: reducing operational costs, enabling reuse of common components, and supporting more responsive services. Cloud technologies are therefore no longer treated as a purely technical upgrade but as a strategic instrument to prepare public administrations for more data-intensive, AI-enabled and integrated service delivery.

Figure 2.11. Security and resilience are the most prevalent reasons OECD countries are adopting cloud technologies in government

Percentage of OECD countries reporting selected objectives for public cloud infrastructure strategies, 2023 and 2025



Note: Data not included for Germany, Sweden or the United States.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/elutpv

Most OECD countries provide shared cloud infrastructure that can be reused across the public sector, signalling a shift toward more centralised and scalable digital foundations. Data from the 2025 DGI shows extensive coverage: 83% of OECD countries (30 out of 36) have shared cloud storage initiatives, 86% (31 countries) provide shared cloud computing environments and hosting services. Around two-thirds of OECD accession candidate countries report similar capabilities. This marks a clear movement away from agency-specific cloud projects and toward common, reusable services that can support government-wide modernisation, bring greater consistency to security and operations, and form a more resilient digital public infrastructure.

However, countries vary in how far cloud strategies drive deeper structural change. While many governments use cloud computing to modernise and stabilise existing systems – improving availability, performance and cost-efficiency – fewer explicitly use it to address the fragmentation of legacy technology or to open up markets to a wider range of suppliers, including smaller technology companies. These more ambitious objectives require technical migration and changes to governance, procurement models, workforce capabilities and budgeting practices. The uneven emphasis on these goals suggests that many governments view cloud adoption primarily as an incremental improvement rather than an opportunity to fundamentally redesign the architecture and long-term sustainability of their digital systems.

This reinforces the need to treat security, risk management and operational continuity as core elements of cloud governance, not as separate concerns to be manged elsewhere. As more services depend on shared cloud infrastructure, governments face new risks from concentration – too many critical functions depending on too few systems or suppliers. They need clear accountability for security, incident response and continuity across all participating organisations. Many governments are currently running a mixture of cloud and traditional on-site systems - a common transitional state that can introduce uneven security standards and complex dependencies if not actively managed. Gradually reducing reliance on outdated systems while maintaining operational stability is essential to ensure that cloud adoption strengthens rather than inadvertently weakens overall digital resilience.

2.6.2. Open-source software: Growing adoption, but governance determines the benefits

Open-source software (OSS) refers to software whose underlying code is publicly available for anyone to inspect, use, modify and share, subject to certain conditions. Unlike proprietary software, open-source software can be distributed, adapted, re-used and built upon by anyone with the skills to do so.

For governments, OSS offers several potential advantages. It can reduce dependence on single suppliers, making it easier to switch providers or bring capabilities in-house. It supports interoperability by enabling systems to be built on shared, openly documented standards. It improves the ability to verify the security and reliability of critical systems, since the underlying code can be independently inspected. It also enables reuse of software components across sectors and across borders, reducing duplications and lowering costs (see Box 2.9).

However, realising these benefits requires sound governance. Adopting open-source software without a plan for maintaining it, funding it sustainably and assigning clear responsibility for security can create as many problems as it solves. Governments need clear procurement guidance, staff with the right technical skills, reliable funding for ongoing maintenance, defined responsibilities for keeping code secure and policies that encourage collaboration across organisations. Without these enablers, OSS risks being adopted as a cost-cutting measure without the long-term stewardship needed to make it a genuine strength.

Box 2.9. Cross-border collaboration through open-source software

Open-source software can lower barriers to cross-border collaboration by making code transparent, in line with standards, openly documented and free from dependency on closed platforms.

France, **Germany**, and the **Netherlands** are co-developing a digital workplace for civil servants, implemented nationally as LaSuite (France), openDesk (Germany) and Mijn Bureau (The Netherlands). The three countries share development roadmaps, reuse each other's code and use open communication protocols to ensure secure, compatible tools across all three implementations.

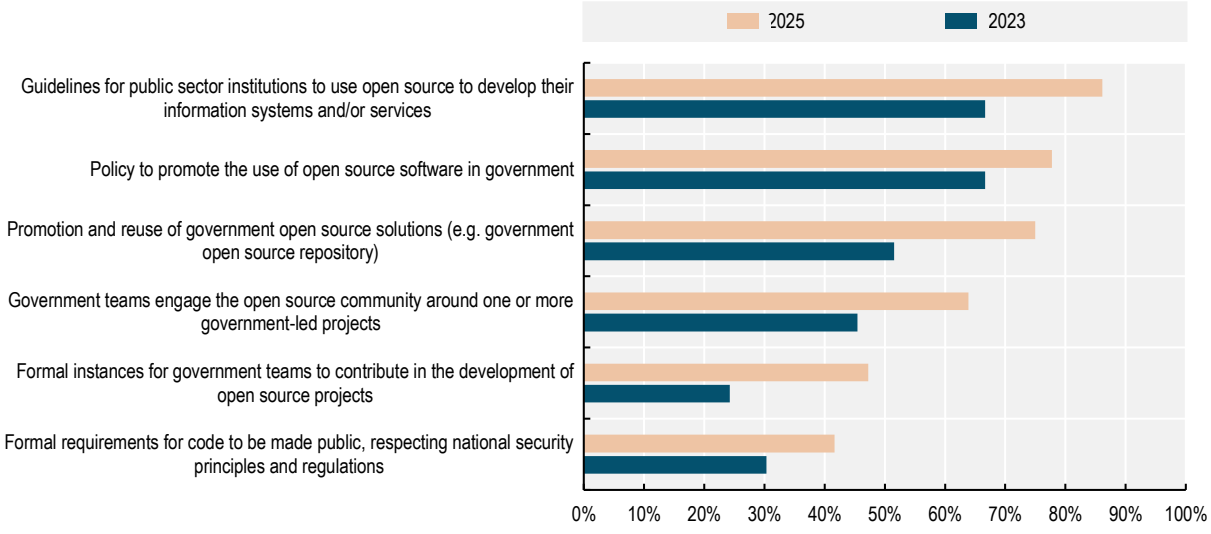
Governance is distributed: in France, the Interministerial Digital Directorate (DINUM) steers development; in Germany, the Centre for Digital Sovereignty (ZenDiS) manages the program under a federal sovereign workplace initiative; in the Netherlands, the Ministry of the Interior and Kingdom Relations (MinBZK) co-ordinates with local authorities including the City of Amsterdam.

This collaboration demonstrates how open-source approaches can support both national digital sovereignty and cross-border reuse, reducing costs and increasing transparency without requiring countries to adopt identical systems.

Source: (Government of France, n.d.[35]; Government of Germany, n.d.[36]; Government of the Netherlands, n.d.[37]).

Figure 2.12. Initiatives to promote the adoption of use of open-source technologies in government have expanded significantly across OECD countries

Percentage of OECD countries reporting selected policies and practices related to open source, 2023 and 2025



Note: Covers only central/federal government level. Data not available for Germany or the United States.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/s4wocj

Data from the 2025 DGI shows increased prioritisation of OSS across OECD governments. In 2025, 28 out of 36 (78%) OECD countries reported a national or federal government policy to promote the use of open-source software, an increase from 67% in 2023. These policies are often complemented by guidance for public bodies on using open-source to develop their own systems and services: 31 out of 36 (86%) OECD countries reported such guidelines in 2025, up from 67% in 2023. Other measures are also becoming more common, including central repositories of open-source software available for government use, formal arrangements for government teams to contribute to OSS projects, and requirements to publish code publicly (Figure 2.12).

Box 2.10. Open-Source Programme Offices in the Netherlands and Czechia

Open-Source Programme Offices (OSPO) are teams involved in the co-ordination of efforts around open-source software. Setting up OSPOs in governments can steer governance, development of software, stakeholder engagement and international co-operation.

The Netherlands established an OSPO at the Ministry of Interior and Kingdom Relations in 2023, with a mandate to advance the government's "open, unless" policy and improve transparency, security and efficiency. The office curates and publishes major government open-source projects including the NL Wallet, the public Algorithm Register, and the Mijn Bureau office suite developed jointly with France and Germany. It also works to remove internal barriers to open-source adoption and engages with the wider community through a dedicated platform and public online presence.

Czechia launched its national OSPO in 2024 to organise and co-ordinate open-source use across public administration and foster collaboration between the public sector and academia. Its secretariat, hosted by the Open Cities association, provides technical, legal and methodological support for open and modular digital solutions at the local government levels. The national Open Code Portal code.gov.cz aggregates and shares public-sector projects. Security guidance is provided jointly by the National Cyber and Information Security Office and the Ministry of the Interior through non-binding recommendations for secure, open-source development in public administration.

Source: (Opensourcewerken, n.d.[38]; Open Source Program Office (OSPO), n.d.[39]; Ministry of the Interior and Kingdom Relations (MinBZK), n.d.[40]; Otevřená města, n.d.[41]; Otevřená města et al., 2022[42]; NÚKIB, 2022[43]).

Annex 2.A. Additional tables with country data

Annex Table 2.A.1. Availability of digital public infrastructure

Country	Digital post[1]		Digital Notifications		Digital payments		Data sharing		Single digital gateway		Digital identity providing access to +50% of services	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
Australia	●	●	●	●	●	●	●	●	●	●	●	●
Austria	●	●	●	●	●	●	●	●	●	●	●	●
Belgium	●	●	●	●	●	●	●	●	●	●	●	●
Canada	○	○	●	●	○	○	●	○	●	●	○	○
Chile	○	○	○	●	○	●	●	●	●	●	●	○
Colombia	○	○	○	○	●	○	●	●	●	●	○	○
Costa Rica	○	○	○	○	○	○	○	○	●	●	○	○
Czechia	●	●	○	●	●	●	●	●	●	●	●	●
Denmark	●	●	●	●	●	●	●	●	●	●	●	●
Estonia	●	●	○	●	○	○	●	●	●	●	●	●
Finland	●	●	●	●	●	●	●	●	●	●	●	●
France	○	○	○	○	○	●2	●	●	●	●	○	●
Greece	N/A	●	N/A	●	N/A	●	N/A	●	N/A	●	N/A	○
Hungary	●	●	●	●	●	●	●	●	●	●	●	○
Iceland	●	●	●	●	○	●	●	●	●	●	●	●
Ireland	●	●	●	●	○	●	●	○	●	●	○	●
Israel	○	○	○	○	●	●	●	●	●	●	○	○
Italy	●	●	●	●	●	●	●	●	○	●	○	●
Japan	○	●	○	●	○	●	●	●	●	●	●	○
Korea	●	●	●	●	●	●	●	●	●	●	●	●
Latvia	●	●	●	●	●	●	●	●	●	●	●	●
Lithuania	○	○	●	●	○	●	●	●	●	●	●	●
Luxembourg	○	●	○	●	○	○	●	●	●	●	●	●
Mexico	●	●	●	●	●	●	○	○	●	●	●	●
Netherlands	○	●	○	●	○	○	●	●	○	○	●	●
New Zealand	○	○	○	●	○	○	○	○	○	○	○	○
Norway	●	●	●	●	○	○	●	●	●	●	●	●
Poland	○	○	○	○	○	○	○	○	○	○	●	●
Portugal	○	●	○	●	○	●	●	●	●	●	●	●
Slovak Republic	N/A	●	N/A	●	N/A	○	N/A	●	N/A	●	N/A	●
Slovenia	●	●	○	○	●	●	●	●	●	●	●	●
Spain	○	●	●	●	●	●	●	●	●	●	○	●2
Sweden	●	●	○	○	●	●	●	●	○	○	●	●
Switzerland	N/A	●	N/A	●	N/A	○	N/A	●	N/A	●	N/A	○
Türkiye	●	●	●	●	●	●	●	●	●	●	●	●
United Kingdom	●	●	●	●	●	●	○	●	●	●2	●	●

Country	Digital post[1]		Digital Notifications		Digital payments		Data sharing		Single digital gateway		Digital identity providing access to +50% of services	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
OECD Total												
● Yes	19	27	18	29	18	24	28	30	28	31	24	25
○ No	14	9	15	7	15	12	5	6	5	5	9	11
No Information	3		3		3		3		3		3	
Argentina	○	○	●	●	○	●	●	●	●	●	●	○
Brazil	○	○	●	●	●	●	●	●	●	●	●	●
Bulgaria	N/A	○	N/A	●	N/A	●	N/A	●	N/A	○	N/A	○
Croatia	○	○	○	○	○	○	●	●	●	●	●	●
Indonesia	N/A	○	N/A	○	N/A	●	N/A	●	N/A	○	N/A	○
Peru	○	●	○	●	●	●	●	●	●	●	○	○
Romania	○	○	○	○	○	○	●	●	●	●	○	○
Thailand	N/A	○	N/A	○	N/A	○	N/A	●	N/A	○	N/A	○

Note: Single digital gateway: availability of a catalogue of services accessible to users. Data sharing: availability of a data interoperability system. Digital identity: at least 50% of national online public services can be accessed through a digital identity solution with two-factor authentication. 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
1. Some countries, including France, offer digital post through multiple different systems.
2. Data were updated following a request from the country after the publication of the 2025 DGI; therefore, these changes are not reflected in the 2025 DGI results.
Source: OECD (2025) Survey on Digital Government 3.0.

Annex Table 2.A.2. Authentication methods for digital identity solutions

Availability of methods for authentication exist among the current digital identity solutions to access public services

Country	Username and password		Smartcard		Digital certificate file		SMS 2FA		Email 2FA		App 2FA		Other	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
Australia	●	●	○	●	●	●	●	●	●	●	●	●	○	●
Austria	○	○	○	○	○	○	○	○	○	○	●	●	○	○
Belgium	●	●	●	●	●	●	●	●	●	●	●	●	○	○
Canada	●	●	○	○	○	○	●	●	○	●	●	○	○	○
Chile	●	●	○	●	○	●	○	○	○	○	○	○	○	●
Colombia	●	●	○	○	○	○	○	○	●	●	●	●	○	○
Costa Rica	●	●	○	○	○	●	○	○	●	●	○	○	○	●
Czechia	●	○	●	●	●	●	●	●	○	○	●	●	●	●
Denmark	●	●	○	○	○	○	○	○	○	○	●	●	●	●
Estonia	○	○	●	●	●	●	○	○	○	○	○	●	●	●
Finland	○	●	●	●	●	●	○	○	○	○	●	●	●	●
France	●	●	○	●	○	●	○	○	○	●	●	○	●	●
Greece	N/A	●	N/A	●	N/A	○	N/A	○	N/A	○	N/A	●	N/A	○
Hungary	●	○	●	○	○	○	○	○	○	○	●	●	●	●
Iceland	○	○	●	●	●	●	○	○	○	○	●	●	○	○
Ireland	●	●	○	○	○	○	○	○	○	○	○	●	●	●
Israel	●	●	●	●	●	●	●	●	●	●	●	●	○	○
Italy	●	●	●	●	●	●	○	○	○	○	●	●	○	○
Japan	○	●	●	●	○	●	○	●	○	○	○	●	○	○
Korea	○	○	○	○	●	●	●	●	○	○	●	●	○	○

Country	Username and password		Smartcard		Digital certificate file		SMS 2FA		Email 2FA		App 2FA		Other	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
Latvia	○	●	●	●	○	○	○	○	○	○	○	●	○	○
Lithuania	○	○	●	●	●	●	○	○	○	○	○	○	○	○
Luxembourg	○	○	●	●	○	○	○	○	○	○	●	●	●	○
Mexico	○	●	○	○	●	○	○	○	●	○	●	○	○	●
Netherlands	●	●	●	●	○	○	●	●	○	○	○	●	●	●
New Zealand	●	●	○	○	○	○	●	●	○	●	●	○	○	○
Norway	●	●	●	●	●	●	●	●	●	●	●	●	○	○
Poland	●	●	○	●	●	●	●	●	●	●	●	●	○	○
Portugal	●	●	●	●	●	●	●	●	●	●	●	●	○	○
Slovak Republic	N/A	●	N/A	●	N/A	●	N/A	○	N/A	○	N/A	●	N/A	●
Slovenia	●	●	●	●	●	●	●	●	●	○	○	○	○	○
Spain	●	●	○	○	●	●	○	○	○	○	○	○	○	○
Sweden	●	●	●	●	●	●	●	●	○	○	●	●	○	○
Switzerland	N/A	○	N/A	●	N/A	●	N/A	●	N/A	○	N/A	●	N/A	○
Türkiye	●	●	●	●	●	●	●	●	○	○	○	○	●	●
United Kingdom	○	●	○	○	○	○	●	●	●	●	●	●	○	○
OECD Total														
● Yes	22	27	18	24	18	23	15	17	11	12	22	26	10	14
○ No	11	9	15	12	15	13	18	19	22	24	11	10	23	22
No Information	3	0	3	0	3	0	3	0	3	0	3	0	3	0
Argentina	●	●	○	○	○	○	○	○	○	○	○	○	●	●
Brazil	●	●	○	○	●	●	○	○	○	○	●	●	○	○
Bulgaria	N/A	○	N/A	○	N/A	●	N/A	●	N/A	○	N/A	○	N/A	●
Croatia	●	●	●	●	●	●	●	●	○	○	●	●	○	○
Indonesia	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○
Peru	●	○	●	●	●	●	●	●	●	●	○	○	○	○
Romania	●	●	○	○	●	○	○	○	○	○	○	○	○	○
Thailand	N/A	●	N/A	●	N/A	●	N/A	●	N/A	●	N/A	●	N/A	○

Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

Annex Table 2.A.3. Actors covered as service providers by the National Digital Identity Strategy

Types of actors covered in the [National Digital Identity Strategy or equivalent] following their role as service providers (i.e. actors in need of verifying the identity of natural and legal persons claiming access to their service)

Country	Central/federal government		Subnational government		Know-your-customer-regulated actors		Private sector organisations with no regulated obligations	
	2023	2025	2023	2025	2023	2025	2023	2025
Australia	●	●	●	●	●	●	●	●
Austria	●	●	○	○	●	●	○	○
Belgium	●	●	○	○	○	○	○	○
Canada	N/A	●	N/A	●	N/A	●	N/A	●
Chile	●	●	●	●	○	●	○	●
Colombia	●	○	●	○	●	○	●	○
Costa Rica	●	●	○	○	○	○	○	○
Czechia	●	●	●	●	●	●	●	●
Denmark	●	●	●	●	●	●	●	●
Estonia	●	●	●	●	●	●	●	●
Finland	●	●	●	●	●	●	●	●
France	●	●	●	●	●	●	○	○
Greece	N/A	●	N/A	●	N/A	●	N/A	●
Hungary	N/A	●	N/A	●	N/A	●	N/A	●
Iceland	●	●	●	●	●	●	○	○
Ireland	●	●	●	●	○	○	○	●
Israel	●	●	●	●	●	○	●	●
Italy	●	●	●	●	●	●	○	○
Japan	●	●	●	●	●	●	○	○
Korea	●	●	●	●	●	●	●	●
Latvia	N/A	●	N/A	●	N/A	○	N/A	○
Lithuania	●	●	○	○	●	●	○	○
Luxembourg	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Mexico	N/A	●	N/A	●	N/A	○	N/A	○
Netherlands	●	●	●	●	○	○	○	○
New Zealand	●	●	○	●	○	●	○	●
Norway	●	●	●	●	●	●	○	○
Poland	●	●	○	○	●	●	○	○
Portugal	N/A	●	N/A	●	N/A	●	N/A	●
Slovak Republic	N/A	●	N/A	●	N/A	○	N/A	○
Slovenia	●	●	●	●	○	○	○	○
Spain	●	●	●	●	●	●	○	○
Sweden	●	●	●	●	○	●	○	●
Switzerland	N/A	●	N/A	●	N/A	●	N/A	●
Türkiye	●	N/A	●	N/A	○	N/A	○	N/A
United Kingdom	●	●	●	●	●	●	●	●
OECD Total								
● Yes	27	32	21	27	18	23	9	16
○ No	0	1	6	6	9	10	18	18
No Information	9	3	9	3	9	3	9	2
Argentina	●	●	●	●	●	●	●	●
Brazil	●	●	●	●	○	○	○	○

Country	Central/federal government		Subnational government		Know-your-customer-regulated actors		Private sector organisations with no regulated obligations	
	2023	2025	2023	2025	2023	2025	2023	2025
Bulgaria	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Croatia	N/A	○	N/A	○	N/A	○	N/A	○
Indonesia	●	●	●	●	○	○	○	○
Peru	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Romania	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Thailand	N/A	●	N/A	○	N/A	●	N/A	●

Note: 2025 data not available for Germany and the United States. In 2025, Bulgaria, Canada, Luxembourg, Peru, Romania and Türkiye did not report the existence of a National Digital Identity Strategy or equivalent. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. In 2023, Canada, Croatia, Hungary, Latvia, Luxembourg, Mexico, Peru, Portugal and Romania did not report the existence of a National Digital Identity Strategy or equivalent. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

Annex Table 2.A.4. Data management standards or guidelines for public servants

Availability of types of data management standards or guidelines exist at the central/federal government level

Country	Metadata management		Data quality assessments		Data inventories		Data anonymisation		Data access and sharing arrangements between institutions		Sharing arrangements with external data providers		Compliance with data protection regulations		Compliance with security regulations	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
Australia	●	●	○	●	●	●	●	●	●	●	○	●	●	●	●	●
Austria	●	●	○	○	○	●	○	●	○	○	○	●	○	○	○	○
Belgium	○	●	○	●	○	●	○	○	○	●	○	●	○	●	○	●
Canada	●	●	●	●	●	●	○	●1	●	●	●	●	●	●	○	●
Chile	○	●	○	●	○	●	○	●	○	●	○	●	●	●	○	●
Colombia	●	●	●	●	●	●	●	●	●	●	○	●	●	●	○	●
Costa Rica	●	●	○	○	○	○	●	●	○	○	○	○	○	○	○	○
Czechia	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Denmark	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Estonia	●	●	●	●	○	○	●	●	●	●	●	●	●	●	○	●
Finland	●	●	●	●	●	●	○	○	●	●	●	●	●	●	●	●
France	●	●	●	●	○	●	○	●	●	●	○	●	○	●	○	●
Greece	N/A	●	N/A	○	N/A	●	N/A	●	N/A	●	N/A	●	N/A	●	N/A	●
Hungary	●	●	○	○	●	●	○	●	○	○	●	●	●	●	●	●
Iceland	○	○	●	●	●	●	●	○	●	●	●	●	●	●	●	●
Ireland	○	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●
Israel	○	○	○	○	○	○	○	○	○	●	○	●	○	●	○	●
Italy	●	●	○	●	●	●	●	●	●	●	○	●	●	●	○	●
Japan	●	●	●	●	●	●	○	●	○	●	○	●	○	●	○	●
Korea	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Latvia	●	●	○	○	●	●	●	●	●	●	●	●	●	●	○	○
Lithuania	○	●	○	○	○	○	○	○	●	●	○	○	●	●	●	●
Luxembourg	○	●	○	●	●	●	○	●	●	●	●	●	●	●	●	●
Mexico	○	○	●	○	●	○	○	○	●	○	○	○	●	●	●	●
Netherlands	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Country	Metadata management		Data quality assessments		Data inventories		Data anonymisation		Data access and sharing arrangements between institutions		Sharing arrangements with external data providers		Compliance with data protection regulations		Compliance with security regulations	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
New Zealand	●	●	○	○	●	●	○	○	○	○	○	●	●	●	●	●
Norway	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Poland	●	●	○	○	○	○	●	●	●	●	○	○	●	●	○	○
Portugal	○	●	○	●	○	●	○	○	○	●	○	○	○	●	○	○
Slovak Republic	N/A	●	N/A	●	N/A	○	N/A	●	N/A	●	N/A	○	N/A	●	N/A	●
Slovenia	●	●	○	○	●	●	○	○	○	○	○	○	●	●	●	●
Spain	○	●	○	●	○	○	●	●	●	●	○	○	●	●	●	●
Sweden	●	●	○	○	●	●	○	●	○	●	○	●	●	●	●	●
Switzerland	N/A	●	N/A	●	N/A	●	N/A	●	N/A	●	N/A	●	N/A	●	N/A	●
Türkiye	●	●	○	○	●	●	○	●	●	●	○	○	●	●	●	●
United Kingdom	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
OECD Total																
● Yes	23	33	15	23	21	28	16	26	22	30	14	27	26	34	19	31
○ No	10	3	18	13	12	8	17	10	11	6	19	9	7	2	14	5
No Information	3	0	3	0	3	0	3	0	3	0	3	0	3	0	3	0
Argentina	○	●	○	○	○	○	○	●	○	●	○	○	●	●	○	●
Brazil	○	●	●	●	●	●	●	●	●	●	●	●	○	●	○	●
Bulgaria	○	●	○	○	○	○	○	○	○	●	○	○	○	●	○	●
Croatia	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A
Indonesia	N/A	●	N/A	●	N/A	●	N/A	○	N/A	●	N/A	●	N/A	●	N/A	●
Peru	●	●	●	●	●	●	●	●	●	●	○	○	●	●	●	●
Romania	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A
Thailand	N/A	●	N/A	○	N/A	●	N/A	○	N/A	○	N/A	○	N/A	●	N/A	●

Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023. Data anonymisation does not consider broader de-identification guidance or standards.

1. Data were updated following a request from the country after the publication of the 2025 DGI; therefore, these changes are not reflected in the 2025 DGI results. TBS (Canada) Privacy Implementation Notices provide federal guidance related to privacy-preserving treatment of data and identifiability reduction, including de-identification, disclosure-risk mitigation, and re-identification risk management.

Source: OECD (2025) Survey on Digital Government 3.0.

REFERENCES

Byrom, N., M. Piccinin-Barbieri and P. Wells (2024), "Towards effective governance of justice data", *OECD Working Papers on Public Governance*, No. 74, OECD Publishing, Paris, https://doi.org/10.1787/d2950e02-en. [15]

Estonian Business and Innovation Agency (n.d.), "e-Identity", *e-Estonia*, https://e-estonia.com/solutions/estonian-e-identity/id-card/ (accessed on 13 May 2026). [10]

Government of France (n.d.), "La plateforme des données publiques françaises", *datagouv*, Direction Interministérielle du Numérique (DINUM), https://www.data.gouv.fr/ (accessed on 13 May 2026). [22]

Government of France (n.d.), "L'espace de travail ouvert et souverain des agents de l'État", Direction interministérielle du numérique (DINUM), https://lasuite.numerique.gouv.fr/ (accessed on 13 May 2026). [35]

Government of Germany (n.d.), "openDesk", Center for Digital Sovereignty (ZenDiS), https://www.opendesk.eu/de. [36]

Government of Italy (n.d.), "Explore the Public Administration API", Department for Digital Transformation, https://api.gov.it/en/ (accessed on 13 May 2026). [30]

Government of Italy (n.d.), *Identità Digitale: firmato il decreto che assegna 40 milioni di euro ai gestori Spid*, https://innovazione.gov.it/notizie/comunicati-stampa/identita-digitale-firmato-il-decreto-che-assegna-40-milioni-di-euro-ai-gestori-spid/ (accessed on 13 May 2026). [11]

Government of Japan (n.d.), "Digital Agency", https://www.digital.go.jp/en (accessed on 13 May 2026). [31]

Government of the Czech Republic (n.d.), "National Open Data Catalogue", https://data.gov.cz/ (accessed on 13 May 2026). [21]

Government of the Netherlands (n.d.), "Over Mijn Bureau", Ministry of the Interior and Kingdom Relations (MinBZK), https://minbzk.github.io/mijn-bureau/ (accessed on 13 May 2026). [37]

Hlacs, A. and H. Wells (2025), "Using digital technology to strengthen oversight of public procurement in Portugal: The use of data analytics and machine learning by the Tribunal de Contas", *OECD Working Papers on Public Governance*, No. 83, OECD Publishing, Paris, https://doi.org/10.1787/43add03b-en. [13]

Ministry of the Interior and Kingdom Relations (MinBZK) (n.d.), "Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (MinBZK) GitHub organisation", https://github.com/minbzk/ (accessed on 13 May 2026). [40]

MitID (n.d.), *MitID website*, https://www.mitid.dk/om-mitid/ (accessed on 13 May 2026). [9]

NÚKIB (2022), "NÚKIB a Ministerstvo vnitra vydaly bezpečnostní doporučení pro vývoj otevřeného softwaru", https://nukib.gov.cz/cs/infoservis/doporuceni/1827-nukib-a-ministerstvo-vnitra-vydaly-bezpecnostni-doporuceni-pro-vyvoj-otevreneho-softwaru/ (accessed on 23 March 2026). [43]

OECD (2026), *Anti-Corruption and Integrity Outlook 2026: Harnessing the Integrity Advantage*, OECD Publishing, Paris, https://doi.org/10.1787/16708b78-en. [23]

OECD (2025), *Developing a data-driven corruption risk model to strengthen integrity in Belgium: Practical considerations for the Federal Internal Audit*, OECD Publishing, Paris, https://doi.org/10.1787/e85587eb-en. [16]

OECD (2025), *Digital Government Review of Korea: Harnessing Digital and Data to Transform Government*, OECD Digital Government Studies, OECD Publishing, Paris,, https://doi.org/10.1787/9defc197-en. [28]

OECD (2025), "Digital transformation of public procurement: Good practice report", *OECD Public Governance Policy Papers*, No. 77, OECD Publishing, Paris, https://doi.org/10.1787/79651651-en. [12]

OECD (2025), *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*, OECD Publishing, Paris, https://doi.org/10.1787/795de142-en. [25]

OECD (2025), "Implementing Chile's national digital identity strategy: Insights from country experiences", *OECD Public Governance Policy Papers*, No. 81, OECD Publishing, Paris, https://doi.org/10.1787/04a67b8b-en. [34]

OECD (2025), "Mapping relevant data collection mechanisms for AI training", *OECD Artificial Intelligence Papers*, No. 48, OECD Publishing, Paris, https://doi.org/10.1787/3264cd4c-en. [26]

OECD (2025), *Results User Satisfaction with Public Services*, Unpublished. [2]

OECD (2024), "Digital public infrastructure for digital governments", *OECD Public Governance Policy Papers*, No. 68, OECD Publishing, Paris, https://doi.org/10.1787/ff525dc8-en. [1]

OECD (2024), *G20 Compendium on Data Access and Sharing Across the Public Sector and with the Private Sector for Public Interest*, OECD Publishing, Paris, https://doi.org/10.1787/df1031a4-en. [32]

OECD (2024), *G7 Compendium of Digital Government Services*, OECD Publishing, Paris, https://doi.org/10.1787/69fbf288-en. [7]

OECD (2024), *G7 Mapping Exercise of Digital Identity Approaches*, OECD Publishing, Paris, https://doi.org/10.1787/56fd4e94-en. [8]

OECD (2024), *Modernising Access to Social Protection: Strategies, Technologies and Data Advances in OECD Countries*, OECD Publishing, Paris, https://doi.org/10.1787/af31746d-en. [27]

OECD (2024), "Recommendation of the Council on Human-centred Public Administrative Services", *OECD Legal Instruments*, OECD/LEGAL/0503, OECD, Paris, https://legalinstruments.oecd.org/instruments/instruments/OECD-LEGAL-0503. [6]

OECD (2024), *Strengthening Oversight of the Court of Auditors for Effective Public Procurement in Portugal: Digital Transformation and Data-driven Risk Assessments*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/35aeab1e-en. [14]

OECD (2023), "2023 OECD Open, Useful and Re-usable data (OURdata) Index: Results and key findings", *OECD Public Governance Policy Papers*, No. 43, OECD Publishing, Paris, https://doi.org/10.1787/a37f51c3-en. [24]

OECD (2023), *Moving forward on data free flow with trust: New evidence and analysis of business experiences*, OECD Digital Economy Papers, No. 353, OECD Publishing, Paris, https://doi.org/10.1787/1afab147-en. [33]

OECD (2023), "Recommendation of the Council on the Governance of Digital Identity", *OECD Legal Instruments*, OECD/LEGAL/0491, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491. [5]

OECD (2021), "OECD Good Practice Principles for Data Ethics in the Public Sector", *OECD Public Governance Policy Papers*, No. 57, OECD Publishing, Paris, https://doi.org/10.1787/caa35b76-en. [20]

OECD (2021), "Recommendation of the Council on Enhancing Access to and Sharing of Data", *OECD Legal Instruments*, OECD/LEGAL/0463, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463. [4]

OECD (2020), *"The OECD Digital Government Policy Framework: Six dimensions of a digital government"*, OECD Public Governance Policy Papers, No. 2, OECD Publishing, Paris, https://doi.org/10.1787/f64fed2a-en. [29]

OECD (2019), *The Path to Becoming a Data-Driven Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/059814a7-en. [17]

OECD (2014), "Recommendation of the Council on Digital Government Strategies", *OECD Legal Instruments*, OECD/LEGAL/0406, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406. [3]

Open Source Program Office (OSPO) (n.d.), "website", *social.overheid.nl*, Open Source Program Office (OSPO), Netherlands, https://social.overheid.nl/@BZKopensource (accessed on 13 May 2026). [39]

Opensourcewerken (n.d.), *website*, https://opensourcewerken.nl/ (accessed on 13 May 2026). [38]

Otevřená města (n.d.), "Czech National OSPO", https://otevrenamesta.cz/czech-ospo (accessed on 13 May 2026). [41]

Otevřená města et al. (2022), *Brno Open Source Declaration*, https://otevrenamesta.cz/declaration (accessed on 23 March 2026). [42]

Republic of Poland (2021), *Open Data Programme for the years 2021-2027*, https://dane.gov.pl/en/knowledgebase/useful-materials/program-otwierania-danych-na-lata-2021-2027 (accessed on 20 February 2026). [18]

Secretaría de Gobierno Digital (2024), *Estrategia de Datos del Gobierno*, https://web.archive.org/web/20251118092609/https://www.digital.gob.cl/biblioteca/estrategias/estrategias-de-datos-del-gobierno/ (accessed on 20 February 2026). [19]

3 Governing digital investment and capabilities to deliver at scale

Effective digital government depends on making smart investments in digital technologies and having the people and skills needed to deliver results. Drawing on findings from the 2025 Digital Government Index, this chapter shows that progress has been strongest in the early stages of investment - planning, needs identification and securing funding - but weaker in what happens next, including adjusting funding as work progresses, managing risk throughout delivery, procuring in ways suited to modern digital projects, and evaluating whether investments have actually worked. These gaps limit governments' ability to scale what works, stop what does not and learn consistently from experience. By bringing together digital investment management and digital talent and skills as two mutually reinforcing priorities, this chapter shows how better-governed investment and stronger internal capability can jointly improve value for money, reduce dependence on external providers and sustain digital transformation over time, including as AI adoption accelerates.

Key messages

- **Digital government only delivers when governments manage investments and build capabilities at the same time.** Technology alone does not transform government and its public services. Governments need to plan and spend on digital technologies in ways that generate real results, and they need the right people and skills to make those investments work. When investment management and capability building are treated as separate concerns, both suffer. When they work together, governments can deliver more reliably, adapt quickly and demonstrate clear value for money.
- **Planning, funding, risk management and procurement guidance are all improving, but have not yet adapted to the way modern digital projects work.** Most OECD countries have processes for assessing ex ante the value of digital investments, dedicated funding mechanisms, stronger procurement guidance, and more systematic risk assessments. However, these tools remain largely designed around upfront approval and annual budget cycles rather than the staged, iterative delivery that digital projects require. Risk assessment methods are often too generic to capture the specific challenges of digital and AI-enabled initiatives, and procurement approaches suited to flexible delivery see uneven uptake. This limits governments' ability to adjust investments as technologies evolve, scale up what is working, stop what is not, spot problems early, and avoid long-term dependency on individual suppliers.
- **Monitoring is common, but evaluating whether investments have delivered remains the missing link.** Most OECD governments track project progress during delivery, but few systematically assess whether their digital investments achieved the results they promised. Only one in four OECD countries conducts cost-benefit analysis of completed digital projects. Without this, governments cannot learn consistently from experience, demonstrate value for money or make better investment decisions over time.
- **Digital skills efforts are expanding, but remain fragmented and disconnected from long-term workforce planning.** OECD countries are doing more to assess skills gaps, attract digital talent and provide training. But these efforts are often isolated initiatives rather than parts of a coherent, government-wide workforce strategy. Only six OECD countries have a dedicated strategy for digital talent and skills in the public sector. Without a more strategic approach, governments risk remaining under-equipped to manage data-intensive systems, oversee AI responsibly and sustain digital transformation over time.
- **Governments need the right balance between outsourcing and in-house capability to sustain transformation and preserve agency.** External providers can bring skills and capacity that government does not have and accelerate delivery. But over-reliance hollows out the internal knowledge and judgement that governments need to define what they want, assess whether they are getting it, hold suppliers to account and adapt systems when circumstances change. Several OECD countries are actively rebuilding internal digital capability. The goal is not to bring everything in-house, but to ensure government retains the core expertise needed to govern digital transformation responsibly.

3.1. Introduction

Effective digital government depends on making smart investments in digital technologies and having the people and skills needed to deliver results. This chapter looks at both: how governments manage their digital investments, and how they build the internal capability to make those investments work.

Getting digital investment right means more than approving the right projects at the outset. It means actively managing them throughout, from identifying needs and making the case for funding, through delivery and adaptation, to decommissioning systems when they are no longer fit for purpose. This full cycle matters because digital technologies evolve quickly, risks change during delivery, and what looks like a sound decision at the approval stage may need to be revisited as circumstances change. Governments that manage this cycle well can scale what works, stop what does not, and learn consistently from experience. Those that do not tend to accumulate costly, outdated systems, repeat avoidable mistakes and lose control over the technologies they depend on.

As public sector spending on digital technologies grows, so does the importance of governing investments in ways that maximise value and avoid inefficiencies (OECD, 2025[1]). The 2025 Digital Government Index (DGI) shows that OECD countries have made strong progress on the early stages of this cycle: identifying needs, building the case for investment and securing funding. However, important capabilities are often missing once delivery starts. Many governments lack flexible funding that can be adjusted as work progresses, clear decision points to decide whether to continue or change courses, procurement approaches suited to modern digital delivery, and regular reviews that examine what is working and why. When these elements are missing, governments struggle to adapt to changing technologies, user needs and risks, and it is harder to demonstrate that public money is being well spent.

The same pattern appears in digital skills. Governments increasingly recognise the need to build digital capability, and many are doing more to assess skills gaps, attract talent and provide training. But these efforts are often fragmented and disconnected from longer-term workforce planning. Without a coherent, government-wide approach to building and retaining the right skills, governments risk becoming overly dependent on external technology providers, losing institutional knowledge and lacking the internal expertise needed to govern, oversee and adapt digital systems responsibly.

This chapter examines both challenges in sequence. It first looks at how government manage digital spending, covering planning and funding, risk management and procurement, and monitoring and evaluation. It then examines how governments can build and sustain digital skills and talent. Finally, it addresses the question of how governments can strike the right balance between developing capability in-house and drawing on external providers.

3.2. Governing digital investment: progress in planning, gaps in delivery

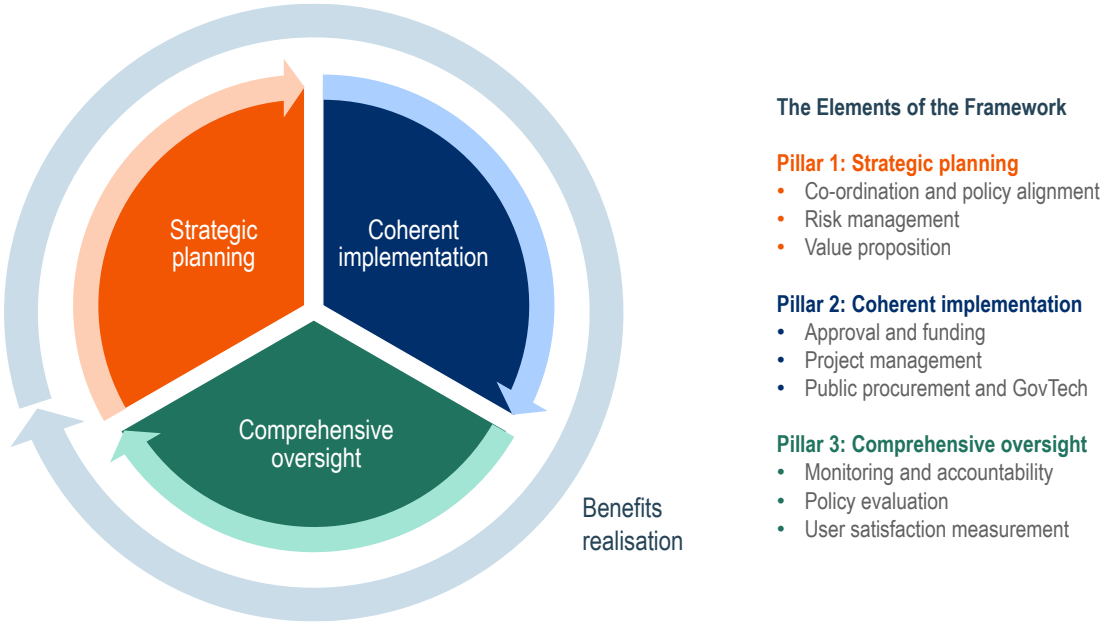
3.2.1. Stronger central oversight is improving investment decisions, but lifecycle management remains uneven

Investing well in digital technologies requires more than securing the right budget. It means making sound decisions throughout the full life of an investment, from identifying needs and assessing options, through delivery and adjustment, to reviewing outcomes and decommissioning systems when they are no longer needed. When this is done well, governments can get better value for money, avoid accumulating outdated systems, and retain control over the technologies they rely on. When it is not, spending grows without clear results, systems become harder to update or replace, and governments find themselves locked into arrangements that no longer serve their needs (OECD, 2025[1]; OECD, 2024[2]).

The OECD Recommendation on Digital Government Strategies underlines the importance of coherent and well-governed investment arrangements to steer digital transformation and safeguard long-term value. Building on this, the OECD Digital Government Investments Framework translates these principles into actionable tools and guidance for managing investments throughout their full life - from early planning and business cases through to delivery, scaling and continuous improvement (Figure 3.1).

Figure 3.1. OECD Digital Government Investments Framework

Three pillars to guide the management of investments throughout the project lifecycle

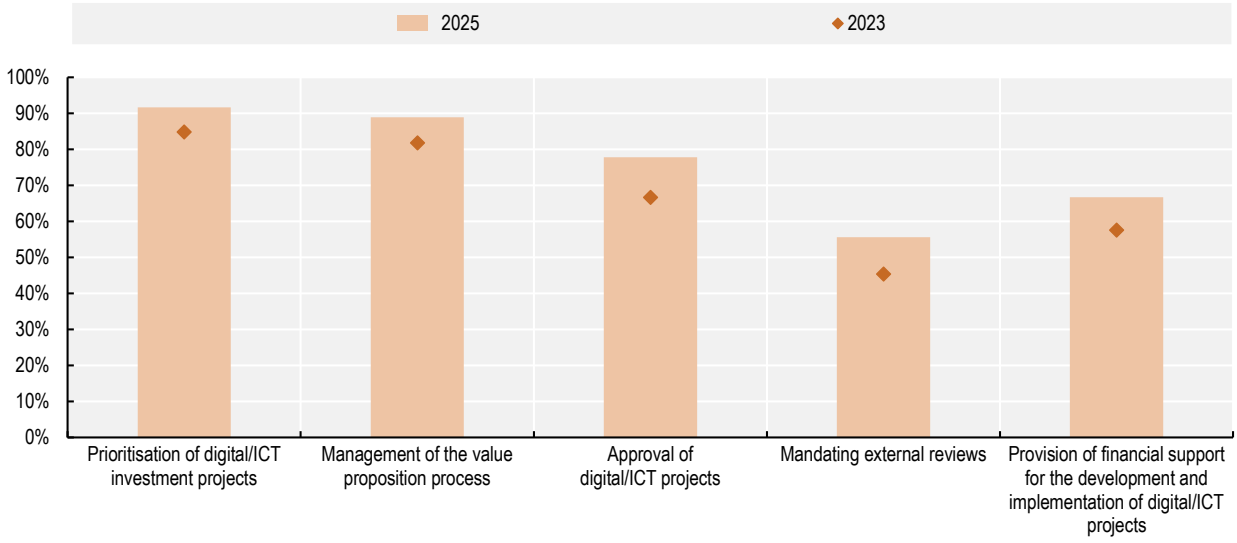


Source: (OECD, 2025[1])

A first step towards better investment management is giving the central digital government authority a clear mandate to oversee spending across government. This helps align investments with strategic priorities, identify opportunities to share costs and infrastructure, and avoid duplicating spending across agencies (OECD, 2025[1]; OECD, 2021[3]). According to the 2025 DGI, 33 out of 36 OECD countries (92%) report that their leading digital government institution is responsible for prioritising digital and ICT investment projects across central government, up from 85% in 2023 (Figure 3.2 and Annex Table 3.A.1). This reflects growing recognition that fragmented agency-by-agency decisions can undermine coherence, duplicate spending, and make it harder for systems to work together. While countries have developed different models for central oversight (Box 3.1), the direction is consistent: stronger central roles create better conditions for managing investments strategically and keeping digital systems reliable and adaptable over time.

Figure 3.2. Countries have strengthened the decision-making responsibilities of leading digital government institutions

Total of OECD countries with specific decision-making responsibilities of digital government leading institutions, 2023 and 2025



Note: 2025 data not available for Germany and the United States. 2023 data not available for Germany, Greece, Slovak Republic, Switzerland and the United States. Refer to Annex Table 3.A.1 for comprehensive OECD and Accession country data.
Source: OECD Survey on Digital Government 3.0 (2025); OECD (2026[4]; 2024[5]).

StatLink https://stat.link/60y7m4

Box 3.1. Strengthening central oversight of digital investment

Clear mandates and governance arrangements ensure that digital investments are prioritised strategically, managed coherently, and held accountable for results, rather than fragmented across ministries with no one responsible. Most OECD countries have strengthened the mandate and role of digital government authorities to manage digital investments, making it a strong lever to exert this role and steer a whole-of-government digital transformation:

- **New Zealand**'s Government Chief Digital Officer has progressively strengthened cross-government oversight of digital spending to reduce duplication and improve value for money, including through closer scrutiny of investment proposals and greater use of common platforms and shared services.
- **Chile**'s Secretariat of Digital Government, within the Ministry of Finance, plays a central role in coordinating and financing digital government initiatives, aligning funding decisions with the broader State Modernisation Agenda.
- **Korea** uses legal mandates to give the Ministry of the Interior and Safety binding authority over project selection, prioritisation and management through its E-Government Project Support Programme. Annual funding is agreed with the Ministry of Economy and Finance, creating a direct link between investment and budget allocation.

Sources: (New Zealand Government, 2025[6]; Ministerio de Hacienda, 2026[7]; Ministry of Public Administration and Security, 2022[8]).

Alongside a clear mandate, governments benefit from managing investments in a joined-up way across their lifecycle – not just at the point of initial approval. Joined-up approaches help governments track whether expected benefits are being realised, spot problems early and adjust course when needed (OECD, 2025[1]). The 2025 DGI suggests that many investment management systems remain focused primarily on the planning stage and are not well connected to delivery oversight, funding decisions or evaluation. As a result, governments often lack the feedback they need during delivery to identify when something is going wrong or when a project should be changed or stopped (OECD, 2025[1]). More integrated approaches, where regular reviews link funding to progress and outcomes, can help governments manage complex programmes more effectively and keep investments aligned with evolving needs (Box 3.2).

Box 3.2. Managing digital investments across their lifecycle: Australia and Switzerland

Some OECD countries are advancing in the development of integrated approaches to managing digital investments, from the moment of appraisal to the evaluation of results.

Australia's Digital and ICT Investment Oversight Framework brings together policies, processes and tools to manage investments from initial planning through to completion. It requires agencies to define, track, and report on the benefits they expect to achieve, supported by central guidance from the Digital Transformation Agency. Funding is released in stages, tied to milestone completion. Portfolio-level tools - including Digital Investment Overview and a Major Digital Projects Report – provide transparency across both planned and active investments.

Switzerland applies HERMES, a whole-of-government project management approach, to oversee digital investments across their lifecycle. It embeds business case development and review – covering objectives, value for money and risk – and mandates final evaluations to assess outcomes and capture lessons learned. Project documentation is recorded in a central portfolio management tool, giving departments visibility across investments. For strategic initiatives, progress is published via the Digital Switzerland Action Plan portal.

Sources: (OECD, 2025[9]; HERMES, 2025[10]; Digital Switzerland, 2025[11]; HERMES, 2025[12]).

3.2.2. Planning tools are widely available, but not yet adapted to the pace of modern digital delivery

Most OECD countries have put in place the basic tools to plan and estimate spending on digital government. According to the 2025 DGI, 33 out of 36 OECD countries (89%) having such mechanism, broadly unchanged from 88% in 2023, reflecting established planning standards across the OECD area.

However, in many countries these tools were designed for a different era of technology delivery. They work well for large, one-off projects with fixed requirements and predictable costs. They work less well for the way digital projects are now typically delivered - in stages, with requirements that evolve as work progresses, using flexible technologies such as cloud services that are paid for on a subscription basis rather than as a one-off purchase, or AI tools that need to be tested and adapted over time.

In practice, planning tools are often used to justify an investment at the approval stage rather than to guide its delivery, adaptation or oversight as the work progresses. Projects may appear sound when first approved but become harder to adjust as technology change, risk emerge or user needs evolve. More flexible planning and funding approaches – one that allows decision to be revisited and investments to be adjusted as new information becomes available – would better protect value for money and reduce the risk of governments becoming locked into approaches that no longer work.

Several OECD countries are adapting their planning processes to address this, introducing greater flexibility and more risk-proportionate review (Box 3.3).

Box 3.3. Making investment planning more flexible and iterative

Several OECD countries are adapting their investment planning processes to better support digital delivery:

- **Canada** requires departments to develop a concept case before proceeding to a full business case. This helps clarify the problem or opportunity, provides an early indication of potential investments, and ensures alignment with strategic and departmental priorities before significant resources are committed.
- **New Zealand**'s Better Business Cases framework adjusts the level of scrutiny to the scale and complexity of a project – lighter touch for smaller or lower-risk investments, more rigorous for larger or more complex ones.
- The **United Kingdom** has updated its investment appraisal guidance and is piloting staged funding approaches that allow early funding for initial exploration and testing, reducing the risk of committing too early to a particular solution.
- **Australia**'s Digital and ICT Investment Oversight Framework manages investments from planning through to completion, requiring agencies to define and track expected benefits. For higher-risk proposals, funding may be released in stages tied to milestone completion to help de-risk the investment, supported by portfolio-level transparency tools across planned and active projects.

Sources: (OECD, 2025[13]; OECD, 2025[9]; Australian Government, 2026[14]; HM Treasury, 2024[15]; The Treasury, 2025[16]; Government of Canada, 2025[17]; Korean Government, 2022[18])

3.2.3. Dedicated funding for digital government is growing, but is not yet flexible enough

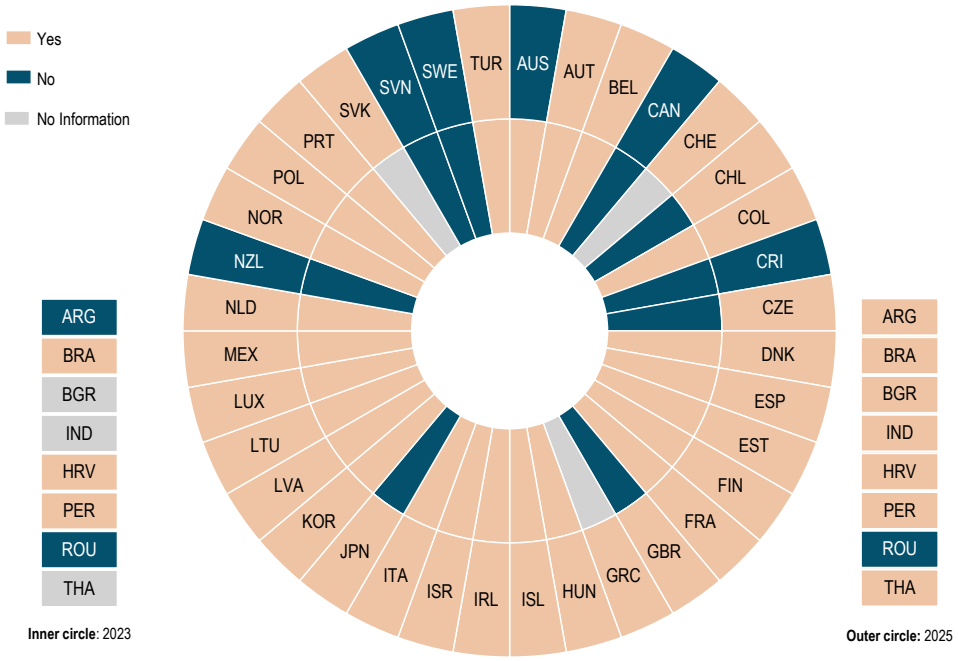
Having a dedicated source of funding for digital investments, separate from general departmental budgets, helps governments fund shared platforms and systems for government institutions that would not have the budget to build alone. The share of countries with such dedicated funding has risen from 73% in 2023 to 81% in 2025 (29 out of 36 countries), reflecting a growing recognition that strategic digital investment requires stable, purpose-built funding mechanisms (Figure 3.3).

However, most of these funding mechanisms are still tied to annual budget cycles and upfront approval processes. They are designed to approve spending at the start of a project, not to adjust it as the project evolves. This makes it harder to manage investments that span multiple years, change in scope as technology develops, or need to scale up once an initial phase has demonstrated results. It also makes it difficult to stop or redirect spending when a project is underperforming, since funding decisions have typically already been made.

Moving towards more outcome-focused funding - where resources are released progressively based on demonstrated progress rather than committed upfront in full - would better support the way digital projects actually work and improve governments' ability to get value from their investments (Box 3.4).

Figure 3.3. Most OECD countries have established dedicated funding programmes to support government digital transformation initiatives

Availability of a dedicated funding programme or initiative for ICT/digital projects in government, 2023 and 2025



Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD Survey on Digital Government 3.0 (2025); OECD (2026[4]; 2024[5]).

StatLink https://stat.link/4fw67p

Box 3.4. OECD countries experimenting with more flexible digital investment approaches

Several OECD countries are adapting how digital investment funding works in practice:

- The **United Kingdom** is piloting staged funding for digital projects, testing approaches where funding is released in tranches tied to demonstrated progress, with regular reviews informing subsequent tranches.
- **France's** Public Action Transformation Fund (FTAP) awards funding based on expected return on investment and alignment with identified priorities, with the Interministerial Digital Directorate (DINUM) playing a central review and co-ordination role. This model demonstrates how dedicated funding can be paired with central oversight and performance mechanisms.
- **Japan's** co-ordinates digital and technology budgeting centrally thorough its Digital Agency, allocating strategic investment funds to ministries in a way that promotes alignment with cross-government objectives and reduce fragmentation.
- **Norway's** co-financing scheme requires the agencies receiving funding to contribute a share themselves, reinforcing ownership and accountability, and linking funding to assessed benefits.

Sources: (HM Treasury/DSIT/GDS, 2025[19]; République française, 2024[20]; Digital Agency, Japan, 2025[21]).

3.2.4. Risk management is improving, but it is not yet consistently tailored to digital delivery

Identifying and managing risks is a fundamental part of making good investments decisions. For digital projects specifically, this matters because risks can change significantly during delivery – as technologies evolve, dependencies on other systems emerge, or user needs shift in ways that were not anticipated at the outset. Governments that manage risk well throughout a project's life are better placed to spot problems early, adjust course before issues become costly, and avoid accumulating outdated or poorly performing systems.

Most OECD countries have put strong foundations in place for managing cybersecurity risks. All OECD countries have:

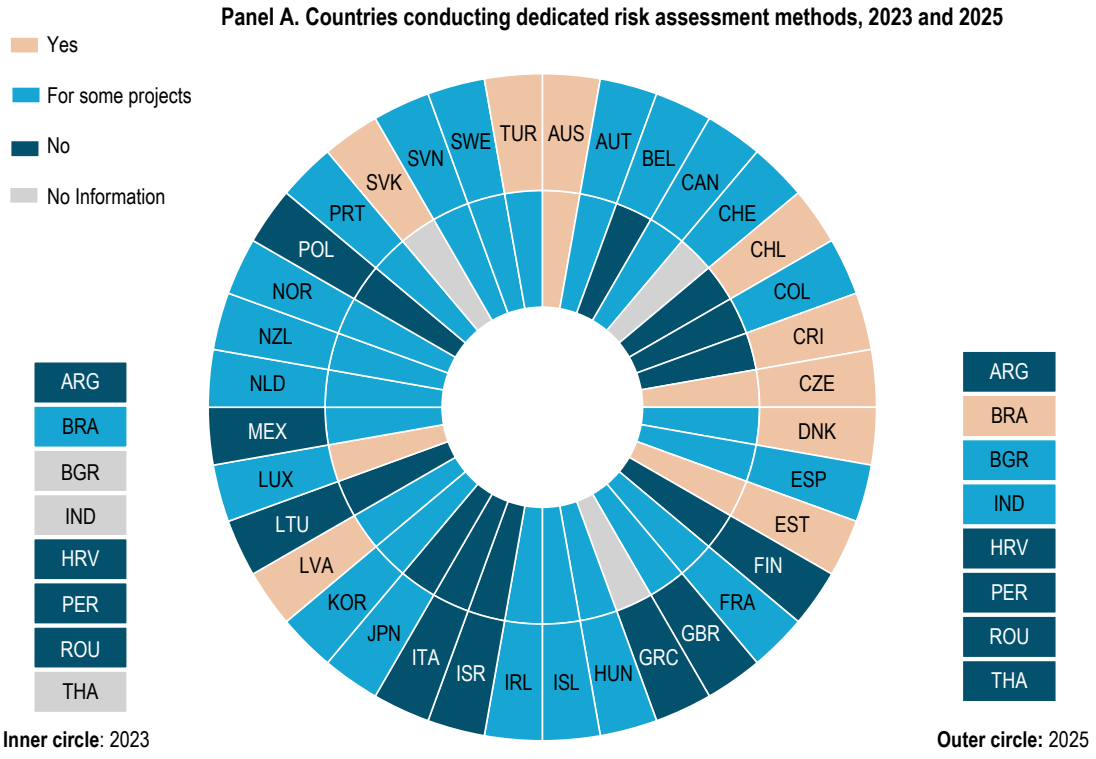
- a strategy or policy for information security
- legislation or regulation covering the security of critical digital infrastructure
- a leading institution to co-ordinate cybersecurity at the national level
- an institution with a mandate to investigate and prosecute cybercrime

Almost all also have a national team to respond to cybersecurity incidents - Computer Emergency Response Team (CERT) - and a dedicated security operation function - Security Operations Centre (SOC). This reflects the priority governments place on keeping the systems and infrastructure that underpin public services secure and available.

However, managing cybersecurity risks is only part of the picture. Digital projects also carry delivery risks - the risk that a project takes longer or costs more than expected; governance risks - the risk that accountability is unclear or oversight is inadequate; and technology-specific risks such as dependency on a single supplier, difficulties integrating with existing systems, or uncertainty about how AI tools will perform in practice. These risks require different assessment approaches from those used for traditional infrastructure or administrative projects, and many governments have not yet adapted their methods accordingly.

The number of OECD countries where the leading digital government body conducts dedicated risk assessments for all or selected digital projects increased from 23 out of 33 countries in 2023 (70%) to 28 out of 36 in 2025 (77%) – a meaningful improvement, indicating that such assessments are being mainstreamed across the OECD area (Figure 3.4, Panel A). Where risk assessments do exist, they frequently rely on generic tools designed for traditional projects and can become a compliance exercise — completed at the approval stage and rarely revisited during delivery. This means that new risks emerging during a project - changes in technology, shifts in user needs, problems with supplier performance - may not be picked up until they have already caused significant disruption or cost. Furthermore, existing risks assessment methods prioritise cybersecurity and service continuity risk analysis, followed by risks associated to legacy technologies (Figure 3.4, Panel B). Several OECD countries are taking concrete actions to have a more tailored and fit-for-purpose approach to managing risks in digital and ICT investments (Box 3.5).

Figure 3.4. OECD countries are not fully embracing tailored risk-assessment methods for ICT and digital projects



Note: Panel A represents the individual responses to the question "Has the leading digital government unit conducted dedicated risk assessments for digital/ICT projects at the central/federal government?". Panel B represents the aggregated responses for OECD countries to the question "Please specify what kind of risks were included for such assessments". 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Slovak Republic, Switzerland and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.

Source: OECD Survey on Digital Government 3.0 (2025); OECD (2026[4]).

StatLink https://stat.link/82fjtp

Box 3.5. OECD countries are strengthening risk assessment to inform investment decisions

Several OECD countries are strengthening how they assess and manage digital-specific risks, including by linking risk assessment more explicitly to investment decisions and funding:

- **Ireland** embeds oversight for major digital initiatives within a wider public spending and infrastructure governance framework, supported by the Digital Government Oversight Unit and the Public Spending Code. Higher-value digital projects receive structured scrutiny against risk and feasibility criteria before proceeding.
- **Lithuania** uses a structured method for evaluating and prioritising digital initiatives that includes explicit criteria on feasibility, governance capacity and cybersecurity, linking project approval to compliance with these requirements.
- **New Zealand**'s Digital Investment Office support business case review and investment decisions, with a focus on risk-sensitive assessment, strategic alignment and managing the overall portfolio of digital investments across government.

Source: (OGCIO, 2024[22]; Government of Ireland, 2023[23]; Government of New Zealand, 2025[24]).

3.2.5. Procurement guidance is improving, but purchasing practices have not yet caught up

Public procurement – the process by which governments buy products and services from external providers, including digital technologies and services – is one of the most important levers governments have for getting value from digital investment. How governments buy shapes what they get: the flexibility of contracts, the range of suppliers they can access, and their ability to adjust as needs change during delivery.

Central guidance on procuring digital technologies has improved significantly. The number of OECD countries with dedicated procurement guidelines for digital and technology projects increased from 22 out of 33 countries (67%) in 2023 to 27 out of 36 (75%) in 2025. However, having good guidance is not the same as procuring in ways that suit modern digital delivery. Many digital projects today do not follow a simple pattern of specifying requirements upfront, selecting a supplier and delivering a fixed product. They are iterative – requirements evolve as work progresses, technologies change, and what is needed at the end may look quite different from what was envisaged at the start. Procurement procedures designed for traditional, fixed-scope projects are poorly suited to this reality.

When looking at the uptake of procurement mechanisms, several countries have developed central platforms and co-ordinated purchasing arrangements that make it easier for agencies to buy consistently and at better value (Box 3.6). This reflects growing maturity in procurement governance and a recognition that co-ordinated approaches reduce duplication and transaction costs (OECD, 2022[25]).In contrast, the 2025 DGI shows that more flexible and innovation-oriented procurement mechanisms see uneven uptake. This includes purchasing arrangements that allow the supplier pool to be updated over time, contracts structured around outcomes rather than fixed specifications, dialogue-based processes that allow governments and suppliers to explore solutions together, and partnerships designed specifically to develop new approaches. Only 20 out of 36 OECD countries (55%) report using a broader set of procurement mechanisms suitable for digital delivery, an improvement from 44% in 2023 but still one of the weakest performance areas across the investment lifecycle (Annex Table 3.A.2).

This gap reflects several practical challenges. Procurement teams may lack the skills and organisational conditions to use more flexible approaches. Risk-averse cultures can make officials reluctant to move away from familiar compliance-driven

processes. Budget and approval cycles may not align with iterative delivery models. And central guidance, while valuable for consistency, can inadvertently reinforce standardised approaches if it is not accompanied by training, support and outcome-focused contract models (OECD, 2017[26]; OECD, 2025[1]).

Moving toward adaptive procurement approaches that are better suited to digital delivery is essential for government to work effectively with a wider range of suppliers – including smaller, more innovative companies – manage delivery more flexibly, and avoid becoming locked into long-term arrangements that are difficult and costly to exit (Box 3.6). In line with more traditional procurement mechanisms, agile procurement benefits from adequate planning, capability and governance arrangements, which remain essential to obtain expected outcomes.

Box 3.6. Procurement frameworks for digital government

Several OECD countries are establishing dedicated frameworks and capabilities to better procure digital technologies in governments:

- **Australia**'s Digital Transformation Agency manages whole-of-government digital procurement through BuyICT, a central platform covering purchasing arrangements, framework agreements, flexible supplier panels and contract management. This provides consistent and coordinated access to digital suppliers across departments.
- The **United Kingdom** uses its Digital Marketplace and Crown Commercial Service agreements to procure digital services and specialists. These platforms simplify access to suppliers and support more flexible sourcing, including smaller suppliers that might not succeed in traditional large-contract procurement processes.
- **Korea** organises centralised digital procurement through the Smart Nara Marketplace and Digital Service Mall, supported by legal and procedural guidance. These mechanisms support transparency, co-ordination and consistent practice across government.

Sources: (Australian Government, 2026[27]; GOV.UK, 2026[28]; Crown Commercial Service, 2026[29]; Public Procurement Service, 2026[30]; Public Procurement Service, 2026[31]).

3.2.6. Monitoring is common, but evaluating results remain the missing link

Getting real value from digital investment depends on three connected capabilities: keeping delivery on track while work is underway; tracking performance as work progresses; and assessing whether the expected benefits were actually achieved once a project is complete. In most OECD countries, the first of these is reasonably well established. The second and third remain significantly weaker – and this gap limits governments' ability to learn from experience, demonstrate value for money and make better investment decisions over time.

Monitoring is the most mature of the three. The 2025 DGI shows that 31 out of 36 OECD countries (86%) have central monitoring mechanisms to track the progress of digital projects, broadly unchanged from 85% in 2023. This widespread adoption is a solid foundation. However, what is being tracked matters as much as whether tracking exists. In most countries, monitoring focuses on inputs and process - whether milestones have been met and budgets spent - rather than on whether projects are delivering the outcomes they were designed to achieve or whether new risks are emerging that require a change in direction. This kind of compliance-focused monitoring is useful for basic accountability, but it does not tell governments whether their investments are working in practice.

Public transparency around monitoring results is also limited. Only 17 out of 36 countries (48%) published progress or monitoring data online in 2025, up from 39% in 2023. This positive trend notwithstanding, in more than half of OECD countries information about how major digital projects are performing is not routinely

available to parliament, civil society or the public, reducing the scope for external scrutiny, independent challenge and shared learning across government.

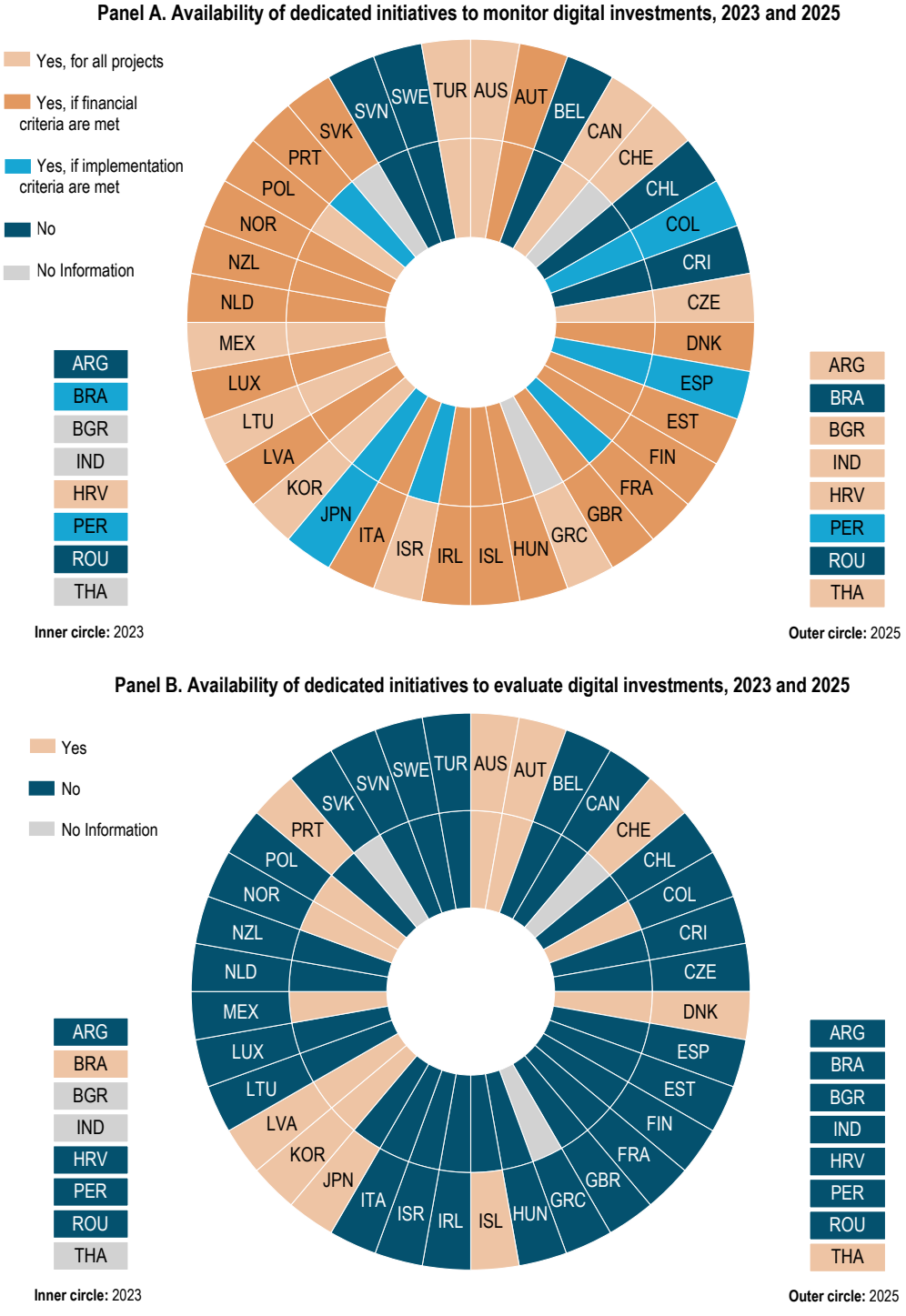
The use of more iterative project management approaches – which builds in regular review points and allows plans to be adjusted as work progresses – has increased from 39% of countries in 2023 to 53% in 2025. This is encouraging progress, but these approaches remain a minority practice. Many oversight systems are still better suited to large, linear projects than to the more flexible, staged delivery that modern digital projects, including those involving AI, typically require.

Policy evaluation – systematically assessing whether investments achieved their intended results after completion – is the least developed area. Challenges in establishing strong evaluation systems are not limited to the evaluation of digital investments. The need to systematise and strengthen policy evaluation efforts across government is reflected in the adoption of the OECD Recommendation on Public Policy Evaluation, which supports countries in developing robust evaluation systems (OECD, 2022[32]). By way of example, only 9 out of 36 OECD countries (25%) conduct cost-benefit analysis of completed digital projects, virtually unchanged from 27% in 2023. Only 16 out of 36 countries (44%) have a common method or tool for evaluating digital projects, up from 39% in 2023. These figures reflect a significant gap: governments are approving and funding digital investments without consistently measuring whether those investments delivered what was promised.

Without this feedback, governments find it harder to understand what worked and what did not, to scale up initiatives that are delivering results, or to stop funding approaches that are not. They may repeat avoidable mistakes, accumulate systems that no longer serve their purpose and struggle to make the case to decision-makers and the public that digital spending is worthwhile. As governments take on more complex digital programmes, particularly involving AI and large-scale data systems, the absence of systematic evaluation becomes an increasingly significant gap in investment governance.

Figure 3.5 illustrates this imbalance clearly: monitoring is broadly in place across OECD governments, but evaluation of outcomes and impact after delivery remains far less common. Qualitative evidence from the 2025 DGI suggests that evaluation tends to happen sporadically — triggered by individual project requirements, audits or external reviews rather than as a standard, built-in part of how digital investments are governed.

Figure 3.5. The majority of OECD countries monitor digital investments, but only half are actively evaluating their impact and results



Note: Panel A represents the individual responses to the question "Does the central/federal government have a monitoring system to track progress of digital/ICT projects?". Panel B represents the individual responses to the question "Has the leading digital government institution conducted any ex-post cost-benefit analysis of digital/ICT projects at the central/federal government level?". 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.

Source: OECD Survey on Digital Government 3.0 (2025); OECD (2026[4]; 2024[5]).

StatLink https://stat.link/qfmhc1

Several OECD countries are making monitoring a more systematic and routine part of how digital investments are managed (Box 3.7). For investments evaluation, countries are moving away from one-off reviews towards ongoing performance tracking that informs both current delivery and future investment decisions. These practices show how consistent evaluation can help governments learn from implementation, scale what is working, redirect initiatives that are falling short, and build a more evidence-based approach to digital investment over time (Box 3.8).

Box 3.7. Embedding monitoring tools into digital investment management

Some OECD countries have developed structured approaches to embedding monitoring and tracking into their digital investment frameworks:

- **Australia** builds continuous benefits tracking into its Digital and ICT Investment Oversight Framework, linking the identification, monitoring and review of expected benefits to key decision points. This connects funding decisions to measurable outcomes rather than process compliance.
- **Denmark**'s national IT council publishes twice-yearly public assessments of large digital projects using a traffic-light system to signal their status. This provides both transparency and an early warning mechanism, surfacing problems while there is still time to address them.
- **Italy** makes data on the progress and delivery of digital projects and programmes publicly available through dashboards and observatories, enabling ongoing scrutiny of how investments are performing.

Sources: (OECD, 2025[9]; Økonomistyrelsen, 2026[33]; Italiadomani, 2026[34]).

Box 3.8. Building evaluation mechanisms into digital investment management

Korea's e-Government Performance Management Plan institutionalises a data-driven approach to tracking the performance and impact of public-sector digital initiatives. Two tools sit at its core. The Integrated Evaluation System (e-IPSES) is a central digital platform that consolidates performance data from all government agencies in real time, aligning results against strategic goals and providing an evidence base for financial planning and resource allocation. Performance-Based Budgeting ensures that budget decisions are directly informed by programme outcomes: agencies submit annual performance plans and results, conduct self-assessments and participate in targeted evaluations, with findings feeding directly into the budgeting process. Together, these tools link fiscal decisions to demonstrated public value.

New Zealand's Department of Internal Affairs runs a system assurance function that provides independent oversight of high-risk digital investments. The oversight is conducted by assessors who are independent of the programmes being reviewed, strengthening its credibility. The Department also manages a pre-qualified panel of independent assurance providers — the GCDO Assurance Services Panel — giving agencies straightforward access to external assessment without a full procurement process.

Iceland's Digital Iceland has developed a common evaluation toolkit for assessing the impact of digital projects after completion. Published evaluations quantify the benefits achieved — including from the Digital Mailbox and online application systems, creating a direct feedback loop between delivery experience and future investment prioritisation.

Portugal uses a shared monitoring and evaluation platform (e-avalia) operated by the Agency for State Technology Reform, to track performance and outcomes consistently across digital initiatives. By providing a common platform rather than leaving each agency to develop its own approach, the tool supports more consistent assessment and enables course correction where projects deviate from their intended objectives.

Source: (Korea Institute of Public Finance, 2019[35]; Digital Iceland, 2025[36]; Digital Iceland, 2024[37]; Agência para a Reforma Tecnológica do Estado, 2024[38]; Yang and Torneo, 2015[39]; Government of New Zealand, 2019[40]).

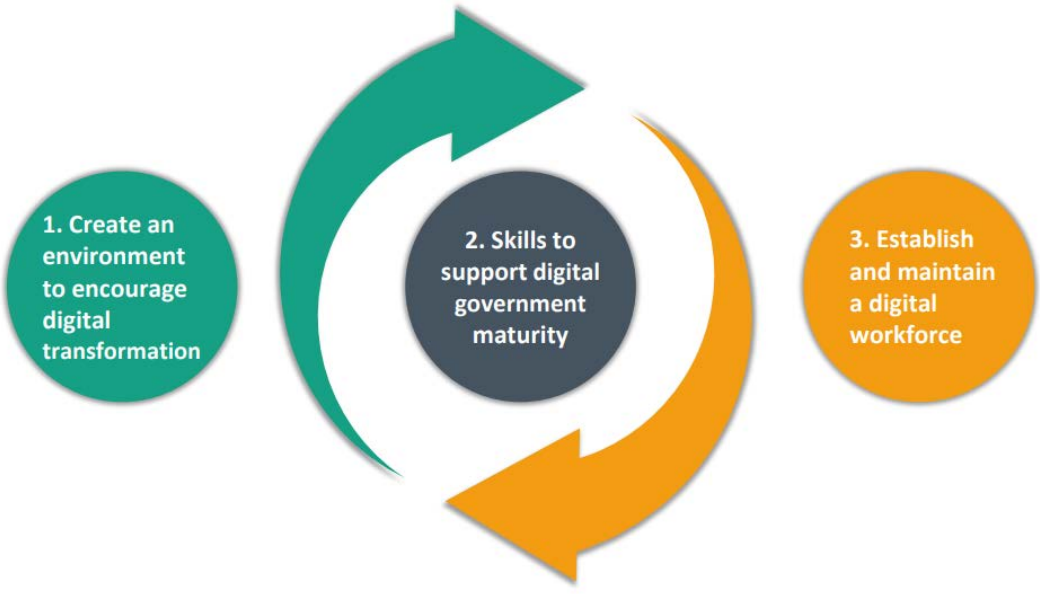
3.3. Building digital talent and skills: Awareness is growing, but action lags

Digital transformation is not only a technology challenge, but also a people challenge. The public sector needs people who can lead and deliver digital change: who understand user needs, can work with data, oversee AI systems responsibly, and collaborate across organisational boundaries. Technology alone cannot substitute for these capabilities. When the right skills are absent, digital investments underperform, external providers gain disproportionate influence over government systems, and the public sector loses the institutional knowledge it needs to govern technology well over the long term.

Three interconnected things need to work together to build a capable digital workforce: (1) creating the organisational conditions that support digital ways of working; (2) equipping public servants with the right technical, leadership, data and user-focused skills; and (3) putting in place systems to attract, develop and retain digital talent over time (Figure 3.6) (OECD, 2021[41]; Burtscher, Piano and Welby, 2024[42]; OECD, 2025[43]). Leadership, cross-functional teamwork and a culture of continuous learning are central to all three.

The 2025 DGI shows that OECD countries are making progress across all three areas, but that efforts remain fragmented and are not yet anchored in coherent, government-wide workforce strategies. Without this shift, governments risk falling behind in the skills needed to manage data-intensive systems, oversee AI responsibly and lead digital transformation with confidence.

Figure 3.6. OECD Framework for Digital Talent and Skills in the Public Sector



Source: (OECD, 2021[41])

3.3.1. Most countries have some strategic direction on digital skills, but dedicated strategies remain rare

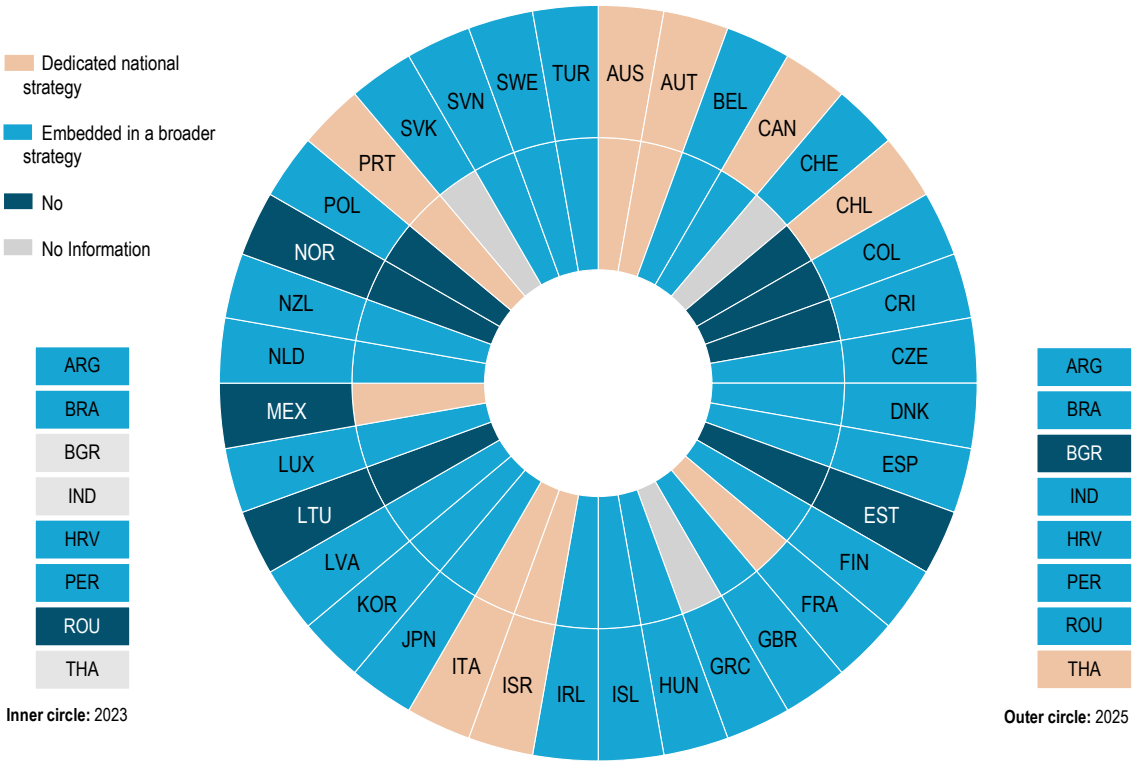
A coherent approach to building digital talent starts with a strategy, one that looks ahead, identifies what capabilities will be needed, and connects recruitment, training and career development into a single, consistent effort. When digital skills strategies are aligned with broader workforce planning, governments can anticipate emerging roles, guide recruitment and retraining, and build sustainable internal capability over time.

OECD countries increasingly recognise the importance of digital skills, and most have included them within broader strategies. According to the 2025 DGI, 32 out of 36 OECD countries (90%) have some strategic direction in place for digital talent and skills (Figure 3.7). However, only six of these countries have a dedicated strategy focused specifically on digital talent and skills – Australia, Austria, Chile, Israel, Italy and Portugal – a slight increase since 2023 but still a small minority. Most countries address digital skills as one component of a broader digital government or workforce rather than a priority. Four countries did not report including digital talent and skills in any form of strategy.

A dedicated strategy matters because it creates the focus and accountability needed to act consistently at scale. Countries with dedicated strategies are better positioned to set clear targets, allocate resources specifically to digital capability and track progress over time (Box 3.9).

Figure 3.7. Only six OECD countries have set dedicated strategies for a strategic direction to boost digital talent and skills in government

Availability of a digital talent and skills strategy for civil servants at the central/federal government, 2023 and 2025



Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023. Data for Canada were updated following a request from the country to requalify their Digital Talent and Skills Strategy as a dedicated strategy after the publication of the 2025 DGI; therefore, this change is not reflected in the 2025 DGI results.
Source: OECD Survey on Digital Government 3.0 (2025); OECD (2026[4]; 2024[5]).

StatLink https://stat.link/h1ferq

Box 3.9. Examples of dedicated strategies for digital talent and skills

Korea's Comprehensive Plan for Civil Servant Talent Development, led by Ministry of Personnel Management, aims to build a capable and adaptable public workforce. The plan strengthens digital and AI skills alongside broader policy-execution capability, and promotes self-directed learning through training tailored to roles and career stages. The plan combines foundational training for new recruits with continuous professional development, ethical-AI training and expanded use of digital learning platforms, aligned with long-term challenges including demographic change and technological transformation.

Australia's Data, Digital and Cyber Workforce Plan 2025-2030 sets out a government-wide approach to building sustainable digital capabilities across the civil service, organised around four priorities: (1) attracting, recruiting and retaining a data, digital and cyber workforce; (2) enhancing technical capabilities; (3) growing and deploying specialist cohorts; and (4) increasing capability planning across agencies.

Sources: (OECD, 2025[13]; Australian Government, 2025[44]).

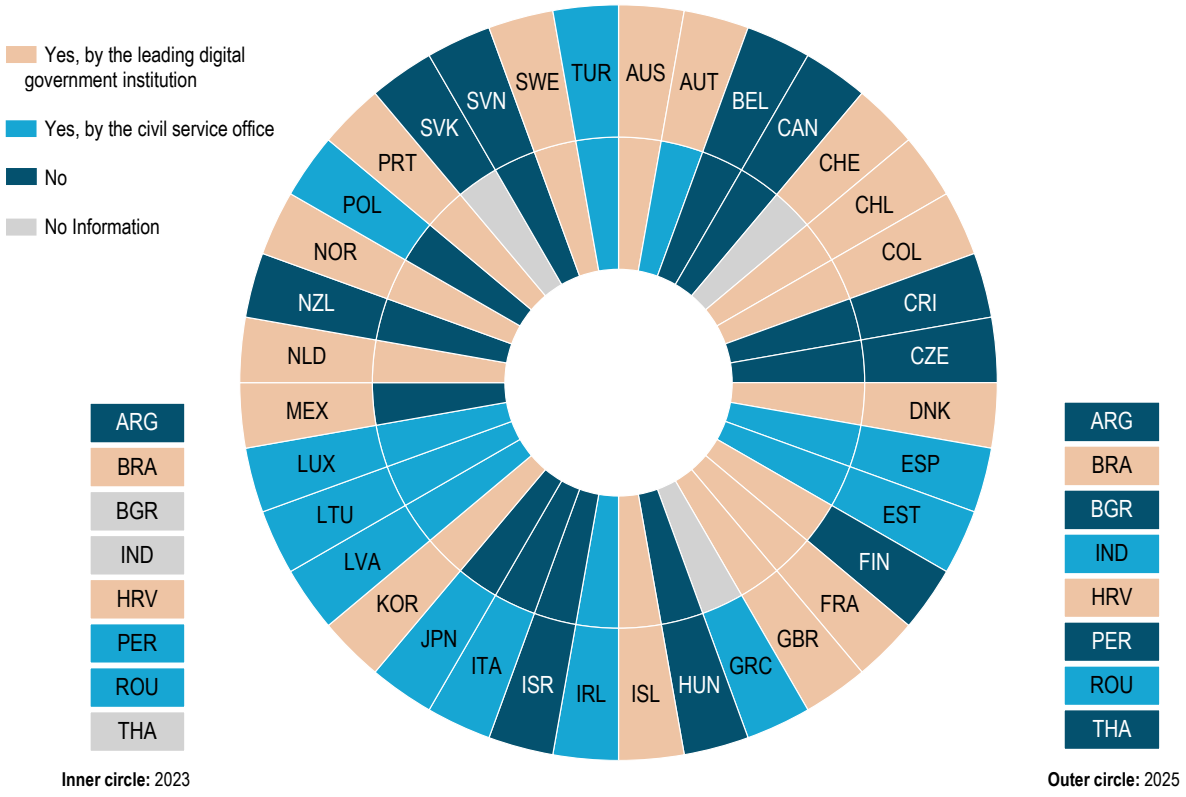
3.3.2. Skills assessments are improving, but gaps in action remain

Knowing where skills gaps exist is a prerequisite for addressing them. Without a clear picture of current capabilities and future needs, workforce development efforts risk being misdirected, training people in skills that are already available while leaving genuine gaps unaddressed.

The 2025 DGI shows that OECD countries are doing more to assess their digital skills needs. 26 out of 36 countries (72%) have conducted an assessment of digital talent and skills in the public sector, an improvement from 64% in 2023. However, 10 out of 36 countries (28%) still have not done so (Figure 3.8). Countries that have not assessed their skills base risk making workforce development decisions that are not grounded in evidence or targeted at the right areas. These results are consistent with broader challenges to conduct strategic workforce planning in government. Most countries that carry out workforce planning do it only at Ministry level (40%), and in 17% of countries workforce planning is carried out by the central HR body (OECD, 2025[45]).

Figure 3.8. A third of OECD countries still do not assess needs for digital skills

Conduction of an assessment of digital talent and skills in the public sector, 2023 and 2025



Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD Survey on Digital Government 3.0 (2025); OECD (2026[4]; 2024[5]).

StatLink https://stat.link/aozu1k

Beyond assessment, translating findings into action is the harder challenge. Despite more countries having assessed their skills needs, practical efforts by central digital government bodies to build capabilities have risen more modestly — from 51% of countries in 2023 to 62% in 2025. This gap between identifying needs and acting on them systematically suggests that many countries have not yet put in place the mechanisms – targeted learning pathways, strengthened digital leadership, co-ordinated workforce planning – needed to turn strategic awareness into real capability. Examples from Australia, Canada and France show how skills assessments can be connected directly to action (Box 3.10).

Box 3.10. Connecting skills assessments to action

France assesses its digital skills needs through a formal, evidence-based approach led by the Interministerial Digital Directorate (DINUM), which identifies workforce gaps and coordinates action across ministries. This includes digital HR hubs, strengthened governance between ministries, and a Digital Campus to support training, assessment and career development.

Australia analyses data about its civil service workforce to understand current skills gaps across different locations and functions. It also uses data about its digital government investments and the services or skills it is buying from the market to anticipate future demand and identify where internal capability needs to be strengthened.

Canada links investment planning data to strategic workforce planning to critical organizational priorities, creating a joined-up view of current and planned digital talent needs, sourcing decisions, and development activities based on data collected from agencies in annual planning and reporting exercises.

Sources: (General Council of the Economy, 2023[46]; Australian Government, 2025[44]; OECD, 2025[9]; Government of Canada, 2023[47]; Government of Canada, 2024[48]; Government of Canada, 2025[49]).

3.3.3. Attracting and retaining digital talent in government remains a persistent challenge

As governments expand their use of digital technologies, data and AI, attracting and keeping people with the right skills is increasingly difficult. Competition from the private sector is strong, particularly in areas such as data science, AI, cybersecurity and digital service design, and governments cannot typically match private sector salaries. Without strong internal capability, governments risk over-reliance on external suppliers, loosing institutional knowledge, and lacking the expertise needed to govern, oversee and adapt digital systems responsibly.

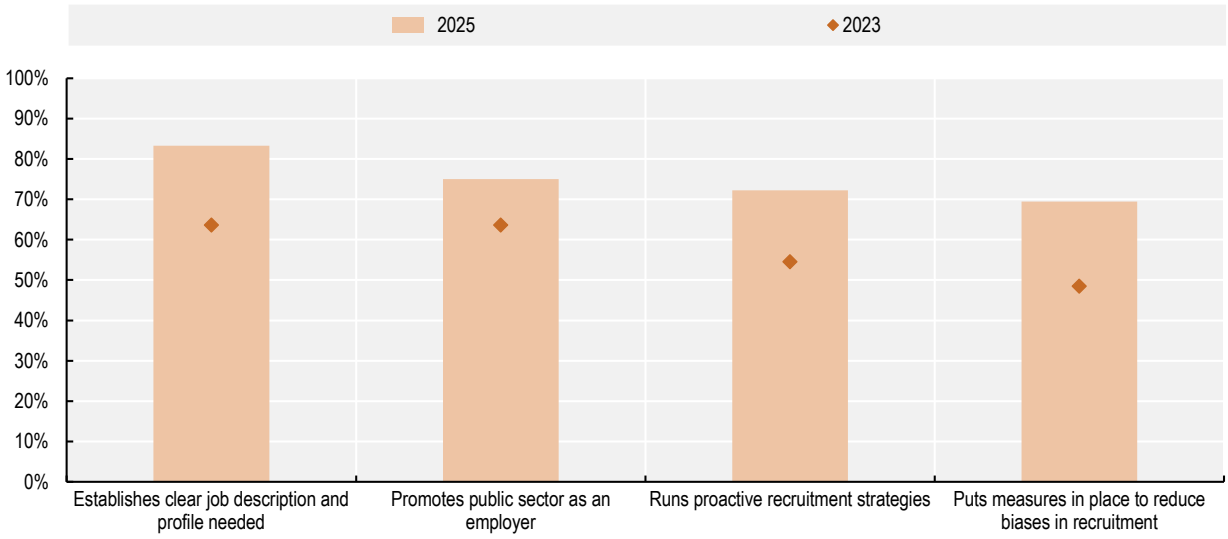
Addressing this challenge requires more than competitive remuneration: it calls for clear career pathways, meaningful and mission-driven work, continuous learning opportunities and modern, flexible working arrangements. Embedding digital skills and specialist expertise across policy, operational and leadership roles would ensure that digital transformation becomes part of core decision-making rather than confined to technical teams.

The 2025 DGI shows progress. The average score across initiatives to attract digital talent to the public sector increased from 58% in 2023 to 75% in 2025. As shown in Figure 3.9, across OECD countries:

- 30 countries have established clear job descriptions and profiles.
- 26 countries run proactive recruitment strategies.
- 27 countries are trying to actively promote on public sector as an employer.
- 25 countries have implemented measures to reduce biases in recruitment.

Figure 3.9. Initiatives to attract digital talent to the public sector

Percentage of OECD countries with selected initiatives to attract public-sector digital talent, 2023 and 2025



Note: 2025 data not available for Germany and the United States. 2023 data not available for Germany, Greece, Slovak Republic, Switzerland and the United States. Refer to Annex Table 3.A.3 for comprehensive OECD and Accession country data.
Source: OECD Survey on Digital Government 3.0 (2025); OECD (2026[4]; 2024[5]).

StatLink https://stat.link/24kqga

These are encouraging developments. However, many governments still need to go further — particularly as the demand for people who can work with AI systems, govern their use and assess their risks grows rapidly. Several OECD countries are experimenting with innovative approaches to broaden the talent pipeline, including fast-track immigration routes, international talent programmes and regional skills partnerships (Box 3.11).

Box 3.11. Initiatives to attract digital talent

- **Canada's** Global Talent Stream Skills Strategy offers fast-track enables the rapid hiring of highly skilled workers in in-demand fields, including digital and technology roles, through expedited work permits (often within two weeks) and enhanced employer support. for highly skilled technology workers, allowing employers to fill critical digital roles quickly;
- **Finland's** Talent Boost programme supports employers in urban and regional areas to attract international experts, with a particular focus on the technology sector;
- **France's** Tech Visa provides a fast-track immigration pathway for technology founders, employees and investors, reinforcing the country's image as a destination for digital talent and entrepreneurship;
- **Estonia's** pioneering e-Residency program allows entrepreneurs worldwide to establish and manage EU-based digital businesses remotely, enhancing the country's profile as a digital hub, and attracting internationally mobile digital professionals;
- the **United Kingdom's** Digital Skills Partnerships addresses regional skills gaps by bringing together government, industry and education providers to deliver tailored digital training at a local level.

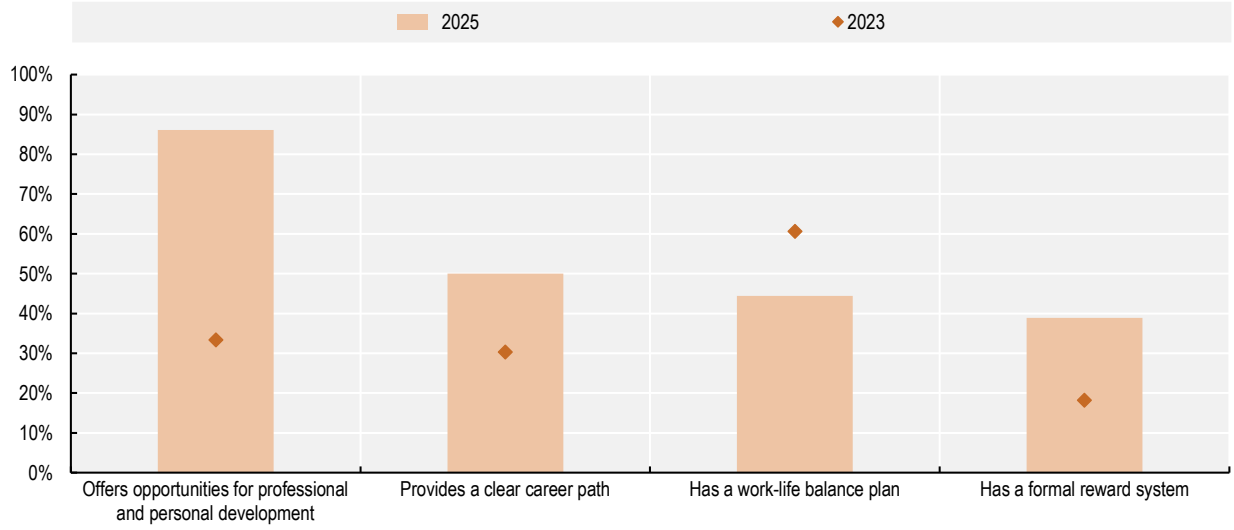
Sources: (Government of Canada, 2025[50]; Ministry of Economic Affairs and Employment, 2026[51]; La French Tech, 2023[52]; Government of Estonia, 2026[53]; Department of Science, Innovation and Technology, 2023[54])

Progress in attracting talent needs to be matched by stronger efforts to keep it. The 2025 DGI indicator on actions to develop and maintain digital skills rose from 36% in 2023 to 55% in 2025 — an improvement, but still low for such a critical area. As shown in Figure 3.10, the most common initiative is offering opportunities for professional and personal development. However, fewer countries provide clear career pathways for digital roles or formal recognition and reward for digital expertise. The number of countries offering work-life balance plans and modern working conditions, which matter significantly for retention, particularly among younger digital professionals, has declined since 2023. Strengthening these areas is essential if governments are to build and keep the internal capability they need, particularly as AI, large-scale data systems and cloud-based service delivery become more central to how government operates.

These findings are consistent with what public employees themselves report. A 2025 survey of nearly 57 000 employees from central government ministries and agencies in eight European Union countries showed that learning opportunities were the strongest drivers of engagement and wellbeing (OECD, 2025[45]). Public employees who have opportunities for mobility and to develop their digital skills tend to have more positive perceptions of organisational performance, and professional growth is particularly important for employee engagement. However, only half of employees feel that they are growing professionally, or that their organisation provides regular opportunities to build their digital skills, while only a third feel that their organisation supports mobility for career building.

Figure 3.10. OECD countries risk failing to build or retain internal digital capability

Percentage of OECD countries with selected activities to develop and maintain digital skills in the public sector, 2023 and 2025



Note: 2025 data not available for Germany and the United States. 2023 data not available for Germany, Greece, Slovak Republic, Switzerland and the United States.
Source: OECD Survey on Digital Government 3.0 (2025); OECD (2026[4]; 2024[5]).

StatLink https://stat.link/t37bds

Several OECD countries illustrate how performance frameworks, well-being initiatives and organisational continuity can support retention (Box 3.12).

Box 3.12. Examples of initiatives to retain digital talent

Greece has introduced performance-based incentives linked to the achievement of annual objectives, supported by individual development plans that align personal skill development (including digital skills) with organisational priorities. This approach strengthens motivation while reinforcing accountability and professional growth.

Chile requires public institutions to implement work-life balance protocols under national quality-of-work-life standards, helping public servants sustain long-term careers in government.

Estonia supports continuity by maintaining long-serving technical staff within core digital bodies, such as central IT and digital leadership functions, preserving institutional memory and stable digital governance over time.

Sources: OECD Survey on Digital Government 3.0 (2025)

Looking ahead, governments need to move beyond scattered initiatives towards a more strategic and sustained approach to building internal digital capability. Progress in recruitment and training is encouraging, but future efforts must embed these within coherent workforce strategies that connect skills development, career progression and working conditions to long-term institutional needs. Governments that invest consistently in clear career pathways, continuous learning and supportive working environments will be better placed to compete with the private sector for digital talent, retain critical expertise and reduce their dependence on external providers.

3.4. Building in-house or buying in: Finding the right balance

As governments expand use of digital technologies and AI, they face a fundamental question about how to deploy limited resources: what should be built or developed internally, and what should be bought from external providers? This is not a purely technical question. It has significant implications for long-term capability, accountability and value for money.

External providers can offer skills and capacity that governments do not have, accelerate delivery and provide access to specialist expertise. But over-reliance on the market poses risks. If governments outsource too much, they can lose the internal knowledge and judgement needed to define what they actually need, assess whether they are getting it, hold suppliers to account and adapt systems when circumstances change. These risks are compounded when the technologies involved demand transparency, such as AI models whose inner workings may not be fully visible to the buyer, or raise questions around data quality, dependency and ethical use that require strong in-house capacity to govern. When this happens, governments become dependent on external providers in ways that are difficult and costly to reverse, and that can undermine their ability to govern digital systems responsibly.

Within the spectrum of possibilities, the right answer is not to choose one approach over the other, but to be deliberate about the balance. Governments need sufficient internal expertise to define needs clearly, procure responsibly, manage suppliers effectively and maintain oversight across the life of a contract. External providers can then complement this internal capability, used strategically for specific skills or capacity rather than as a substitute for core expertise that governments should hold itself.

As AI adoption accelerates, the question of what governments should build in-house and what they should procure externally has become more pressing. AI systems require ongoing oversight, adaptation and governance, not just initial deployment. Governments that lack internal expertise in AI risk adopting systems they do not fully understand, cannot effectively evaluate and cannot adjust when they produce poor or harmful outcomes.

At the same time, AI creates real demand for highly specialised skills that can be difficult to build internally at pace. Data scientists, machine learning engineers and AI governance specialists are in high demand across

both the public and private sectors. For specific, well-defined applications where mature solutions already exist, procuring AI from the market, with appropriate safeguards, can be faster and more cost-effective than building in-house. For high-impact, mission-critical or data-sensitive applications, however, the case for internal development or at minimum strong and highly skilled internal oversight is much stronger.

In practice, the most sustainable approach is usually a deliberate combination: sufficient internal expertise to define needs, assess options, manage procurement, evaluate performance and govern AI systems responsibly, combined with selective use of external providers where the market is better placed to deliver. Matched to the risk profile and strategic importance of each initiative, this approach offers governments the best chance of using AI effectively while maintaining accountability and control (OECD, 2025[55]).

This sits within a broader effort across OECD countries to bolster internal digital capability while using external providers more strategically. Increasingly, the goal is not to eliminate external dependence altogether, but to ensure government retains enough expertise in-house to shape decisions, manage procurement, and govern digital and AI-enabled services effectively (Box 3.13).

Box 3.13. Rebuild internal digital capability

Several OECD countries are taking active steps to reduce reliance on external consultants and strengthen in-house digital expertise:

- the **United Kingdom** has introduced controls on consultancy spending and is investing in permanent digital, data and technology roles, supported by clearer career and pay frameworks for digital professionals across government;
- **Canada** has taken steps to rebalance spending away from external professional services, including technology contractors, by expanding targeted recruitment and upskilling of internal staff to build in-house digital capacity. These efforts are complemented by strengthened enterprise oversight of digital sourcing and contracting practices to reduce dependence reliance on the market external professional services for core digital delivery;
- **Australia** is reducing labour-hire and consultancy spending while reinvesting in data, digital and cybersecurity capability – backed by a dedicated workforce plan setting out how internal capability will be built and sustained through 2030;
- **France** has strengthened central digital capacity and governance through its Interministerial Digital Directorate (DINUM), reducing fragmentation across government and decreasing dependence on outsourced delivery.

Sources: (Government Digital Service, 2025[56]; Cabinet Office, 2024[57]; Giswold and Stanton, 2024[58]; Gallagher, 2024[59]; Australian Government, 2025[44]; Moal, 2026[60])

These examples point to a shared direction of travel: governments recognising that outsourcing can accelerate delivery in the short term but risks hollowing out the internal expertise needed to sustain digital transformation over time. Maintaining internal capability is not just about cost - it is about preserving the knowledge, judgement and accountability that effective digital government requires. Governments that develop this capability-led approach, balancing outsourcing with internal expertise, will be better placed to adapt to evolving technologies, govern AI responsibly and deliver secure, high-quality public services over the long term.

Annex 3.A. Additional tables with country data

Annex Table 3.A.1. Decision-making responsibilities of digital government leading institutions

Country	Prioritisation of digital investments		Management of the value proposition process		Approval of digital projects		Mandating external reviews		Provision of financial support for digital projects	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
Australia	●	●	●	●	●	●	●	●	●	●
Austria	●	●	●	●	●	●	○	○	●	○
Belgium	●	●	●	●	○	○	○	○	○	○
Canada	●	●	●	●	●	●	●	●	●	○
Chile	●	●	●	●	●	●	○	●	○	●
Colombia	●	●	●	●	●	●	●	●	●	●
Costa Rica	○	●	○	●	●	●	○	○	○	●
Czechia	●	●	●	●	●	●	○	○	○	○
Denmark	●	●	●	●	●	●	●	●	●	●
Estonia	●	●	●	●	●	●	●	●	●	●
Finland	○	○	●	●	○	○	○	○	○	○
France	○	●	○	○	○	●	○	●	●	●
Greece	N/A	○	N/A	●	N/A	●	N/A	○	N/A	●
Hungary	●	●	●	●	●	●	●	●	●	●
Iceland	●	●	●	●	○	●	○	○	●	●
Ireland	●	●	●	●	●	●	●	●	●	●
Israel	○	●	●	●	○	●	●	●	○	●
Italy	●	●	○	○	○	○	○	○	●	●
Japan	●	●	○	○	○	●	○	●	○	●
Korea	●	●	●	●	●	●	●	●	●	●
Latvia	●	●	●	●	●	●	●	●	●	●
Lithuania	●	●	○	●	●	●	○	●	●	●
Luxembourg	●	●	●	●	●	●	○	○	●	●
Mexico	●	●	●	●	●	●	●	●	○	○
Netherlands	○	○	○	○	○	○	○	○	○	○
New Zealand	●	●	●	●	○	○	○	○	●	○
Norway	●	●	●	●	●	●	○	○	●	●
Poland	●	●	●	●	●	●	●	○	●	●
Portugal	●	●	●	●	●	○	●	●	○	○
Slovak Republic	N/A	●	N/A	●	N/A	●	N/A	○	N/A	●
Slovenia	●	●	●	●	○	○	○	○	○	○
Spain	●	●	●	●	●	●	○	●	○	●
Sweden	●	●	●	●	●	●	○	○	●	●
Switzerland	N/A	●	N/A	●	N/A	●	N/A	●	N/A	●
Türkiye	●	●	●	●	○	○	●	●	○	○
United Kingdom	●	●	●	●	●	●	●	●	○	○

Country	Prioritisation of digital investments		Management of the value proposition process		Approval of digital projects		Mandating external reviews		Provision of financial support for digital projects	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
OECD Total										
● Yes	28	33	27	32	22	28	15	20	19	24
○ No	5	3	6	4	11	8	18	16	14	12
No Information	3	0	3	0	3	0	3	0	3	0
Argentina	●	●	●	●	○	○	○	○	●	●
Brazil	○	○	○	○	○	●	○	○	○	○
Bulgaria	N/A	●	N/A	●	N/A	●	N/A	●	N/A	○
Croatia	●	●	●	●	●	●	●	●	○	○
Indonesia	N/A	●	N/A	●	N/A	●	N/A	●	N/A	●
Peru	○	●	●	●	●	●	●	●	○	○
Romania	○	○	○	○	●	●	○	○	●	●
Thailand	N/A	●	N/A	●	N/A	●	N/A	○	N/A	○

Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

Annex Table 3.A.2. Procurement mechanisms used in digital government

Procurement mechanisms used for acquiring digital/ICT goods and services in the central/federal government

Country	Centralised purchasing		Joint procurements		Framework agreements		Dynamic Purchasing System (DPS)		Competitive dialogue	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
Australia	●	●	○	●	●	●	●	●	●	●
Austria	●	●	○	○	●	●	○	○	○	○
Belgium	●	●	○	○	●	●	○	○	●	●
Canada	●	●	○	○	●	●	○	○	○	○
Chile	○	●	●	●	●	●	○	○	○	Yes
Colombia	○	○	○	○	●	●	○	○	○	○
Costa Rica	●	●	○	○	○	●	○	○	○	○
Czechia	●	●	○	○	●	●	●	●	●	●
Denmark	●	●	●	●	●	●	●	●	●	●
Estonia	●	●	●	●	○	●	○	●	●	●
Finland	●	●	●	●	●	●	●	●	●	●
France	●	●	●	●	●	●	○	○	○	○
Greece	N/A	●	N/A	○	N/A	●	N/A	○	N/A	○
Hungary	●	●	○	●	●	●	●	●	○	○
Iceland	●	●	●	●	●	●	●	●	●	●
Ireland	●	●	○	○	●	●	●	●	●	●
Israel	●	●	○	○	○	●	○	●	○	○
Italy	●	●	○	○	●	●	●	●	○	○
Japan	○	●	○	●	○	○	○	○	○	○
Korea	●	●	●	●	●	●	●	●	●	●
Latvia	○	●	○	○	○	●	○	○	○	○
Lithuania	●	●	○	○	○	○	○	○	○	○
Luxembourg	●	●	○	○	●	●	○	○	●	●
Mexico	○	●	○	●	●	●	○	○	○	○
Netherlands	○	●	○	●	○	●	○	●	○	○

Country	Centralised purchasing		Joint procurements		Framework agreements		Dynamic Purchasing System (DPS)		Competitive dialogue	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
New Zealand	●	●	●	○	●	●	○	○	●	○
Norway	●	●	●	●	●	●	●	●	●	●
Poland	○	N/A	○	○	○	○	○	○	○	○
Portugal	○	●	○	○	○	○	○	○	○	○
Slovak Republic	N/A	●	N/A	●	N/A	●	N/A	○	N/A	○
Slovenia	●	●	●	●	●	●	○	●	○	○
Spain	●	●	○	●	●	●	●	●	○	●
Sweden	○	○	●	●	●	●	●	●	●	●
Switzerland	N/A	●	N/A	●	N/A	●	N/A	○	N/A	●
Türkiye	●	●	○	●	○	○	○	○	○	○
United Kingdom	●	●	●	●	●	●	●	●	○	○
OECD Total										
● Yes	24	33	12	20	23	31	13	17	13	14
○ No	9	2	21	16	10	5	20	19	20	21
No Information	3	1	3	0	3	0	3	0	3	0
Argentina	○	○	○	○	○	●	○	○	○	○
Brazil	●	●	●	●	●	●	○	○	○	●
Bulgaria	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○
Croatia	●	●	○	○	●	●	○	○	○	○
Indonesia	N/A	●	N/A	●	N/A	●	N/A	●	N/A	○
Peru	○	○	○	○	●	●	○	○	○	○
Romania	○	○	○	○	○	○	○	○	○	○
Thailand	N/A	●	N/A	○	N/A	○	N/A	○	N/A	○

Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

Annex Table 3.A.3. Initiatives to attract digital talent to the public sector

Availability of initiatives at central/federal government have initiatives to attract digital talents implemented by either the leading digital government institution or the civil service office (or equivalent)

Country	Establishes clear job description and profile needed		Runs proactive recruitment strategies		Promotes public sector as an employer		Puts measures in place to reduce biases in recruitment	
	2023	2025	2023	2025	2023	2025	2023	2025
Australia	●	●	●	●	●	●	●	●
Austria	●	●	○	○	●	●	●	●
Belgium	●	●	●	●	●	●	●	●
Canada	●	●	●	●	●	●	●	●
Chile	N/A	●	N/A	●	N/A	●	N/A	●
Colombia	●	○	●	○	●	○	○	○
Costa Rica	N/A	○	N/A	●	N/A	●	N/A	○
Czechia	N/A	●	N/A	●	N/A	○	N/A	○
Denmark	N/A	●	N/A	●	N/A	○	N/A	○
Estonia	●	●	●	●	●	●	●	●
Finland	●	●	●	●	●	●	●	●
France	○	●	●	●	●	●	○	●
Greece	N/A	●	N/A	○	N/A	○	N/A	●

Country	Establishes clear job description and profile needed		Runs proactive recruitment strategies		Promotes public sector as an employer		Puts measures in place to reduce biases in recruitment	
	2023	2025	2023	2025	2023	2025	2023	2025
Hungary	●	●	●	●	○	●	○	○
Iceland	○	●	○	●	●	●	●	●
Ireland	●	●	●	●	●	●	●	●
Israel	●	●	●	●	●	○	○	○
Italy	●	●	●	●	●	●	○	○
Japan	●	●	●	●	○	●	○	●
Korea	●	●	●	●	●	●	●	●
Latvia	N/A	○	N/A	○	N/A	○	N/A	●
Lithuania	●	●	○	○	●	●	○	○
Luxembourg	●	●	○	○	●	●	●	●
Mexico	●	●	●	●	●	●	●	●
Netherlands	●	●	●	●	●	●	●	●
New Zealand	●	●	○	●	●	●	●	●
Norway	N/A	○	N/A	●	N/A	●	N/A	●
Poland	●	●	○	○	○	○	○	○
Portugal	N/A	●	N/A	●	N/A	●	N/A	●
Slovak Republic	N/A	●	N/A	○	N/A	○	N/A	●
Slovenia	○	○	○	○	●	●	○	○
Spain	○	●	●	●	○	●	●	●
Sweden	N/A	○	N/A	○	N/A	○	N/A	○
Switzerland	N/A	●	N/A	●	N/A	●	N/A	●
Türkiye	●	●	●	●	●	●	●	●
United Kingdom	●	●	●	●	●	●	●	●
OECD Total								
● Yes	21	30	18	26	21	27	16	25
○ No	4	6	7	10	4	9	9	11
No Information	11	0	11	0	11	0	11	0
Argentina	○	○	○	○	○	○	○	○
Brazil	●	●	○	○	●	●	○	●
Bulgaria	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Croatia	○	○	○	○	○	○	○	○
Indonesia	N/A	●	N/A	●	N/A	●	N/A	○
Peru	●	●	●	●	●	●	●	●
Romania	○	○	○	○	○	○	○	○
Thailand	N/A	○	N/A	●	N/A	○	N/A	○

Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

REFERENCES

Agência para a Reforma Tecnológica do Estado (2024), *e-avalia*, https://eavalia.arte.gov.pt/. [38]

Australian Government (2026), *BuyICT*, https://www.buyict.gov.au/public. [27]

Australian Government (2026), *Digital and ICT Investment Oversight Framework*, https://www.digital.gov.au/investment. [14]

Australian Government (2025), *APS Data, Digital and Cyber Workforce Plan 2025-30*, https://www.dataanddigital.gov.au/sites/default/files/documents/2025-10/APS%20Data%2C%20Digital%20and%20Cyber%20Workforce%20Plan%202025-30_v1.0.pdf. [44]

Burtscher, M., S. Piano and B. Welby (2024), "Developing skills for digital government: A review of good practices across OECD governments", *OECD Social, Employment and Migration Working Papers*, No. 303, OECD Publishing, Paris, https://doi.org/10.1787/f4dab2e9-en. [42]

Cabinet Office (2024), *New controls across government to curb consultancy spend and save over £1.2 billion by 2026*, https://www.gov.uk/government/news/new-controls-across-government-to-curb-consultancy-spend-and-save-over-12-billion-by-2026. [57]

Crown Commercial Service (2026), *Search agreements*, https://www.crowncommercial.gov.uk/agreements. [29]

Department of Science, Innovation and Technology (2023), *Digital Skills Partnership*, https://www.gov.uk/guidance/digital-skills-partnership. [54]

Digital Agency, Japan (2025), *Control and management of national information systems*, https://www.digital.go.jp/en/policies/development_management. [21]

Digital Iceland (2025), *Benefits of digital processes*, https://island.is/en/o/digital-iceland/benefits-of-digital-processes. [36]

Digital Iceland (2024), *About 2.8 billion in benefits from the Ísland.is Digital Mailbox 2024*, https://island.is/en/news/about-2-8-billion-in-benefits-from-the-island-is-digital-mailbox-2024. [37]

Digital Switzerland (2025), *Action plan*, https://digital.swiss/en/action-plan/. [11]

Gallagher, K. (2024), *APS set to bring more than half a billion dollars of core work in-house*, https://ministers.pmc.gov.au/gallagher/2024/aps-set-bring-more-half-billion-dollars-core-work-house. [59]

General Council of the Economy (2023), *The State's human resources in digital technology*, https://www.economie.gouv.fr/cge/filiere-numerique-Etat#haut-de-page. [46]

Giswold, J. and J. Stanton (2024), *Refocusing Government Spending in 2023-24*, https://www.pbo-dpb.ca/en/publications/RP-2324-024-C--refocusing-government-spending-in-2023-24--recentrer-depenses-gouvernementales-2023-2024. [58]

GOV.UK (2026), *Digital Marketplace*, Government of the United Kingdom, https://www.applytosupply.digitalmarketplace.service.gov.uk/. [28]

Government Digital Service (2025), *Government Digital and Data Profession Capability Framework*, https://ddat-capability-framework.service.gov.uk/. [56]

Government of Canada (2025), *Directive on Digital Talent: Learn more about how the Government of Canada is strengthening the talent base of the GC digital community*, https://talent.canada.ca/en/directive-on-digital-talent. [49]

Government of Canada (2025), *Hire a top foreign talent through the Global Talent Stream*, https://www.canada.ca/en/employment-social-development/services/foreign-workers/global-talent.html. [50]

Government of Canada (2025), *Policy on the Planning and Management of Investments*, https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32593. [17]

Government of Canada (2024), *The Government of Canada Digital Talent Strategy*, https://www.canada.ca/en/government/system/digital-government/digital-talent-strategy.html. [48]

Government of Canada (2023), *Directive on Digital Talent*, https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32749. [47]

Government of Estonia (2026), *E-Residency of Estonia*, https://www.e-resident.gov.ee/. [53]

Government of Ireland (2023), *The Public Spending Code*, https://www.gov.ie/en/department-of-public-expenditure-infrastructure-public-service-reform-and-digitalisation/publications/the-public-spending-code/. [23]

Government of New Zealand (2025), *Digital Investment Office*, https://www.digital.govt.nz/standards-and-guidance/governance/investment/digital-investment-office. [24]

Government of New Zealand (2019), *Assuring Digital Governemnt Outcomes*, https://www.digital.govt.nz/assets/Documents/All-of-Government-ICT-Operations-Assurance-Framework.pdf. [40]

HERMES (2025), *Final project evaluation*, https://www.hermes.admin.ch/en/project-management/outcomes/final-project-evaluation.html. [12]

HERMES (2025), *Method overview: HERMES project management - The big picture*, https://www.hermes.admin.ch/en/project-management/method-overview.html. [10]

HM Treasury (2024), *Agile digital and IT projects: clarification of business case guidance*, https://www.gov.uk/government/publications/agile-digital-and-it-projects-clarification-of-business-case-guidance/agile-digital-and-it-projects-clarification-of-business-case-guidance. [15]

HM Treasury/DSIT/GDS (2025), *Performance Review of Digital Spend*, https://www.gov.uk/government/publications/performance-review-of-digital-spend. [19]

Italiadomani (2026), *Andamento dell'attuazione del piano*, https://www.italiadomani.gov.it/content/sogei-ng/it/it/strumenti/andamento-sull-attuazione-del-piano.html?orderby=%40jcr%3Acontent%2FyearAndSemesterLabel&sort=desc. [34]

Korea Institute of Public Finance (2019), *Performance Management of Budgetary Systems*, https://www.kipf.re.kr/cpemeng/Ecpm_CpemInfo1.do. [35]

Korean Government (2022), *ELECTRONIC GOVERNMENT ACT*, https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=ELECTRONIC+GOVERNMENT+ACT&x=28&y=23#liBgcolor0. [18]

La French Tech (2023), *French Tech Visa*, https://lafrenchtech.gouv.fr/en/come-work-in-france/french-tech-visa/. [52]

Ministerio de Hacienda (2026), *Coordinación de Modernización del Estado*, https://www.hacienda.cl/areas-de-trabajo/modernizacion-del-estado. [7]

Ministry of Economic Affairs and Employment (2026), *Talent Boost*, https://tem.fi/en/talent-boost-en. [51]

Ministry of Public Administration and Security (2022), *E-Government Act*, https://www.law.go.kr/LSW/lsInfoP.do?efYd=20220712&lsiSeq=239279#0000. [8]

Moal, C. (2026), *La nouvelle voie de la Dinum*, https://www.alliancy.fr/fr/la-nouvelle-voie-de-la-dinum-7a473c1d-74c7-42cd-974f-3be20756099e. [60]

New Zealand Government (2025), *Driving down the cost of digital in government*, https://www.digital.govt.nz/news/driving-down-the-cost-of-digital-in-government. [6]

OECD (2026), "Digital Government Index and Open, Useful and Re-usable Data Index: 2025 Results and Key Findings", *OECD Working Papers on Public Governance*, No. 90, OECD Publishing, Paris, https://doi.org/10.1787/6347ec74-en. [4]

OECD (2025), *Digital Government in Australia: Enhancing Digital Investment*, OECD Publishing, Paris, https://doi.org/10.1787/91c22326-en. [9]

OECD (2025), *Digital Government Review of Korea: Harnessing Digital and Data to Transform Government*, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/9defc197-en. [13]

OECD (2025), "Effectively Managing Investments in Digital Government: An OECD Policy Framework", *OECD Public Governance Policy Papers*, No. 76, OECD Publishing, Paris, https://doi.org/10.1787/5c324e91-en. [1]

OECD (2025), *Harnessing Artificial Intelligence in Social Security: Use Cases, Governance and Workforce Readiness*, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/b52405c1-en. [43]

OECD (2025), *Public Procurement of Artificial Intelligence: A Driver of AI Implementation in the Public Sector*, Internal document, unpublished. [55]

OECD (2025), *Workforce Insights from Central Governments: Findings of the 2024 OECD/EU Survey on Public Servants*, OECD Publishing, Paris, https://doi.org/10.1787/2f9080b1-en. [45]

OECD (2024), "2023 OECD Digital Government Index: Results and key findings", *OECD Public Governance Policy Papers, No. 44, OECD Publishing, Paris*, https://doi.org/10.1787/1a89ed5e-en. [5]

OECD (2024), *Good Practices for Procuring Computers and Laptops in Latin America: Fostering Neutrality and Market Engagement*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/cdf11f4d-en. [2]

OECD (2022), "Recommendation of the Council on Public Policy Evaluation", *OECD Legal Instruments*, OECD/LEGAL/0478, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0478. [32]

OECD (2022), *Towards Agile ICT Procurement in the Slovak Republic: Good Practices and Recommendations*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/b0a5d50f-en. [25]

OECD (2021), *The E-Leaders Handbook on the Governance of Digital Government*, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/ac7f2531-en. [3]

OECD (2021), "The OECD Framework for digital talent and skills in the public sector", *OECD Working Papers on Public Governance*, No. 45, OECD Publishing, Paris, https://doi.org/10.1787/4e7c3f58-en. [41]

OECD (2017), *Public Procurement for Innovation: Good Practices and Strategies*, OECD Public Governance Reviews, OECD Publishing, Paris,, https://doi.org/10.1787/9789264265820-en. [26]

OGCIO (2024), *Digital Oversight*, https://www.ogcio.gov.ie/en/corporate-pages/policy/digital-oversight/. [22]

Økonomistyrelsen (2026), *Statusrapporter*, https://oes.dk/it-og-oekonomistyring/statens-it-raad/statusrapporter/. [33]

Public Procurement Service (2026), *Digital Service Mall*, https://digitalmall.g2b.go.kr/. [31]

Public Procurement Service (2026), *Nara Market*, https://www.g2b.go.kr/. [30]

République française (2024), *Lauréats guichets numériques du Fonds pour la transformation de l'action publique (FTAP)*, https://www.data.gouv.fr/datasets/laureats-guichets-numeriques-du-fonds-pour-la-transformation-de-laction-publique-ftap. [20]

The Treasury (2025), *Better Business Cases*, https://www.treasury.govt.nz/information-and-services/public-sector-leadership/investment-management/better-business-cases. [16]

Yang, S. and A. Torneo (2015), "Government Performance Management and Evaluation in South Korea: History and Current Practices", *Public Performance & Management Review*, Vol. 39/2, pp. 279-296, https://doi.org/10.1080/15309576.2015.1108767. [39]


45.09
40
58
59
Chat
Website
E-mail
Blog
30% 55% 65% 80%
Communication Network
STATUS 1
STATUS 1
STATUS 1
STATUS 1

4 Adopting and governing AI in government

While key enablers for AI adoption in government are reaching maturity, delivery capabilities remain uneven. Governments are taking important steps to upskill public servants, but there is room for growth in using AI for specific purposes. And while most countries fund AI initiatives, support for procurement lags. Cloud computing capacities for AI are also solidifying but other forms of digital infrastructure are less developed. Strong governance is the cornerstone of successful AI adoption in government, and most countries have oversight or advisory bodies, but activity focuses on guidance rather than enforcement. Similarly, most countries commit to algorithmic transparency but few have formal standards or open algorithm registers. In addition, limited internal repositories of AI use cases constrain transparency and governance. Challenges to measuring the impact of AI limit decision-making and contribute to a proliferation of pilots with little potential to scale. While stakeholder engagement around strategies is strong overall, sustained, user and cross-border involvement remain limited.

Key messages

- **Artificial intelligence (AI) use in government is spreading, but not evenly.** AI is now used in at least one area of government in 35 of 36 (97%) of OECD countries, with strongest uptake in internal processes and public services. Use in policymaking and oversight remains more limited, reflecting higher-stakes applications and stronger requirements for data quality, transparency and assurance.
- **Governance frameworks for AI in government are becoming more widespread, but enabling conditions remain uneven.** Nearly all OECD countries have an AI-in-government strategy and 30 of 36 countries (83%) have at least one institution responsible for governing AI in the public sector. Yet the practical conditions for scaling AI – including data governance, infrastructure, skills and organisational capacity – remain uneven across countries.
- **AI skills efforts are expanding, but activity-specific training lags.** Across the OECD, 32 of 36 countries (89%) report training programmes to support AI in government. Yet fewer offer training on using AI in public services or policymaking (13 of 36 countries, or 36%, each), suggesting that broad capability is improving faster than role-specific readiness.
- **Funding outpaces procurement readiness.** Most OECD countries fund AI initiatives, but only 21 of 36 countries (58%) provide central support for procuring AI goods and services. Governments therefore need stronger capabilities to manage vendor lock-in, accountability, transparency, data rights and lifecycle risks.
- **Guardrails are expanding, but operational controls lag.** All OECD countries have at least one form of guardrail, yet only 14 of 36 countries (39%) require pre-deployment risk assessments, 12 of 36 (33%) have internal review committees and 11 of 36 (31%) conduct post-deployment audits. Transparency is also weak: only 11 of 36 countries (31%) have a formal standard and 6 of 36 (17%) have an open algorithm register.
- **Evidence and user feedback remain limited.** Only 10 of 36 OECD countries (28%) report any financial or non-financial impact measurement of AI use cases in government, even though half say adoption decisions draw on evidence of potential efficiency or cost savings. Engagement is strong in strategy development, but much weaker in implementation: only 15 of 36 countries (42%) engage service users and 8 of 36 (22%) have citizen feedback or complaint mechanisms.

4.1. Introduction

Artificial intelligence (AI) is among the most transformative forces of the 21st century, becoming a critical component of the digital government landscape. Across OECD countries, use of AI in government is shown to improve government productivity (efficiency and effectiveness), support more proactive and human-centred services, and strengthen responsiveness and accountability.[1] As governments confront increasingly complex policy challenges, AI can play a central role in improving decision making, automating routine processes and scaling integrated services.

Unlocking AI's benefits depends on the strength and resilience of underlying digital systems and surrounding ecosystems. As highlighted in previous chapters, AI adoption is only as strong as the foundations on which it rests, including high-quality and interoperable data, coherent digital public infrastructure (DPI), adaptive investment and procurement models, and a public sector workforce with the skills to develop, govern and oversee AI. Where these foundations are weak or fragmented, AI cannot scale effectively and might amplify rather than mitigate risks.

Managing AI's risks is therefore integral to advancing trustworthy and resilient digital transformation. Governments must mitigate ethical risks that can create adverse outcomes and rights infringements, operational risks that erode trust, exclusion risks that widen digital divides, and public resistance to the use of AI by governments. Not adopting AI also presents a risk: it can lead to missed opportunities to enhance services, improve efficiency and strengthen evidence-informed policymaking.

However, governments face implementation challenges, including skills shortages, outdated legacy systems,

inadequate data governance and fragmented investment frameworks. Public administrations also need to pursue AI in ways that reinforce the public interest, uphold rights and ensure societal benefits to distinguish government use of AI from private sector incentives.

The OECD flagship report *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions* highlights that advancing AI in government requires a structured and holistic approach. The OECD Framework for Trustworthy AI in Government (Figure 4.1), provides a roadmap to help governments align their initiatives with the OECD AI Principles (2024[1]). The Framework organises specific activities around three pillars: (1) enablers to facilitate adoption; (2) guardrails to guide trustworthy use; and (3) engagement approaches to shape user-centred and responsive adoption.

Figure 4.1. OECD Framework for Trustworthy Artificial Intelligence in Government

Source: (OECD, 2025[2]).

4.2. Government AI maturity has improved in most OECD countries

Across the OECD, government AI maturity continues to improve, reflecting efforts to build the enablers, guardrails and transparency mechanisms needed for responsible AI adoption. The OECD Digital Government Index (DGI) AI maturity component assesses how well central governments are prepared to use AI strategically and responsibly. This component provides scores to questions in the OECD Survey on Digital Government 3.0, covering enablers such as national AI-in-government strategies and the openness of engagement of their design, guardrails such as oversight and ethical advisory bodies, transparency in the use of algorithms, and the extent to which AI is used in government operations, policymaking and public services. To complement these indicators, the Survey includes a separate AI Annex with qualitative questions to inform the narrative analysis in this chapter. Responses to the Annex were not scored for the 2025 DGI but provide contextual evidence and illustrative examples (see the Methodology annex). For the 2025 DGI, no data are available for Germany and the United States because they did not participate in the Survey.

Between 2023 and 2025, most OECD countries either improved or maintained their government AI maturity. Estonia, France, Korea and the United Kingdom remain consistently high performers, driven by the consolidation of ethical or regulatory oversight bodies and the implementation or strengthening of transparency mechanisms, particularly algorithmic transparency

instruments. France is notable for having in place all items measured in the AI maturity component. Belgium, Israel, Latvia, Norway, and Portugal made significant progress compared to 2023 baselines, largely in the adoption of new strategies, the expansion of AI use and more open engagement approaches. Many other countries recorded smaller improvements, and a few saw declines indicating that maintaining momentum in implementation is as important as introducing new instruments.

Looking ahead, European Union (EU) Members might be poised to advance further as the requirements of the EU AI Act (2024[3]) take effect. Although the Act was adopted in 2024, many provisions relevant to the DGI, such as for algorithmic transparency mechanisms, were not yet applicable during the 2025 DGI analysis window. While a small number of EU Members took proactive steps in advance toward compliance, most had not yet implemented the Act's obligations at the time of measurement. This suggests a likely future increase in maturity scores as countries align their practices with forthcoming requirements.

Taken together, these developments highlight that OECD countries are making steady progress in building the foundations for trustworthy and strategic AI use. However, they also reinforce a recurring theme of the report: governance instruments must be actively implemented, continuously maintained, and integrated into day-to-day decision making to deliver sustained improvements in AI maturity and digital resilience.

4.3. AI USE IN GOVERNMENT HAS GROWN BUT REMAINS LIMITED IN SOME POLICY AREAS

AI adoption in government has expanded significantly, particularly for internal processes, but remains uneven across government activities. The 2025 DGI analysis window coincided with a surge of interest in AI, fuelled by rapid advances in generative AI (GenAI). During this period, the share of OECD countries using AI for internal processes rose from 23 of 33 measured countries (70%) in 2023 to 31 of 36 (86%) in 2025, and adoption in public services increased from 22 of 33 countries (67%) to 27 of 36 (75%) (Figure 4.2). However, adoption remains more limited in policymaking and accountability activities. Only 13 of 36 OECD countries (36%) report using AI to support policymaking (up from 11 of 33 countries, or 33%, in 2023), and 12 of 36 countries (33%) have used AI to strengthen oversight and accountability.

To some extent, the gains reflected in internal processes and public services reflect the relative ease of applying AI to structured administrative tasks – such as document classification and workflow optimisation – compared to policymaking and accountability activities, which can be higher-stakes, involve more contestable judgements, and often have more complex governance and data requirements. More broadly, uneven uptake across government activities reflects varying constraints depending on the type of activity – such as skills shortages, legacy IT, and difficulties accessing and sharing high-quality data – alongside greater requirements for privacy, transparency and representation that can be more demanding in policy and oversight settings.

As a result, AI use in policymaking and accountability activities is often narrower and more cautious, and depends on more comprehensive, integrated data and stronger assurance and oversight arrangements than many administrative applications. Furthermore, these conditions remain uneven across countries (Chapter 2).

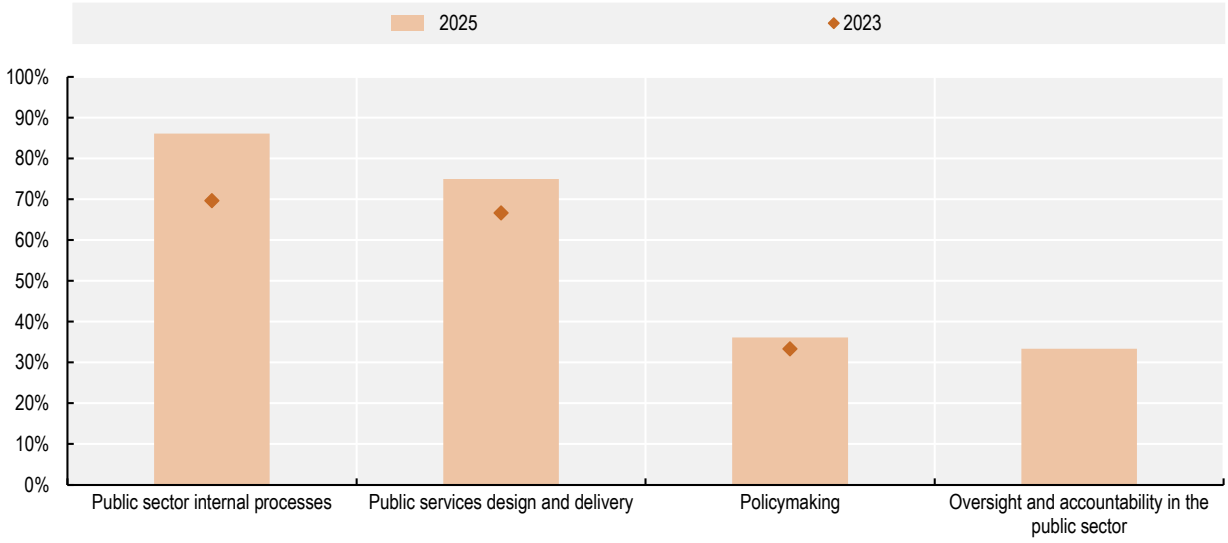
Overall, this report shows that AI use expands most rapidly where foundations are strong, and more slowly where risks, data gaps or governance constraints are greatest. This mirrors other OECD (2025[2]) work specific to AI in government, which found that uptake tends to be faster where data are available and processes are more standardised, and slower where legacy systems, skills gaps, and higher requirements for privacy, transparency and representation raise the bar for deployment.

Still, AI use is nearly universal across the OECD area, with 35 of 36 OECD countries (97%) and three of six accession candidate countries (50%) using AI in at least one of these activities. Seven OECD countries (Chile, Estonia, France, Korea, Latvia, Luxembourg and Norway) use AI in all four areas, while no accession candidate country has reached this breadth.

Box 4.1 offers notable examples of AI applied across OECD countries, including cases that illustrate how countries move from experimentation toward operational deployment. Additional examples from beyond the 2023/24 analysis window are documented in the OECD (2025[2]) report *Governing with AI* and listed on the OECD.AI Policy Navigator,[2] highlighting the rapid pace of change in this field.

Figure 4.2. AI use is more widespread in internal processes and public services than in policymaking and accountability

Percentage of OECD countries using AI in the public sector by policy area, 2023 and 2025



Note: Oversight and accountability in the public sector was not measured in the 2023 survey, therefore no comparison is available. Accession candidate countries report the following use rates: Internal processes (25%); Public services (38%); Policymaking (0%); Oversight and accountability (17%). 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. Data for Indonesia and Thailand cover 1 January 2022 to 31 December 2023, while Oversight and accountability does not include data for these countries. Refer to Annex Table 4.A.1 for comprehensive OECD and Accession country data.
Source: OECD (2025), Survey on Digital Government 3.0.

StatLink https://stat.link/jy4sme

Box 4.1. How governments harness AI across policy areas

AI increasingly demonstrates relevance for a range of government activities, including:

- **Internal processes**, such as **Korea's** e-RFP Assistance System, which brings together several types of AI, including GenAI, to draft requests for proposals and ensure compliance with regulations. The system provides a repository of past government procurement data to inform government officials. Its adoption has resulted in a 70% reduction in document preparation time compared to traditional approaches, and 99.9% compliance with procurement regulations.
- **Public services**, such as **Iceland's** Askur AI chatbot, which supports citizens in accessing information and conducting services on the government's central portal. Askur addresses 90% of citizen correspondence, significantly reducing phone calls and emails to service centres.
- **Policymaking**, such as the **United Kingdom's** Parlex is a research assistant for parliamentary information. It can quickly find and analyse key contributions from members of parliament, parliamentary questions, and committee hearings. Parlex helps bring the views of parliamentarians directly into the policymaking process, prepare ministers more effectively, and refine policy before it is introduced.
- **Oversight and accountability**, such as **Brazil's** Alice system, which continuously analyses public procurement activities for potential risks of fraud, errors and inefficiencies, and facilitates interventions when they are detected. In 2023, it analysed nearly 191 000 acquisitions and triggered 203 audits involving contracts worth EUR 4.15 billion (equivalent). The system also enabled a reduction in audit processing from 400 days to 8 days.

Source: (OECD, 2025[4]; Digital Island, n.d.[5]; UK Government, n.d.[6]; OECD Observatory of Public Sector Innovation (OPSI), n.d.[7]; Korean Public Procurement Service, 2022[8])

While use of GenAI in government is expanding, it remains less prevalent than the use of broader AI and machine learning (ML) systems. This is consistent with findings from the OECD (2025[2]) and the European Commission (EC) (2025[9]) that show uneven levels of preparedness for, and use of GenAI systems in government across countries. Despite these challenges, 64% of OECD countries and 50% of accession candidate countries use GenAI systems for at least one purpose.

Among OECD countries, GenAI use tends to concentrate in lower-risk, productivity-enhancing applications rather than in high-stakes operational contexts. The most common uses include: supporting public servants in their functions (20 of 36 countries, or 56%), such as through drafting assistance, search and knowledge retrieval, or conversational support; generating automated reports or summaries to inform decision-making (15 of 36 countries, or 42%); creating citizen-engagement content (15 of 36, or 42%), such as consultation replies and newsletter texts; drafting or assisting in the creation of policy documents (13 of 36, or 36%); and supporting the design and delivery of public services (13 of 36, or 36%), most often during early ideation, user research or prototype-development phases.

These uses reflect a cautious approach that prioritises internal productivity and augmenting human work over fully automated processes or decision making. They also illustrate reliance on commercial GenAI products such as Microsoft Copilot, OpenAI's ChatGPT or Mistral's Le Chat, and on self-hosted pre-trained open-source or open-weight systems such as Meta's Llama models. Open-weight systems make a model's trained parameters ("weights") available for others to run and fine-tune even if the training data and full development process are not openly shared (OECD, 2025[10]). Governments may favour open-weight systems because they can be deployed in contained environments, offering greater control over data handling and security, more scope for customisation to local languages and procedures, and reduced dependence on a single vendor.

Notably, no OECD Member or accession candidate country imposes a blanket ban on the use of GenAI systems in government, although some restrict the use of specific systems such as DeepSeek and other high-risk or unverified tools. This reinforces a broader trend observed throughout this chapter: governments are generally open to exploring GenAI, but adoption remains measured and risk sensitive, shaped by concerns around security, data protection, quality assurance and public trust.

4.4. Enablers for AI adoption in government are maturing but delivery capabilities remain uneven

Enablers are the foundational elements necessary for trustworthy and scalable AI implementation in government. The OECD identifies seven enablers: governance; data (including open government data); digital infrastructure; skills and talent; AI investment; public procurement; and partnering with non-governmental actors (2025[2]). Several of these – notably data, infrastructure, investment and partnering – are not AI-specific but structural conditions that support all digital transformation. As highlighted in the preceding chapters, these foundations are prerequisites for digital resilience, and their uneven maturity shapes governments' ability to adopt AI safely, strategically and at scale.

4.4.1. Strong governance is the cornerstone of successful AI adoption in government

Robust governance is the primary enabler for trustworthy and effective AI use in government. Two components are critical: (1) a high-level national strategy that articulates objectives for adopting AI in government; and (2) a whole-of-government approach to co-ordinating its implementation, ensuring coherence across ministries and establishing clear accountability for results.

Nearly all OECD countries have such a strategy. During the 2025 DGI analysis window, all but three OECD Members (Canada, Mexico and Switzerland) had an AI-in-government strategy. By 2025, Canada and Switzerland published strategies, marking a small improvement since the 2023 DGI. Among accession candidate countries, Argentina and Brazil also have national strategies.

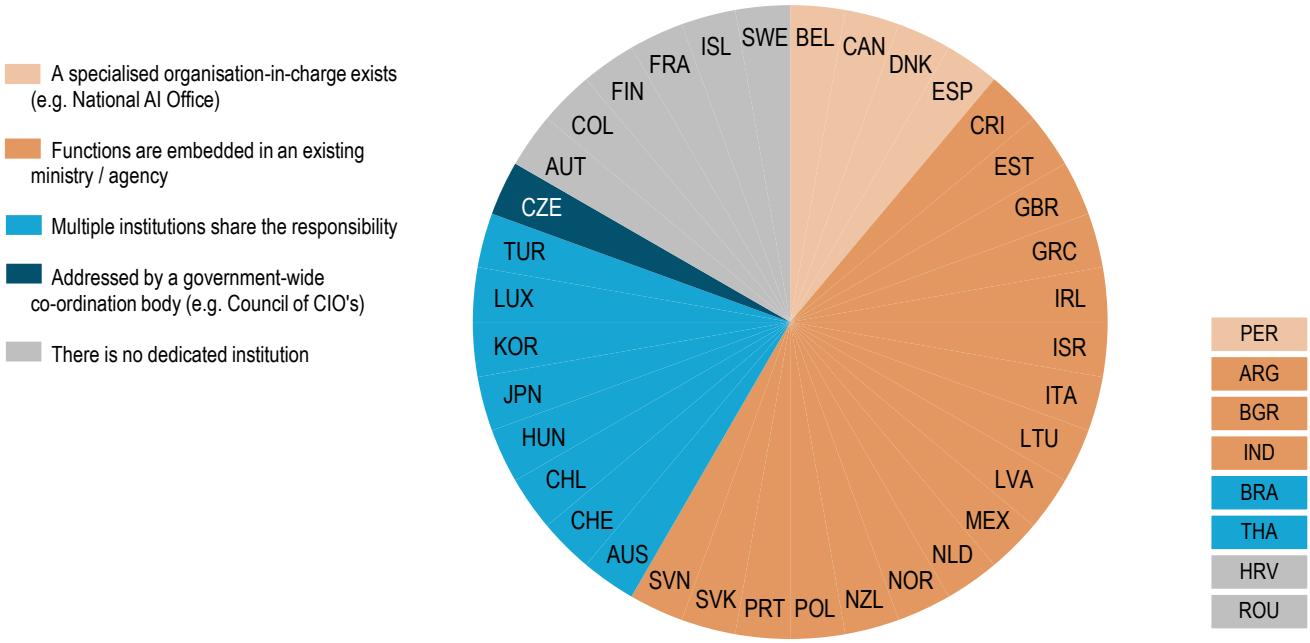
These strategies commonly emphasise trustworthy, human-centric AI, highlighting principles such as fairness, accountability, robustness and security, in line with the OECD AI Principles. They often position

government as a testbed for innovation while setting priorities that mirror the broader digital-government agenda. Common priorities include building data and digital infrastructure, strengthening public sector skills and organisational capabilities, creating dedicated co-ordination and governance mechanisms, and promoting experimentation through pilots, sandboxes and cross-sector collaboration.

Importantly, most countries designate institutions to implement these strategies. According to the DGI, 30 of 36 OECD countries (83%), and four of six accession candidate countries (67%) have at least one public institution responsible for governing the use of AI in the public sector (Figure 4.3). These bodies play central roles in shaping standards, ensuring ethical oversight, guiding procurement and risk management practices, and helping translate high-level intentions into operational decisions (Box 4.2).

Figure 4.3. Most countries designate institutions to implement AI in government strategies

Type of institution(s) responsible for governing AI in the public sector, by country, 2025



Note: Data not available for Germany, the United States, Indonesia or Thailand. Data cover 1 January 2023 to 31 December 2024.
Source: OECD (2025), Survey on Digital Government 3.0.

StatLink https://stat.link/netwcf

Box 4.2. Examples of institutions governing AI in the public sector

Spain

The Spanish Agency for the Supervision of AI (AESIA) is the public body responsible for ensuring the ethical and safe use of AI by public and private entities in Spain, as mandated by the EU AI Act's requirement for national competent authorities. This includes drafting guidelines and legislation for the use of AI in public services, which ensure that: civil servants are sufficiently trained; fundamental rights of citizens are sufficiently protected; and projects comply with national and EU legislation around data governance, transparency and robustness for AI systems.

Czechia

In Czechia, the Committee for AI serves as a permanent advisory and co-ordinating body. Its mandate is to support the implementation of the National Artificial Intelligence Strategy 2030, which outlines "AI in public administration and public services" as one of seven key areas. The committee fulfils this function by publishing regularly updated Action Plans that put forward projects and establish key performance indicators for various goals. These goals include expanding the use of AI in the public sector and ensuring that public-sector employees are aware of the possibilities and limitations of AI.

Source: (Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), n.d.[11]; Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), n.d.[12]; Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), n.d.[13]; Ministry of Industry and Trade, Czech Republic, 2024[14])

4.4.2. Governments take important steps to upskill public servants, with room for growth in using AI for specific purposes

Strong governance frameworks for AI must be matched by the skills and confidence of public servants who use AI tools in their daily work. While strategies and central co-ordination provide essential direction, it is frontline public servants who ultimately make decisions about how AI is applied, interpreted and overseen. Consistent with earlier chapters, the OECD finds that the skills gaps remain the most common challenge hindering successful AI adoption in government (2025[2]).

To close these gaps, 32 of 36 OECD countries (89%) and three of six accession candidate countries (50%) have training programmes for various skills required to support the development and use of AI in government. These focus most frequently on the practical and ethical use of AI tools (28 of 36, or 78%, and 22 of 36, or 61%, of OECD countries, respectively), and data privacy and security (20 of 36 countries, or 56%), with fewer offerings for using AI in public services or policymaking (each 13 of 36 countries, or 36%) (Figure 4.4 and Box 4.3).

Box 4.3. AI in government training efforts for public servants

Training initiatives typically fall into a few recurring patterns, often combining broad baseline literacy with role-specific depth:

- **Broad foundational courses.** Many countries make widely available online courses, such as the globally accessible "Elements of AI" course, accessible through civil-service learning portals (e.g. Czechia, Luxembourg and Norway), or generalist training for the French public service designed by the Digital Campus and accessible through the MENTOR platform, to build baseline awareness of opportunities and risks.
- **Government-tailored fundamentals.** Some administrations offer introductory training aligned with domestic frameworks and guidance, such as Australia's "AI in Government Fundamentals" course for the Australian Public Service (APS), which emphasises safe and responsible use consistent with Australia's AI Ethics Principles.
- **Specialised technical training.** Some programmes target specific capabilities and functions and may require longer participation or in-person engagement, such as the Korean Internet and Security Agency's (KISA) "AI Security Control" course on security monitoring and response to AI-enabled attacks (with both extended in-person and shorter online options).

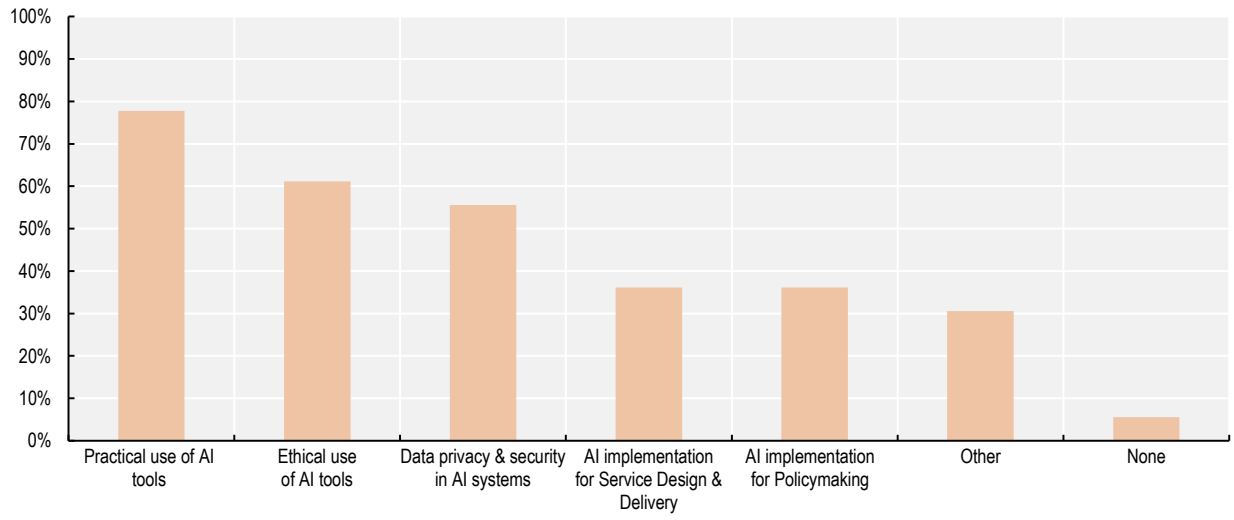
Many initiatives were launched after 2024, helping close gaps in several countries while bolstering efforts in those with existing offerings:

- **Australia's** APS AI Plan, which sets expectations for mandatory capability development and training support for safe and responsible use of GenAI tools;
- **Colombia's** 80-hour, fully virtual and free AI diploma for public servants, delivered with the University of Cartagena and designed to reach thousands of officials;
- **Costa Rica's** national partnership with UNESCO to equip public servants with AI and digital transformation skills, including an online course on AI and digital transformation in government;
- **Finland's** new state-administration learning packages that include an "AI academy" video curriculum within broader digital skills provision;
- **Lithuania's** AI training platform initiative for public sector employees, with staged training and materials covering practical use, privacy, ethics and EU AI Act-related topics;
- the **United Kingdom's** One Big Thing "AI for All" initiative, intended to build confidence and responsible use of AI across the civil service.
- **Brazil's** AI training portal for public servants offers structured learning pathways tailored to five professional profiles (from frontline staff to senior leaders) covering applied AI, data governance, ethics and strategic decision-making.

Source: (University of Helsinki and MinnaLearn, n.d.[15]; Australian Public Service Academy, n.d.[16]; Korea Internet & Security Agency (KISA), n.d.[17]; UK Cabinet Office, 2025[18]; Australian Department of Finance, 2025[19]; Ministry of Information Technologies and Communications (MinTIC), 2025[20]; UNESCO, 2025[21]; Ministry of the Economy and Innovation, 2025[22])

Figure 4.4. Most OECD countries provide training on the practical and trustworthy use of AI, with potential to expand its application to more specific purposes

Percentage of OECD countries reporting training programmes to support AI skills, by topic, 2025



Note: Data not available for Germany, the United States. Data cover 1 January 2023 to 31 December 2024. Refer to Annex Table 4.A.2 for comprehensive OECD and Accession country data.
Source: OECD (2025), Survey on Digital Government 3.0.

StatLink https://stat.link/2e38fa

4.4.3. Most countries fund AI initiatives, but support for procurement lags

Financial resources are as essential as human capabilities for enabling AI adoption, but funding and financing mechanisms often receive limited attention in national strategies for AI in government. Despite this, most OECD countries take steps to resource government AI initiatives. According to the 2025 DGI, 32 of 36 OECD countries (89%) (all except Costa Rica, Hungary, Mexico, and Switzerland) and four of six accession candidate countries (67%) (all except Croatia and Romania) have some form of funding for the development or use of AI systems in government. Among OECD countries that report having funding mechanisms for AI, 15 of 32 countries (47%) have dedicated funding, while 17 of 32 (53%) rely on broader digital government funding streams.

Investments take various forms, including public-sector incubators, dedicated grants, and targeted support programmes to develop or test AI systems (Box 4.4). Despite different institutional designs, all three of these mechanisms channel funding toward practical AI experimentation and delivery, not just strategy or research. They are designed to reduce barriers to early adoption, lower the risks of experimentation for ministries and agencies, accelerate real-world testing, and provide structured support for scaling. This signals a broader trend: governments see AI funding as a way to convert institutional interest into tangible implementation, especially given the constraints of traditional budgeting cycles.

However, funding alone is insufficient if governments lack support for procuring AI technologies. Only 21 of 36 OECD countries (58%) and no accession candidate country provide central government support for procuring AI goods and services. Given the complexities of AI systems and the inherent challenges within public procurement processes, these modest levels of support warrant further action. Without strong procurement guidance, innovation procurement procedures and shared mechanisms such as standard criteria, frameworks and model contract clauses, governments risk vendor lock-in, unclear accountability, and limited transparency into system behaviour and performance. Contracts may also fail to adequately address risk, licensing, data and intellectual property rights,

auditability, monitoring, or model lifecycle management and exit arrangements.

Governments therefore need strong procurement capabilities if they want to use AI well. Buying AI systems is not just about choosing a vendor. It requires enough technical understanding to define what the system should do, set clear safeguards, and check whether suppliers are handling data responsibly, building reliable models, keeping systems secure, and delivering results over time. These capabilities are essential if governments want to move beyond small pilots and use AI in ways that are safe, efficient, and responsive to citizen needs.

As explored in Chapter 3, governments' ability to engage with non-governmental actors through public procurement, public-private partnerships or collaborative innovation models is an important enabler of broader digital transformation efforts. AI further magnifies this need: governments must be able to partner strategically, outsource selectively, and retain sufficient internal capability to govern technology responsibly.

Box 4.4. Funding and procurement support for AI in government

France

France's ALLianNCE incubator supports government actors in AI adoption with a community of learning, guidance, and funding for talent acquisition averaging EUR 100 000 per project. This approach enables agencies to bring in specialised expertise to design and deploy AI systems. The impact of this talent-oriented funding model is reflected in the eight AI products incubated in 2024. Co-financed by the initiatives, the resulting projects addressed opportunities such as automated transcription and French-language LLM calibration, and supported several agencies in the central government.

Denmark

Denmark created two technology investment funds between 2020 and 2024 to encourage integration of AI systems into the public sector. From municipal to central authorities, multiple levels of government were eligible to receive financing. The *Signaturprojekterne* fund encouraged development of AI focused on building concrete public sector experience with the new technology. The *Tilskudspulje for nye teknologier* fund supported new technologies that might address societal challenges. The former supported development of 40 AI projects with approximately EUR 26 million in total funding, and the latter has seen several AI projects awarded.

Türkiye

Türkiye's Scientific and Technological Research Council supports the procurement and co-development of AI through funding consortia. Its efforts bring together public institutions as end-users, and tech firms or research organisations as developers, enabling AI systems to be tailored through structured R&D collaborations. The programme prioritises five domains: (1) smart manufacturing systems; (2) smart agriculture and food; (3) financial technologies; (4) climate change and sustainability; and (5) smart education technologies. The programme is a central mechanism for strengthening Türkiye's AI ecosystem with 41 projects with approximately EUR 4 million over three years.

Source: (Government of France, 2024[23]; Danish Agency for Digital Government, n.d.[24]; Danish Agency for Digital Government, n.d.[25]; Government of the Republic of Türkiye, n.d.[26]; AI in the State, n.d.[27])

4.4.4. Cloud computing capacities for AI are solidifying but other forms of digital infrastructure are less developed

Digital infrastructure is critical for AI development in government, acting as the connective tissue that enables systems to scale, interact and operate reliably (Chapter 2). Figure 4.5 and Annex Table 4.A.3 present AI-relevant infrastructure in OECD Members and accession candidate countries. The 2025 DGI findings show OECD countries making progress, particularly in cloud capabilities, but other components remain less mature.

Most OECD countries (26 of 36 countries, or 72%) have cloud computing capacity to support AI. This is an encouraging sign of progress toward scalable, flexible and resilient infrastructure, especially given the compute intensity of many modern AI systems. Depending on the arrangement, cloud environments allow governments to access elastic capacity, advanced tools, and managed services without the long lead times associated with on-premise infrastructure.

However, only 13 of 36 OECD national governments (36%) report using hardware accelerators such as Graphics Processing Units (GPUs). This likely reflects a mix of factors: greater reliance on cloud or managed AI services, where accelerator capacity is abstracted away from public organisations; the fact that many AI use cases do not require dedicated accelerators; and barriers to acquiring and operating specialised hardware, such as long procurement lead times and supply-chain bottlenecks for advanced accelerators, skills gaps and the operational requirements of hosting them securely.

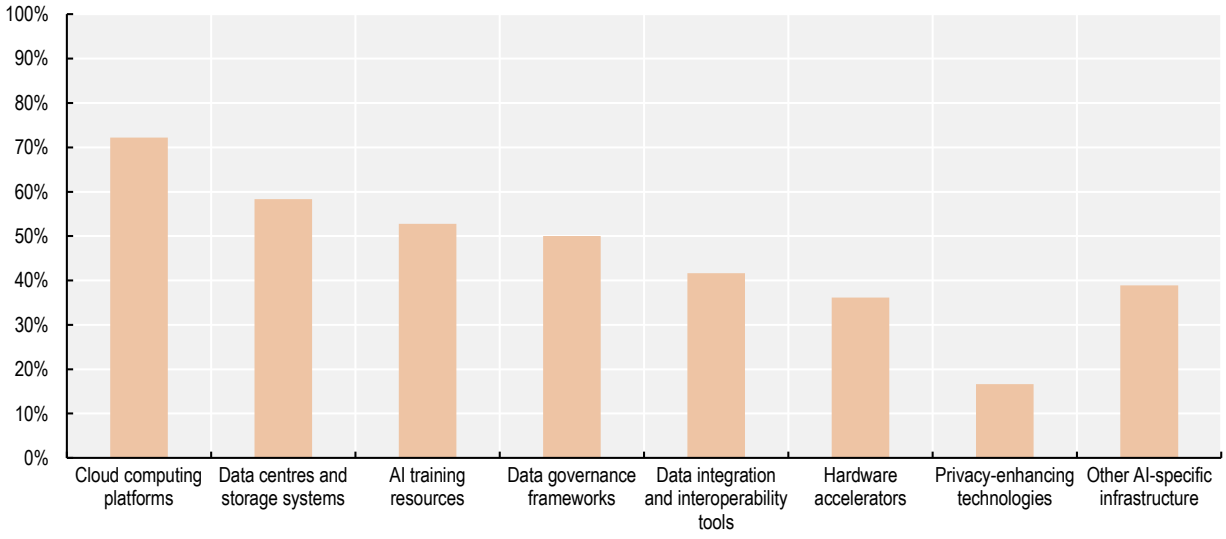
More concerning is the low maturity of data governance frameworks and the unavailability of high-quality data for AI training. The gaps echo findings from Chapter 2: many governments continue to face fragmented data ecosystems, weak quality management, and limited reuse of authoritative datasets. Without strong data foundations, AI models cannot perform reliably and increase risks related to skewed data, poor accuracy, and unreliable outputs.

Adoption of privacy-enhancing technologies (PETs) is also low. While this is unsurprising given their relative novelty and specialised implementation demands, it represents an area for future investment. PETs can help operationalise privacy-by-design principles, support data minimisation, enable responsible data sharing, and facilitate cross-border collaboration for training and evaluation while safeguarding privacy, confidentiality and intellectual property rights (OECD, 2025[2]; 2024[28]; 2023[29]; OECD, 2025[30]).[3] As AI systems handle more sensitive information, and as interoperability expands across organisations and borders, PETs will become increasingly important for maintaining public trust and ensuring compliance with legal and policy requirements.

Box 4.5 presents some promising practices identified during the 2025 DGI analysis. They show that AI-ready governments do not rely on a single infrastructure solution, but build layered, interoperable, and resilient approaches that combine cloud capacity, compute, governance, data accessibility, security and shared AI services. These examples indicate a clear shift from siloed infrastructure to shared, government-wide platforms, and a combination of commercial and sovereign approaches recognising that no single infrastructure model meets all needs.

Figure 4.5. Progress in cloud computing for AI outpaces other digital infrastructure components in OECD countries

Percentage of OECD countries having selected digital infrastructures and components to support AI integration, 2025



Note: Data not available for Germany and the United States. Data cover 1 January 2023 to 31 December 2024. Refer to Annex Table 4.A.3 for comprehensive OECD and Accession country data.
Source: OECD (2025), Survey on Digital Government 3.0.

StatLink https://stat.link/af8umo

Box 4.5. Governments advancing digital infrastructure capacities for AI

Governments around the world undertook a range of investments to strengthen their AI-enabling digital infrastructure. For example:

- **Cloud computing platforms. Belgium's** G-Cloud is a hybrid cloud, using services both offered by private companies in public cloud environments and those hosted in government data centres. The government manages the G-Cloud while the private sector is responsible for its development and operations.
- **Data centres and storage systems. Austria's** Federal Computing Centre operates data centres and analytical infrastructure that process millions of records per year.
- **AI training resources. Portugal** has over 2 000 standardised service factsheets available in open-dataset format, supporting consistent and accurate information, which have been used to train their citizen-facing ChatBot, a virtual assistant housed on the ePortugal Portal.
- **Hardware accelerators (e.g. GPUs).** In 2024, the Export and Investment Fund of **Denmark** (EIFO) funded the Danish Centre for AI Innovation (DCAI), a new company that partially owns and will operate Gefion, Denmark's first supercomputer. It is available to researchers from the public and private sectors.
- **Data governance frameworks. Brazil's** Data Maturity Model (MMD) is a tool for evaluating and improving data governance in public institutions. It is based on DAMA-DMBOK, a widely recognised international standard for data management, which adds credibility and structure.
- **Data integration and interoperability tools.** Ena is **Sweden's** national framework for digital infrastructure, led by the Agency for Digital Government (Digg). It supports data integration and

interoperability by providing shared digital components, such as secure data exchange, standardised interfaces and common frameworks, that enable public-sector organisations to collaborate efficiently.

- **PETs**. The **United Kingdom** Service Standard requires teams to follow secure-by-design approaches, including that they "collect, process and store data securely and in a way which respects users' privacy". The Office for National Statistics (ONS) publishes work on privacy-preserving synthetic data and discusses differential privacy to enable safer access to sensitive data. The government also explores privacy-preserving federated learning, where organisations train models locally and share model updates rather than raw data.
- **Self-deployed foundation models.** ALIA is **Spain's** publicly funded, open, public AI infrastructure, providing language models and related resources in Spanish and co-official languages (Catalan, Valencian, Basque and Galician), co-ordinated by the Barcelona Supercomputing Centre and intended for use by public administrations, researchers, universities and companies.

Countries such as **Japan** acted after 2024 to close gaps, while others took steps to bolster relatively strong positions. Several European Union Members enacted new legislation and policy in 2025 to comply with the EU Data Governance Act (DGA). While the DGA is not an infrastructure programme per se, it can strengthen foundations relevant to data infrastructure and interoperability by encouraging trusted data-sharing and reuse, including through secure processing arrangements. Use of PETs appears to be increasing slightly, with countries such as **France** and the **United Kingdom** conducting relevant efforts and **Israel** issuing guidance in 2025-2026.

Source: (Federal Public Service (FPS), Public Social Security Institutions (IPSS) and ICT organisations, n.d.[31]; Austrian Ministry of Finance (BMF), n.d.[32]; Republic Portuguesa, 2023[33]; Danish Centre for AI Innovation (DCAI), 2024[34]; Brazilian Secretariat of Digital Government, 2024[35]; Sweden Agency for Digital Government (DIGG), n.d.[36]; UK Government, n.d.[37]; Office for National Statistics (ONS) - Data Science Campus, 2023[38]; UK Department of Science, Innovation and Technology, 2023[39]; ALIA, n.d.[40]) (Israel Privacy Protection Authority, 2025[41]; LINC, 2025[42]; NHS Digital, n.d.[43]; UK Department for Science, Innovation and Technology, 2026[44])

4.5. Guardrails are expanding but enforceable controls remain limited

Guardrails help ensure the trustworthy development, deployment and use of AI in government. They are essential for managing risks associated with AI and deploying AI according to legal boundaries and public values. Guardrails also support digital resilience by helping governments detect problems early, adjust implementation pathways and maintain public trust, all necessary for scaling AI safely.

However, they must be seen together with the enablers discussed earlier in the chapter. Strong guardrails without strong enablers can fuel risk-aversion and stall innovation. Likewise, strong enablers without adequate guardrails increase risk exposure. A balanced, proportionate approach, tailoring controls to the risk level of each use case, is critical to avoid both misuse and inaction (OECD, 2025[2]). Governments should determine which guardrails fit their operations and contexts, and apply them to AI uses in a manner commensurate and proportionate to their level of potential risk.

4.5.1. All OECD countries have high-level guardrails to ensure trustworthy AI

Across the OECD area, governments leverage a mix of formal requirements (e.g. binding regulations and mandatory standards) and soft policy levers (e.g. guidelines, standards, ethical principles) to ensure the trustworthy management and use of AI in government, in alignment with the OECD AI Principles. All OECD countries have at least one form of guardrail, 25 of 36 countries (69%) use formal requirements, 30 of 36 (83%) use soft approaches, and 19 of 36 (53%) use both. Among accession candidate countries, Peru uses both formal and soft approaches, while Argentina and Brazil rely primarily on soft mechanisms.

Within OECD countries, many guardrails come from broader digital and data-protection frameworks. For example, aspects of the EU General Data Protection

Regulation (GDPR) operationalise transparency, fairness and accountability obligations relevant to AI.

The EU AI Act is also relevant. While most of its provisions were not yet applicable during the 2025 DGI analysis window, nor even as of early 2026, several EU countries took proactive steps to achieve compliance in advance. In addition to these regional obligations, countries have national principles and practices tailored to their contexts. For example, Greece released AI Working Guidelines as part of its national AI Strategy (Government of Greece, 2024[45]). Peru adopted dedicated AI legislation, demonstrating early regulatory action outside the EU. Countries outside the EU often use government-wide directives to adapt the OECD AI Principles to national priorities (Government of Peru, 2023[46]).

4.5.2. Implementation of guardrails remains limited, especially for enforceable controls

Despite continued progress at strategic and regulatory levels, implementation of guardrails remains uneven and often challenging. The 2025 DGI reveals that concrete, enforceable controls are far less widespread. Among OECD countries, 14 of 36 countries (39%) require ex-ante (pre-deployment) risk-assessments for AI systems, 12 of 36 (33%) have internal review committees overseeing AI use, and 11 of 36 (31%) conduct post-deployment audits (Figure 4.6). Box 4.6 provides examples of these initiatives.

The prevalence of ex-ante tools might reflect that they can be embedded in existing approval and procurement workflows, creating standard checkpoints, templates and sign-offs before deployment. However, ex-ante checks can be insufficient on their own. Guardrails also require clear, risk-based oversight mandates, continuous monitoring and well-designed audits that avoid creating false confidence or "audit washing" (OECD, 2025[2]). Review committees can add coherence and escalation routes across projects, but their impact depends on whether they can make or enforce decisions rather than operating as purely advisory bodies, and on having sufficient influence over government decision making. Ex-post auditing and ongoing monitoring are essential to detect drift (such as changes in data, behaviour or performance over time), and emerging issues and compliance gaps once systems are in use.

Many governments indicate that such measures are under development, including as part of their EU AI Act compliance efforts. Others have high-level principles and guidance in place, but lack concrete procedural requirements or operational processes to make these actionable. This gap reflects a broader pattern throughout this report: while governments make progress developing strong strategies and high-level approaches to digital transformation, translating them into routine practice through enforceable, risk-proportionate mechanisms remains a significant challenge.

Without risk-based assessments, audit structures, accountability frameworks and formal decision paths for high-risk uses, guardrails might remain symbolic rather than operational. This weakens governments' ability to detect emerging risks early, ensure adequate usage and accountability, govern vendor-provided AI systems, uphold public trust and scale AI across institutions.

Box 4.6. OECD countries expanding guardrails for trustworthy AI in government

Many governments have concrete initiatives to facilitate the development and use of trustworthy AI systems in the public sector. Examples include:

- ***Ex ante* risk assessments. Canada's** Algorithmic Impact Assessment (AIA) is a mandatory risk-assessment being completed (with results openly published) by federal departments and agencies before deploying an automated decision-system. It verifies compliance with Canada's Directive on Automated Decision Making and any other binding mandates. Another example, **Australia's** AI Assurance Framework was piloted with 21 volunteer agencies from September to November 2024, testing a draft ex-ante AI impact-assessment tool to help teams evaluate AI use cases against Australia's AI Ethics Principles, including benefits, reliability and risks.

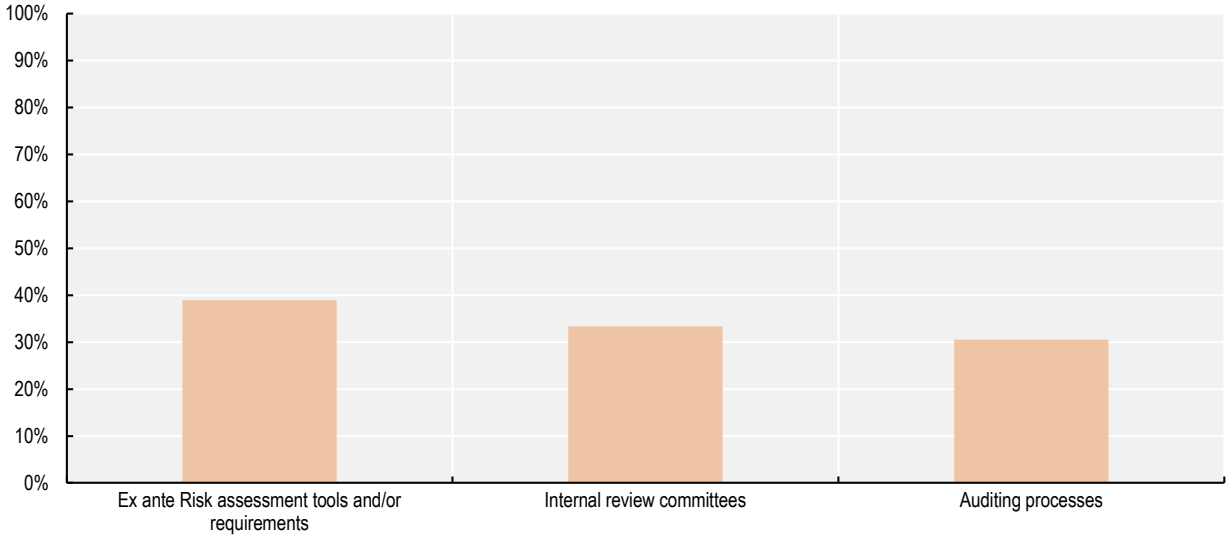
- **Internal review committees**. **Luxembourg's** AI4Gov interministerial committee comprises representatives from the Ministry of Digitalisation, the Media and Communications Service (SMC), the Information and Press Service (SIP), and various technical experts. The committee aims to encourage government agencies to use AI and data science responsibly, to transform their actions and tasks, and to provide them with the necessary support.
- ***Ex post* auditing processes.** As part of its National AI Strategy, **Türkiye** aims to establish an auditing mechanism to ensure the development of trustworthy and responsible AI. The country began a national risk-management certification programme.

Several governments took further action after 2024. **Japan's** Council of Chief AI Officers was established in 2025 and facilitates risk-governance workflows, and the **United Kingdom** made updates to its Algorithmic Transparency Reporting Standard and refreshed its Data and AI Ethics Framework to include a self-assessment tool to identify impacts. Others sought to strengthen existing efforts. For instance, in late 2025, following its aforementioned pilot, **Australia** issued an updated policy for responsible AI in government, requiring agencies to complete the impact-assessment for certain AI use cases and establishing expectations for ongoing monitoring of AI use.

Source: (Government of Canada, 2026[47]; Türkiye Digital Transformation Office and Ministry of Industry and Technology, 2021[48]; Turkish Standards Institution (TSE), 2026[49]; Government of Luxembourg - Ministry of Digitalization, n.d.[50]; TSE Global, n.d.[51]; Digital Agency of Japan, 2025[52]; UK Government Digital Service, n.d.[53])

Figure 4.6. Most OECD countries have yet to translate AI governance frameworks into enforceable controls

Percentage of OECD countries reporting controls to ensure trustworthy AI, by type, 2025



Note: Data not available for Germany and the United States. Data cover 1 January 2023 to 31 December 2024. Refer to Annex Table 4.A.4.for comprehensive OECD and Accession country data.
Source: OECD (2025), Survey on Digital Government 3.0.

StatLink https://stat.link/s6hdcz

4.5.3. Most countries commit to algorithmic transparency but few have formal standards or open algorithm registers

Transparency around how government uses algorithmic AI systems and their outputs is important for building public trust (OECD, 2025[2]). Commitment to algorithmic transparency is growing across OECD countries, but mechanisms to operationalise it remain limited. In 2025, beyond their adherence to the OECD AI Principles, 21 of 36 OECD countries (58%) (up from 17 of 33 countries, or 52%, in 2023) and two of six accession candidate countries (33%) acknowledged the importance of algorithmic transparency as part of responsible AI use.

However, committing to transparency in principle is not the same as enabling it in practice. Only a minority of countries have instruments that make algorithmic transparency actionable. Two mechanisms matter most: (1) transparency standards and laws that require organisations to document how and why they use algorithmic tools; (2) open algorithm registers that publicly list algorithmic tools in use across governments. Across OECD countries, 11 of 36 countries (31%) have a law or other standard and 6 of 36 (17%) have an open register. Only six OECD countries have both (Canada, Estonia, France, Korea, the Netherlands, and the United Kingdom), while 25 of 36 countries (69%) have neither, meaning there is no formal structure to ensure transparency beyond high-level commitments. Box 4.7 presents examples of these mechanisms.

Among OECD accession candidate countries, only Peru has formal requirements in the form of a law to mandate the sharing of algorithm source code with political organisations, but only in the context of digital voting systems, making it narrow in scope (Congress of the Republic of Peru, 2025[54]).

Progress has been modest compared with 2023 DGI results, with the share of countries reporting either a transparency standard or algorithm register increasing from 7 of 33 countries (21%) to 11 of 36 (31%). Still, adoption remains low, suggesting that algorithmic transparency is a relatively weak area of AI governance across the OECD area. The gap between commitment and implementation again underscores the recurring theme of this report: governments recognise the importance of trustworthy AI but practical mechanisms for transparency, accountability and oversight remain underdeveloped. Strengthening algorithmic transparency will be essential to build public trust and support responsible AI scaling across the public sector.

Box 4.7. How governments operationalise algorithmic transparency

Several governments take tangible steps to enhance transparency around the use of algorithmic systems in public services. Examples include:

- **Laws and guidelines.** The **European Union's** AI Act introduces extensive transparency obligations, with relevant requirements not yet applicable, and pending technical and governance requirements still not applicable during the 2025 DGI analysis window. Some EU Members took earlier action to mandate transparency, such as **France's** *Code des relations entre le public et l'administration*, which requires the disclosure and explanation of algorithm-driven government decisions to impacted individuals. Outside the EU, **Australia's** policy for the Responsible Use of AI in government requires transparency-driven actions in the adoption of AI from each agency, such as the publishing of a transparency statement explaining its overall use of AI and ongoing monitoring of systems for unintended impacts.
- **Algorithm registers**. The government Algorithm Register in the **Netherlands** aggregates over 1 300 algorithms and provides details for each, such as its purpose and points of contact. The **United Kingdom's** Algorithmic Transparency Recording Standard (ATRS) mandates public-sector organisations to disclose details about their use of algorithmic methods in decision-making, including who is responsible for the algorithm, its description and a breakdown of potential risks and mitigation activities. Currently, the ATRS lists 131 records.

Source: (OECD, 2023[55]; Government of France, n.d.[56]; Digital Transformation Agency of Australia, n.d.[57]; UK Government, n.d.[58]; Dutch Government, n.d.[59])

4.5.4. Limited internal repositories of AI use cases constrain transparency and governance

An underlying challenge for trustworthy and scalable AI adoption is that most governments do not have a central repository of AI use cases. Repositories record critical information about AI systems, such as their objectives, implementation stages, outcomes, responsible institutions, timelines and underlying technologies. This information is important for enabling oversight, identifying duplication, monitoring risks, and building organisational learning across the administration. Figure 4.7 shows which countries have algorithmic transparency standards, central use case repositories, and open algorithm registers.

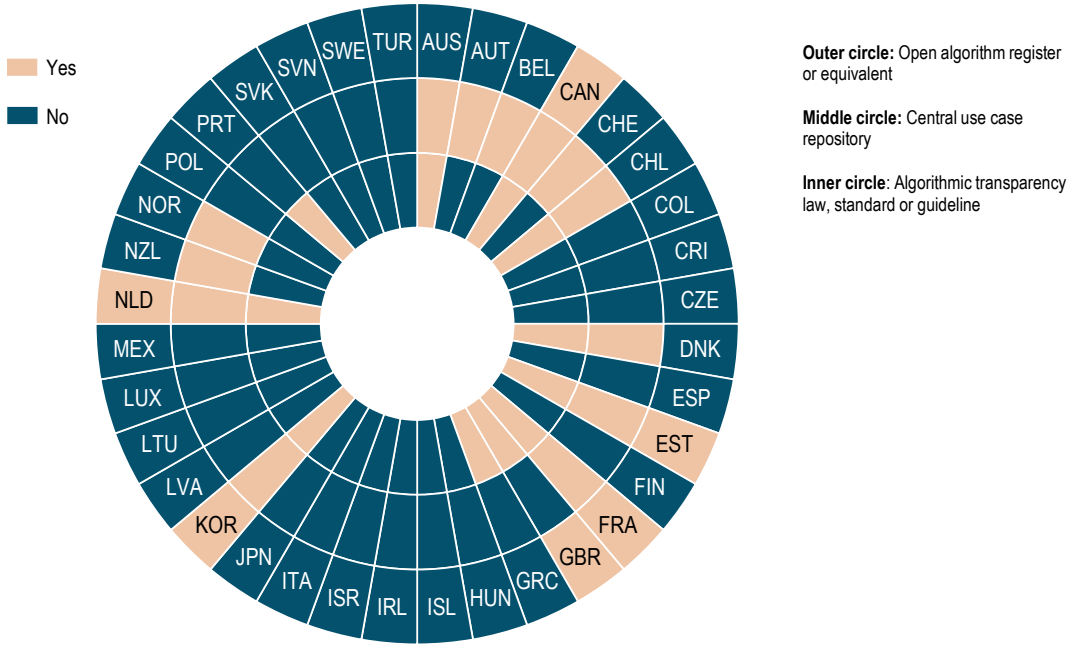
Only three OECD countries have mandatory AI use-case repositories (Australia, Canada and Estonia), while another 10 countries maintain repositories with optional contributions from agencies. No accession candidate country has such a repository. Estonia's approach illustrates the value of a centralised repository. It documents almost 170 public-sector AI use cases across nearly 60 institutions (Government of Estonia, 2026[60]). Each record includes a description of the use case, the implementing institution, partners involved, the type of AI systems, area of impact and status details.

Several countries indicate either plans to create repositories or that they maintain partial lists tied to specific initiatives, but these do not provide a government-wide view. Such repositories can serve as a stepping stone towards an open register, and all countries with an open register have a central repository. The optional nature of most of these repositories raises questions about the completeness of the open registers.

Several countries acted after 2024 to close gaps. For instance, Colombia (Government of Colombia, 2025[61]; Government of Colombia, 2026[62]; Inspector General of Colombia and Ombudsman of Colombia, 2025[63]), Ireland (Government of Ireland, 2025[64]) and Sweden (IMY, 2025[65]) issued directives or guidelines to promote transparency for the public to understand how and why government uses AI. Japan put in place requirements for each ministry to compile an ongoing overview list of AI systems and report it regularly to the Digital Agency (Digital Agency of Japan, 2025[52]).

Figure 4.7. Transparency mechanisms for AI in government remain underdeveloped in OECD countries

Countries reporting open AI registers, use case repositories and transparency standards, 2025



Note: Data not available for Germany, the United States, Indonesia or Thailand. All participating accession candidate countries responded "No" to all answer options. Data cover 1 January 2023 to 31 December 2024.
Source: OECD (2025), Survey on Digital Government 3.0.

StatLink https://stat.link/y8lndq

4.5.5. Most countries have oversight or advisory bodies, but activity focuses on guidance rather than enforcement

Oversight and advisory bodies are increasingly common in government AI governance ecosystems, but their functions remain oriented toward guidance and monitoring rather than hands-on auditing or enforcement. In 2025, 30 of 36 OECD countries (83%) (and three of six accession candidate countries, or 50%) had either a regulatory oversight body or an ethical advisory body dedicated to AI. This represents an improvement since 2023, when 24 of 33 OECD countries (73%) had one of these bodies. Of OECD countries, 15 of 36 (42%) have both, as does Peru among accession candidate countries.

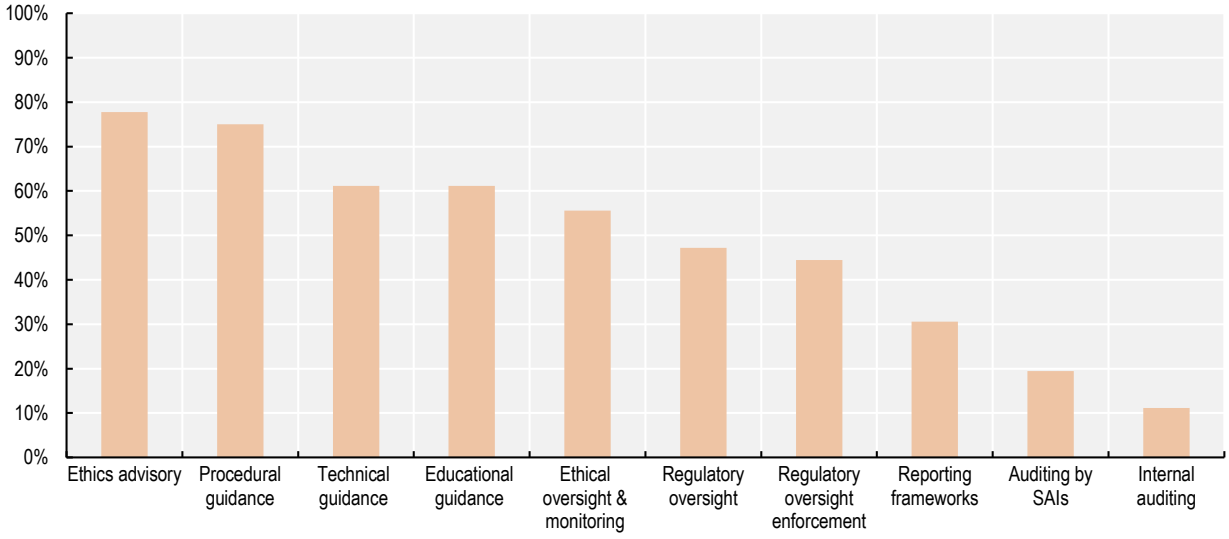
Among countries with such bodies, dominant activities include: developing procedural guidance such as guidelines or codes of conduct (27 of 30 countries, or 90%); producing technical or educational guidance (22 of 30, or 73%); and conducting ethical oversight and monitoring, such as through AI Councils or data-ethics bodies (20 of 30, or 67%).

More hands-on activities remain less common, including auditing, regulatory oversight and enforcement, or developing or executing reporting frameworks such as algorithmic impact-assessments. As one example of such of a regulatory oversight body, Portugal established a Specialised Monitoring Committee that serves as its national competent authority under the EU AI Act and ensures best practices in the development of Large Language Models (LLMs) and compliance with ethical rules.[4] In contrast, an ethics advisory body makes non-binding recommendations, such as Japan's Review Council for the Principles of Human-Centric AI Society, responsible for reviewing guidelines and codes of conduct in line with the ongoing societal impacts of AI (Cabinet Office of Japan, 2026[66]).

Several countries acted after 2024 to close gaps. For instance, Colombia (Consejo Nacional de Política Económica y Social, 2025[67]) and Japan (Digital Agency of Japan, 2025[52]; Digital Agency of Japan, 2025[68]) instituted advisory bodies comprised of internal and external experts, while Japan introduced an internal oversight body and oversight architecture.

Figure 4.8. Most OECD countries are providing ethical, procedural and technical guidance for AI in the public sector

Percentage of OECD countries with public bodies in charge of providing oversight or ethical advice for AI in the public sector, by type of oversight or advice provided, 2025



Note: 2025 data not available for Germany and the United States. Refer to Annex Table 4.A.5 for comprehensive OECD and Accession country data.
Source: OECD (2025), Survey on Digital Government 3.0.

StatLink https://stat.link/l2bj6d

4.5.6. Guardrails for GenAI are less robust compared to other AI systems

Dedicated guardrails for generative AI (GenAI) remain comparatively underdeveloped across OECD countries, reflecting its more recent adoption in public administrations relative to other forms of AI. While governments have used AI for many years, GenAI has only been a focus for the last three to four years (Berryhill et al., 2019[69]; OECD, 2025[2]). Some research suggests that the pace of GenAI adoption outpaces the evolution of guardrails and training needed to use these tools responsibly (Giesecke, 2024[70]; Bright et al., 2024[71]).

GenAI in government differs from other types of AI and machine-learning (ML) systems. ML systems such as risk-scoring tools or resource-allocation models are typically bespoke, domain-specific and procured or developed through formal institutional processes, whereas GenAI is often built on general-purpose models accessible through chat interfaces (OECD, 2026[72]; 2025[2]). Public servants often have access to personal accounts for common GenAI systems and may leverage them in their functions, either with organisational approval or without as so-called "shadow AI". Illustrating this pattern beyond government, while only 40% of companies report purchasing official LLM subscriptions, employees in 90% of surveyed firms report using personal AI tools for work (MIT NANDA, 2025[73]). In addition, GenAI's ability to generate convincing but potentially inaccurate outputs creates distinctive integrity risks. Unlike many earlier AI systems that supported back-office decisions in the background, GenAI is often used to draft or edit citizen-facing content, policy documents and internal communications, which can be difficult to distinguish from human-authored material. This blurring of boundaries between human and machine-authored content raises questions about authenticity, accountability and trust, and underlines the need for appropriate, risk-based guardrails

In addition to (or as part of) the broader controls and transparency mechanisms discussed above, governments have guardrails specific to GenAI. To help ensure GenAI systems are used in a trustworthy manner, most OECD countries have ethical guidelines for the use of GenAI tools (27 of 36 countries, or 75%) and training programmes on the responsible use of such systems (21 of 36, or 58%). However, fewer have transparency measures in place, such as disclosure requirements for AI-generated content (13 of 36, or 36%); data standards or protocols to ensure security and privacy of data used or inserted into GenAI tools (13 of 36, or 36%); independent oversight by external bodies or experts (12 of 36, or 33%), or accountability frameworks to address potential misuse or errors (7 of 36, or 19%). Among accession candidate countries, two of six countries (33%) have training programmes and ethical guidelines, with countries lacking other guardrails (Box 4.8).

Box 4.8. Guardrails for generative AI in government

Examples of initiatives include:

- **Ethical guidelines. Chile's** 2021 National AI Policy was updated in 2023 following the accelerated advance of generative AI. Its reformulated third axis, Governance and Ethics, was published alongside relevant guidelines. **Brazil's** Generative AI Primer in the Public Service guides public servants on the trustworthy use of GenAI tools and is updated as rules and technology evolve.
- **Training programmes. Australia's** course on AI in Government Fundamentals includes a focus on when it is appropriate for public servants to use GenAI.
- **Transparency/disclosure requirements.** The **Netherlands'** Guide to the Responsible Use of Generative AI links use to compliance with domestic law, with requirements consolidated in the Algorithm Framework (including the Open Government Act). It also recommends maintaining documentation on when, why and by whom GenAI is used, publishing this via the Algorithm Register, supported by tools such as impact assessments and publication standards.
- **Data standards. New Zealand's** Responsible AI Guidance for the Public Service: GenAI clarifies data-handling and privacy controls for using GenAI, including assessing the sensitivity of prompts and any data

shared with tools, and using Privacy Impact Assessments (PIAs) to check whether the proposed use aligns with privacy obligations and agency information-management requirements.

- **Accountability frameworks. Ireland's** Interim Guidelines for Use of AI in the Public Service place heavy emphasis on GenAI. They highlight the importance of human judgement, oversight and review.
- **Independent oversight.** Under the **EU** AI Act, Members must designate a national competent authority to supervise and enforce the Act, including where public bodies use AI. In **Spain**, the Agency for the Supervision of AI (AESIA) supports this by publishing practical guidance to help organisations assess obligations under the AI Act, including for GenAI deployments and where systems might fall into higher-risk categories.

Source: (Chile's Ministry of Science, Technology, Knowledge and Innovation, 2024[74]; Chile's Ministry of Science, Technology, Knowledge and Innovation, 2023[75]; Secretariat of Digital Government of Brazil, 2025[76]; Government of the Netherlands, 2026[77]; New Zealand Digital Government, 2025[78]; New Zealand Government, n.d.[79]; Department of Public Expenditure NDP Delivery and Reform, 2024[80]; Spanish Agency for the Supervision of Artificial Intelligence (AESIA), n.d.[81]; Ministry of the Interior and Kingdom Relations, 2025[82])

4.5.7. Challenges in measuring the impact of AI limit decision-making and contribute to a proliferation of pilots with little potential to scale

A major barrier to strategic AI adoption in government is the widespread lack of processes to measure the financial and non-financial impact of government AI investments. The OECD (2025[2]) finds that inability to measure the value, outcomes or cost of AI systems is a core constraint on governments' ability to make informed investment decisions. Without robust evidence on return-on-investment (ROI) or service impact, governments struggle to determine whether pilots are successful, justify scale-up or decide how to allocate limited resources.

This challenge is not unique to governments, as research on the private sector finds that "the main barriers to AI investment and adoption are a lack of understanding of AI benefits and the inability to measure them" (Ramos and Kandaswamy, 2023[83]). In contrast, companies with high levels of AI maturity succeed in delivering value because they design and implement structured metrics that quantify the benefits of their AI projects (Gartner, 2025[84]). Governments face similar difficulties, but with stronger accountability pressures and fewer organisational incentives to take risks.

Across OECD countries, impact measurement remains one of the least developed components of AI governance. Chapter 3 shows that almost half of OECD countries monitor broader digital investments, but only one in four evaluate their impact and realised benefits. These challenges also exist specific to AI investments: most governments do not have the processes for holistic measurement of potential or realised results of AI projects, such as efficiency of spend or quality of services (Figure 4.9). Only 10 of 36 OECD countries (28%) report conducting any financial or non-financial impact measurement studies of AI use cases in government, whether prospective or retrospective. Fewer still report measuring the impact of AI use across a government sector (4 of 36 countries, or 11%), or across government or how its use of AI affects society (6 of 36 each, or 17%).

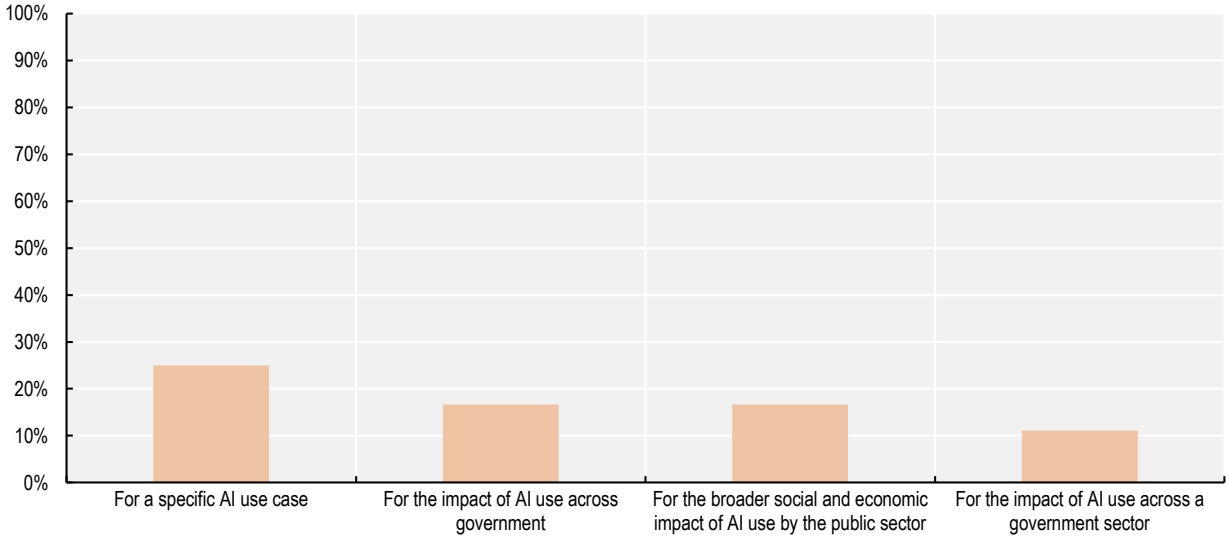
Some governments initiated efforts to close these gaps. Australia (Australian Government, 2024[85]) and the United Kingdom (Government of the United Kingdom, 2025[86]) assess the impact of government-wide Microsoft Copilot trials, generating early insights into productivity and user experience. The United Kingdom also issued Guidance on the Impact Evaluation of AI Interventions in 2024 (updated July 2025), with tailored advice for applying the Treasury ministry's Magenta Book to AI initiatives and helping teams understand whether, to what extent, how and why an AI intervention resulted in its intended impacts.

However, a mismatch persists between decision-making and evidence. While only 28% of OECD countries report conducting an impact assessment on any AI use case, 50% report making decisions for adopting AI based on evidence of potential efficiency or cost savings. This discrepancy raises questions about exactly what evidence governments rely on, whether it is robust and comparable, and whether AI adoption is being guided more by expectations and pressure than by demonstrated value.

Recognising the need to address these challenges, the OECD is working on a practical guide to measuring AI impact in government to help policymakers and AI teams gauge impact at the project level and use the insights for decisions in organisations and across government portfolios (OECD, forthcoming[87]).

Figure 4.9. Few OECD countries measure the impact of AI use in government

Percentage of OECD countries reporting measurement of the financial or non-financial impact of AI in government, by type, 2025



Note: Data not available for Germany, the United States, Indonesia or Thailand. Data cover 1 January 2023 to 31 December 2024. Refer to Annex Table 4.A.6 for comprehensive OECD and Accession country data.
Source: OECD (2025), Survey on Digital Government 3.0.

StatLink https://stat.link/o1dqfu

4.6. Engagement around strategies is strong but sustained, user and cross-border involvement remain limited

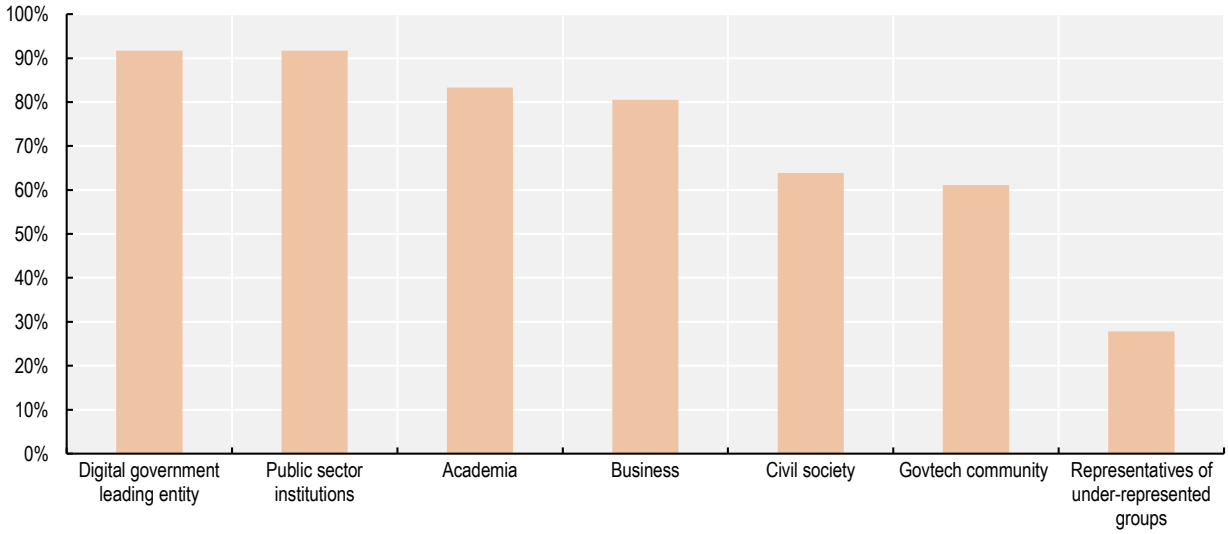
Engaging stakeholders – including the public – is essential for building trust, legitimacy and accountability around how governments use AI. Public engagement helps ensure that AI systems reflect societal needs, reduce risks of exclusion, and support user-centred design (OECD, 2024[88]). Rich engagement also lays the foundation for trustworthy and resilient AI governance, as communities understand how AI is used and have channels to shape its development.

4.6.1. Governments involve a range of stakeholders in their AI in government strategy development

One example of governments' engagement around AI can be seen in the development of their national AI strategies. The 33 OECD countries with a strategy for AI in government were highly collaborative in developing these strategies. Among them, 30 of 33 countries (91%) engaged with academia, 29 of 33 (88%) with industry (large and/or established firms), 23 of 33 (70%) with civil society, and 22 of 33 (67%) with the GovTech community (start-ups and other SMEs) (Figure 4.10). The only potentially weak area was engagement targeting under-represented groups such as young people, women or indigenous communities (9 of 33, or 27%). In addition, 21 of 33 countries (64%) held open public consultations while developing their strategy, around the same as the 66% recorded in 2023. Australia, Chile, Estonia, Iceland, Ireland, New Zealand and Norway are noteworthy in that they engaged all five categories of stakeholders and held a public consultation. Among the two OECD accession candidate countries with strategies, Brazil held a public consultation and engaged with all categories except under-represented groups, while Argentina engaged with business, academia and the GovTech community.

Figure 4.10. Stakeholder engagement in AI in government strategies is strong overall, yet uneven across groups

Percentage of OECD countries indicating stakeholder involvement in the development of AI in government strategy, by stakeholder, 2025



Note: In addition to external engagement, all OECD Members except Türkiye, and all accession candidate countries report internal collaboration among public-sector organisations in developing the strategy. Data not available for Germany, the United States, Indonesia or Thailand. Refer to Annex Table 4.A.7. for comprehensive OECD and Accession country data.
Source: OECD (2025), Survey on Digital Government 3.0.

StatLink https://stat.link/aiqgpe

4.6.2. Governments engage beyond national strategies but ongoing user engagement and cross-border collaboration remain limited

Governments' engagement around AI extends beyond strategy development, with many countries involving internal and external stakeholders in shaping public-sector AI policies, use cases and implementation approaches. These more continuous forms of engagement are important because they occur throughout the lifecycle of an AI initiative, not only during periodic strategy updates.

OECD countries demonstrate strong engagement with public sector organisations (31 of 36 countries, or 86%) and civil servants (26 of 36, or 72%). For example, France's social dialogues with central government unions and staff representatives helped to shape commitments for how AI would be introduced in the civil service (Ministry of Transformation and Civil Service, 2024[89]). This is important as they are at the frontline of public-service delivery and their responsibilities are directly impacted by the introduction of AI technologies. Governments also show substantial engagement with broader ecosystem actors, such as academia, industry and civil society (23 of 36, or 64%).

Some countries have more innovative forms of engagement. In 2024, the Belgian Presidency of the Council of the EU convened a representative group of 60 Belgians to collect citizens' views on AI within the bloc (beEU, 2024[90]). The Belgian government's AI4Belgium initiative is another promising example of an ongoing, multi-stakeholder ecosystem that brings together a variety of actors to support adoption of AI across sectors and within government (BOSA, n.d.[91]; BOSA, n.d.[92]). A further example, France uses the government's Agora participation platform to gather large-scale citizen input on national AI priorities, feeding into the work of the country's AI Commission and its recommendations to public authorities.[5]

However, there appear to be gaps in two key areas: (1) engaging with service users and (2) cross-border collaboration. Only 16 of 36 OECD countries (42%)

engage service users, even though their feedback is crucial to ensure that AI-enabled services are usable and trusted. Only 13 of 36 countries (36%) engage cross-border actors beyond participation in international fora like the OECD.[6] Since date, models and risks are inherently transnational, stronger international co-ordination is needed for interoperability, regulatory alignment and shared learning.

Potential easy opportunities to engage service users are by establishing citizen-complaint mechanisms or other means of gathering feedback. Only 8 of 36 OECD countries (22%) have these. For example, each public sector service provider in Estonia must offer citizens an E-service feedback form, which have now been operationalised as agencies adopt citizen-facing AI solutions.[7]

While engagement practices appear moderate to solid in most areas, data suggests a disconnect between engagement and action. Significant efforts go into listening to external perspectives, but only half of OECD countries and no accession candidate countries report basing their AI investment decisions on citizen needs or demands.

Meanwhile, engagement efforts continued beyond 2024, such as public consultations in 2025 by Canada (Government of Canada, 2025[93]), Israel (Israel National Digital Agency, 2025[94]) and the United Kingdom (Department for Science, Innovation & Technology, 2026[95]) about AI in government strategies, policies and tools.

Annex 4.A. Additional tables with country data

Annex Table 4.A.1. Use of AI in the public sector, by function

Report on the use of AI at central/federal government level to improve public sector functions

Country	Public sector internal processes		Public services design and delivery		Policymaking		Oversight and accountability in the PS	
	2023	2025	2023	2025	2023	2025	2023	2025
Australia	●	●	●	●	○	○	N/A	○
Austria	●	●	●	●	○	○	N/A	○
Belgium	○	●	○	●	○	○	N/A	○
Canada	●	●	●	●	○	○	N/A	○
Chile	●	●	●	●	●	●	N/A	●
Colombia	●	○	●	●	○	●	N/A	○
Costa Rica	○	○	○	○	○	○	N/A	●
Czechia	○	○	○	●	○	○	N/A	○
Denmark	●	●	●	●	○	○	N/A	●
Estonia	●	●	●	●	●	●	N/A	●
Finland	●	●	●	●	○	○	N/A	○
France	●	●	●	●	●	●	N/A	●
Greece	N/A	●	N/A	●	N/A	●	N/A	○
Hungary	●	○	●	●	○	○	N/A	○
Iceland	●	●	●	●	○	○	N/A	●
Ireland	○	●	●	●	○	○	N/A	○
Israel	○	○	○	○	○	○	N/A	○
Italy	●	●	○	○	●	○	N/A	○
Japan	○	●	○	○	○	○	N/A	○
Korea	●	●	●	●	●	●	N/A	●
Latvia	○	●	○	●	○	●	N/A	●
Lithuania	●	●	●	●	●	○	N/A	○
Luxembourg	●	●	○	●	●	●	N/A	●
Mexico	●	●	●	○	○	○	N/A	○
Netherlands	●	●	○	○	○	○	N/A	●
New Zealand	●	●	●	●	●	●	N/A	○
Norway	○	●	○	●	○	●	N/A	●
Poland	○	●	○	●	○	○	N/A	○
Portugal	○	●	●	●	○	●	N/A	○
Slovak Republic	N/A	●	N/A	○	N/A	○	N/A	○
Slovenia	●	●	●	○	○	○	N/A	○
Spain	●	●	●	●	●	●	N/A	○
Sweden	●	●	●	○	○	○	N/A	○
Switzerland	N/A	●	N/A	●	N/A	○	N/A	○
Türkiye	●	●	●	●	●	○	N/A	●
United Kingdom	●	●	●	●	●	●	N/A	○

Country	Public sector internal processes		Public services design and delivery		Policymaking		Oversight and accountability in the PS	
	2023	2025	2023	2025	2023	2025	2023	2025
OECD Total								
● Yes	23	31	22	27	11	13	0	12
○ No	10	5	11	9	22	23	0	24
No Information	3	0	3	0	3	0	36	0
Argentina	○	○	●	●	○	○	N/A	○
Brazil	●	●	●	●	○	○	N/A	●
Bulgaria	N/A	○	N/A	○	N/A	○	N/A	○
Croatia	○	○	○	○	○	○	N/A	○
Indonesia	N/A	○	N/A	●	N/A	○	N/A	N/A
Peru	○	●	●	○	○	○	N/A	○
Romania	○	○	○	○	○	○	N/A	○
Thailand	N/A	○	N/A	○	N/A	○	N/A	N/A

Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023. 2023 data not available for the "Oversight and accountability in the PS" category.
Source: OECD (2025), Survey on Digital Government 3.0.

Annex Table 4.A.2. Existence of training programmes supporting AI skills

Specific training programmes on skills required to support the development and use of AI in the public sector

Country	Practical use of AI tools	Ethical use of AI tools	Data privacy & security in AI systems	AI implementation for Service Design & Delivery	AI implementation for Policymaking	Other	None
Australia	●	●	○	○	○	○	○
Austria	●	●	○	○	○	○	○
Belgium	●	●	●	○	○	○	○
Canada	●	●	●	●	○	●	○
Chile	●	●	●	○	●	○	○
Colombia	○	○	○	○	○	●	○
Costa Rica	○	○	○	○	○	○	○
Czechia	●	○	○	○	○	●	○
Denmark	●	●	●	●	●	●	○
Estonia	●	●	●	●	●	○	○
Finland	○	○	○	○	○	○	○
France	●	●	●	●	○	○	○
Greece	●	●	●	○	○	○	○
Hungary	○	●	○	○	●	○	○
Iceland	○	○	○	○	○	○	●
Ireland	●	●	●	●	●	●	○
Israel	●	○	○	●	●	○	○
Italy	○	○	○	○	○	○	●
Japan	●	○	●	○	○	○	○
Korea	●	●	●	●	●	○	○

Country	Practical use of AI tools	Ethical use of AI tools	Data privacy & security in AI systems	AI implementation for Service Design & Delivery	AI implementation for Policymaking	Other	None
Latvia	●	●	●	○	●	○	○
Lithuania	●	○	○	○	○	○	○
Luxembourg	●	●	●	●	●	●	○
Mexico	●	○	○	○	○	○	○
Netherlands	●	●	●	○	○	○	○
New Zealand	○	○	○	○	○	●	○
Norway	●	●	●	●	●	●	○
Poland	●	●	●	○	○	○	○
Portugal	●	●	●	●	●	○	○
Slovak Republic	●	●	●	●	○	○	○
Slovenia	●	○	○	○	○	○	○
Spain	●	●	●	●	●	○	○
Sweden	○	○	○	○	○	●	○
Switzerland	●	●	●	○	○	●	○
Türkiye	●	○	○	○	○	●	○
United Kingdom	●	●	●	●	●	○	○
OECD Total							
● Yes	28	22	20	13	13	11	2
○ No	8	14	16	23	23	25	34
No Information							
Argentina	○	○	○	○	○	○	●
Brazil	●	●	○	○	○	●	○
Bulgaria	○	○	○	○	○	●	○
Croatia	○	○	○	○	○	○	●
Indonesia	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Peru	●	○	○	○	○	○	○
Romania	○	○	○	○	○	○	●
Thailand	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Note: Data not available for Germany, Indonesia, Thailand and the United States. Data cover 1 January 2023 to 31 December 2024.
Source: OECD (2025), Survey on Digital Government 3.0.

Annex Table 4.A.3. Digital infrastructure and components used to support AI integration

Availability of key components of digital infrastructure used to support the integration of AI in the public sector

Country	Cloud computing platforms	Data centres and storage systems, including for computational power	AI training resources (e.g. public datasets)	Hardware accelerators (e.g. GPUs)	Data governance frameworks	Data integration and interoperability tools	Privacy-enhancing technologies (PETs)	Other AI-specific infrastructure (usually self-deployed foundation models)
Australia	●	○	●	○	●	○	○	○
Austria	●	●	○	●	○	○	○	○
Belgium	●	●	●	○	●	●	○	○
Canada	●	●	○	○	●	○	○	○
Chile	○	○	○	○	●	○	○	○
Colombia	●	○	○	○	○	○	○	○

Country	Cloud computing platforms	Data centres and storage systems, including for computational power	AI training resources (e.g. public datasets)	Hardware accelerators (e.g. GPUs)	Data governance frameworks	Data integration and interoperability tools	Privacy-enhancing technologies (PETs)	Other AI-specific infrastructure (usually self-deployed foundation models)
Costa Rica	●	○	○	○	○	○	○	○
Czechia	○	●	●	○	●	●	●	○
Denmark	●	●	●	●	●	●	○	●
Estonia	●	●	●	●	●	●	●	●
Finland	●	○	○	○	○	○	○	○
France	●	●	●	●	●	●	●	●
Greece	●	●	●	○	○	○	○	●
Hungary	○	○	○	○	○	○	○	○
Iceland	●	●	○	●	●	●	○	●
Ireland	●	○	●	○	●	○	○	●
Israel	●	○	●	○	○	●	○	○
Italy	○	○	○	○	○	○	○	○
Japan	●	○	○	●	○	○	○	○
Korea	●	●	●	●	●	●	●	●
Latvia	●	●	○	●	○	○	○	●
Lithuania	○	●	●	○	●	●	○	○
Luxembourg	●	●	●	●	○	●	○	○
Mexico	○	●	●	○	○	○	○	●
Netherlands	○	●	○	○	○	○	○	●
New Zealand	●	●	○	○	●	●	○	○
Norway	●	○	●	○	●	●	○	●
Poland	●	○	○	○	○	○	○	●
Portugal	○	●	○	●	○	○	○	○
Slovak Republic	●	●	●	●	●	●	○	○
Slovenia	●	●	○	○	○	○	○	○
Spain	●	●	●	●	●	○	●	●
Sweden	○	○	●	○	●	●	○	●
Switzerland	●	○	●	○	○	●	○	●
Türkiye	○	●	●	●	○	○	○	○
United Kingdom	●	○	○	○	●	○	●	○
OECD Total								
● Yes	26	21	19	13	18	15	6	14
○ No	10	15	17	23	18	21	30	22
Argentina	●	●	●	○	●	●	○	●
Brazil	●	●	●	●	●	●	●	○
Bulgaria	○	○	○	○	○	○	○	○
Indonesia	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Croatia	○	○	○	○	○	○	○	○
Peru	○	○	○	○	○	○	○	○
Romania	○	○	○	○	○	○	○	○
Thailand	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Note: Data not available for Germany, Indonesia, Thailand and the United States. Data cover 1 January 2023 to 31 December 2024.
Source: OECD (2025), Survey on Digital Government 3.0.

Annex Table 4.A.4. Internal controls in place to ensure trustworthy AI

Availability of internal controls and mechanisms are in place within the executive branch to ensure accountability in the development and deployment of AI systems by the public sector

Country	Auditing processes	Internal review committees	Ex ante Risk assessment tools and/or requirements
Australia	●	●	●
Austria	○	○	○
Belgium	○	○	○
Canada	○	○	●
Chile	●	●	●
Colombia	○	○	○
Costa Rica	○	○	○
Czechia	○	○	○
Denmark	○	○	○
Estonia	○	●	●
Finland	○	○	○
France	●	●	●
Greece	○	○	●
Hungary	○	○	○
Iceland	○	○	○
Ireland	●	●	○
Israel	○	○	○
Italy	○	○	○
Japan	○	○	●
Korea	●	○	●
Latvia	○	○	●
Lithuania	○	○	○
Luxembourg	○	●	●
Mexico	○	●	○
Netherlands	●	●	●
New Zealand	○	○	○
Norway	●	○	●
Poland	○	○	○
Portugal	○	●	●
Slovak Republic	○	○	○
Slovenia	○	○	○
Spain	●	●	○
Sweden	○	○	○
Switzerland	●	●	●
Türkiye	●	○	○
United Kingdom	●	●	○
OECD Total			
● Yes	11	12	14
○ No	25	24	22
Argentina	○	○	○
Brazil	○	○	○
Bulgaria	○	○	○
Indonesia	N/A	N/A	N/A
Croatia	○	○	○
Peru	○	●	○

Country	Auditing processes	Internal review committees	Ex ante Risk assessment tools and/or requirements
Romania	○	○	○
Thailand	N/A	N/A	N/A

Note: Data not available for Germany, the United States, Indonesia and Thailand. Data cover 1 January 2023 to 31 December 2024.
Source: OECD (2025), Survey on Digital Government 3.0.

Annex Table 4.A.5. Countries' oversight and advisory bodies for AI in government

Public bodies in charge of providing oversight or ethical advice for AI in the public sector, and type of oversight or advice this/these body/bodies provide(s)

Country	Existence of public body(ies) providing:		Type of oversight or advice that these bodies provide							
	Regulatory oversight	Ethical advice	Procedural guidance	Technical guidance	Educational guidance	Ethical oversight & monitoring	Internal auditing	Auditing by SAIs	Reporting frameworks	Regulatory oversight enforcement
Australia	●	●	●	●	●	●	●	●	●	●
Austria	●	●	●	●	○	●	○	○	○	●
Belgium	○	●	●	●	●	●	○	○	○	○
Canada	●	●	●	●	●	●	○	○	●	●
Chile	○	●	●	●	○	●	○	○	●	○
Colombia	○	○	○	○	○	○	○	○	○	○
Costa Rica	○	○	○	○	○	○	○	○	○	○
Czechia	○	●	●	●	●	●	○	○	○	○
Denmark	●	●	●	●	●	●	●	●	●	●
Estonia	●	●	●	●	●	●	○	●	○	●
Finland	●	○	●	○	○	○	○	○	○	●
France	●	●	●	●	●	●	●	●	●	●
Greece	○	●	●	○	●	●	○	○	●	●
Hungary	○	○	○	○	○	○	○	○	○	○
Iceland	○	●	○	○	●	○	○	○	○	○
Ireland	●	●	●	●	○	○	○	○	○	○
Israel	●	●	●	○	●	○	○	○	○	○
Italy	○	●	●	●	○	○	○	○	○	○
Japan	○	●	●	○	○	●	○	○	○	○
Korea	●	●	●	●	●	●	○	○	●	●
Latvia	○	○	○	○	○	○	○	○	○	○
Lithuania	○	○	○	○	○	○	○	○	○	○
Luxembourg	○	●	○	●	○	●	○	○	○	○
Mexico	○	○	○	○	○	○	○	○	○	○
Netherlands	●	●	●	●	●	●	●	●	●	●
New Zealand	○	●	●	●	●	○	○	○	○	○
Norway	●	●	●	○	●	●	○	●	○	●
Poland	○	●	●	●	●	○	○	○	○	○
Portugal	●	●	●	●	●	●	○	○	●	●
Slovak Rep.	●	○	●	○	●	●	○	○	○	●
Slovenia	●	●	○	●	●	●	○	○	○	●
Spain	○	●	●	○	●	●	○	○	○	○
Sweden	○	●	●	●	●	○	○	○	○	○
Switzerland	●	●	●	●	●	○	○	●	●	●
Türkiye	○	●	●	●	○	○	○	○	○	○

Country	Existence of public body(ies) providing:		Type of oversight or advice that these bodies provide							
	Regulatory oversight	Ethical advice	Procedural guidance	Technical guidance	Educational guidance	Ethical oversight & monitoring	Internal auditing	Auditing by SAIs	Reporting frameworks	Regulatory oversight enforcement
United Kingdom	●	●	●	●	●	●	○	○	●	●
OECD Total										
● Yes	17	28	27	22	22	20	4	7	11	16
○ No	19	8	9	14	14	16	32	29	25	20
Argentina	○	●	○	○	●	○	○	○	○	○
Brazil	○	●	○	●	●	●	○	●	○	○
Bulgaria	○	○	○	○	○	○	○	○	○	○
Croatia	○	○	○	○	○	○	○	○	○	○
Indonesia*	○	●	●	●	●	●	●	○	○	○
Peru	●	●	●	●	●	●	●	●	●	●
Romania	○	○	○	○	○	○	○	○	○	○
Thailand*	○	○	○	○	○	○	○	○	○	○

Note: Data not available for Germany or the United States. Data cover 1 January 2023 to 31 December 2024. (*) Data for Indonesia and Thailand cover 1 January 2022 to 31 December 2023.
Source: OECD (2025), Survey on Digital Government 3.0.

Annex Table 4.A.6. Countries measuring the financial or non-financial impact of AI in government

Availability of central/federal government conducted financial and non-financial impact measurement studies on AI use in the public sector, either prospective, retrospective, or both

Country	For a specific AI use case	For the impact of AI use across a government sector	For the impact of AI use across government	For the broader social and economic impact of AI use by the public sector
Australia	●	○	●	●
Austria	○	○	○	○
Belgium	○	○	○	○
Canada	○	○	○	○
Chile	○	○	○	○
Colombia	○	○	○	○
Costa Rica	○	○	○	○
Czechia	○	○	●	○
Denmark	●	○	●	○
Estonia	●	○	○	○
Finland	○	○	○	○
France	●	○	○	○
Greece	○	○	○	○
Hungary	●	○	○	○
Iceland	○	○	●	○
Ireland	●	○	○	○
Israel	●	○	○	○
Italy	○	○	○	○
Japan	●	○	○	○
Korea	○	○	○	●

Country	For a specific AI use case	For the impact of AI use across a government sector	For the impact of AI use across government	For the broader social and economic impact of AI use by the public sector
Latvia	○	●	○	○
Lithuania	○	○	○	○
Luxembourg	○	○	○	○
Mexico	○	○	○	○
Netherlands	○	●	○	○
New Zealand	○	○	○	●
Norway	○	○	○	●
Poland	○	○	○	○
Portugal	○	○	○	○
Slovak Republic	○	○	○	○
Slovenia	○	○	○	●
Spain	○	●	○	●
Sweden	○	●	●	○
Switzerland	●	○	○	○
Türkiye	○	○	○	○
United Kingdom	○	○	●	○
OECD Total				
● Yes	9	4	6	6
○ No	27	32	30	30
Argentina	○	○	○	○
Brazil	○	○	○	○
Bulgaria	○	○	○	○
Croatia	○	○	○	○
Indonesia	N/A	N/A	N/A	N/A
Peru	○	○	○	○
Romania	○	○	●	○
Thailand	N/A	N/A	N/A	N/A

Note: Data not available for Germany, Indonesia, Thailand and the United States. Data cover 1 January 2023 to 31 December 2024.
Source: OECD (2025), Survey on Digital Government 3.0.

Annex Table 4.A.7. External engagement in developing the AI in government strategy

Actors that collaborated in the process of developing the national strategy, agenda or plan for AI in the public sector

Country	Digital government leading entity	Public sector institutions	Business	Academia	Civil society	Govtech community	Representatives of under-represented groups
Australia	●	●	●	●	●	●	●
Austria	●	●	●	○	○	○	○
Belgium	●	●	●	●	●	●	○
Canada[1]	●	●	●	●	●	●	●
Chile	●	●	●	●	●	●	●
Colombia	●	●	●	●	●	○	○
Costa Rica	●	●	●	●	●	○	○
Czechia	●	●	●	●	○	●	○
Denmark	●	●	●	●	●	●	○

Country	Digital government leading entity	Public sector institutions	Business	Academia	Civil society	Govtech community	Representatives of under-represented groups
Estonia	●	●	●	●	●	●	●
Finland	●	●	●	●	○	○	●
France	●	●	●	●	●	●	○
Greece	●	●	●	●	○	●	○
Hungary	●	●	●	●	●	●	○
Iceland	●	●	●	●	●	●	●
Ireland	●	●	●	●	●	●	●
Israel	●	●	●	●	○	●	○
Italy	●	●	○	●	○	○	○
Japan	●	●	●	●	●	●	○
Korea	●	●	●	●	●	●	○
Latvia	●	●	●	●	○	○	○
Lithuania	●	●	●	●	○	●	○
Luxembourg	●	●	○	○	●	○	○
Mexico	○	○	○	○	○	○	○
Netherlands	●	●	●	●	●	●	○
New Zealand	●	●	●	●	●	●	●
Norway	●	●	●	●	●	●	●
Poland	●	●	●	●	●	●	●
Portugal	●	●	●	●	●	●	○
Slovak Republic	●	●	○	○	○	○	○
Slovenia	●	●	●	●	●	●	○
Spain	●	●	○	●	○	○	○
Sweden	●	●	●	●	●	○	○
Switzerland	○	○	○	○	○	○	○
Türkiye	●	●	●	●	●	○	○
United Kingdom	●	●	●	●	●	●	●
OECD Total							
● Yes	33	33	29	30	23	22	10
○ No	3	3	7	6	13	14	26
Argentina	○	●	●	●	○	●	○
Brazil	●	●	●	●	●	●	○
Bulgaria	○	○	○	○	○	○	○
Croatia	○	○	○	○	○	○	○
Indonesia	●	●	●	●	●	●	○
Peru	○	○	○	○	○	○	○
Romania	○	○	○	○	○	○	○
Thailand	○	○	○	○	○	○	○

Note: Data not available for Germany and the United States. Data cover 1 January 2023 to 31 December 2024. Data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.

1. Data were updated following a request from the country after the publication of the 2025 DGI; therefore, these changes are not reflected in the 2025 DGI results.

Source: OECD (2025), Survey on Digital Government 3.0.

REFERENCES

Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) (n.d.), *Ensuring ethical and responsible AI*, https://aesia.digital.gob.es/es. [11]

Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) (n.d.), *Guides on Artificial Intelligence*, https://aesia.digital.gob.es/en/guides. [12]

Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) (n.d.), *Organisational structure and governance*, https://aesia.digital.gob.es/en/estructura-organizativa. [13]

AI in the State (n.d.), *Incubateur ALLiaNCE*, https://ia.numerique.gouv.fr/incubateur-alliance/les-produits-incub%C3%A9s/. [27]

ALIA (n.d.), *Public AI infrastructure in Spanish and co-official languages*, https://alia.gob.es. [40]

Australian Department of Finance (2025), *Introducing the APS AI Plan*, https://www.finance.gov.au/about-us/news/2025/introducing-aps-ai-plan. [19]

Australian Government (2024), "Evaluation of the whole-of-government trial of Microsoft 365 Copilot", https://www.digital.gov.au/initiatives/copilot-trial. [85]

Australian Public Service Academy (n.d.), *AI in government fundamentals*, https://www.apsacademy.gov.au/course-sessions/ai-government-fundamentals. [16]

Austrian Ministry of Finance (BMF) (n.d.), *Predictive Analytics Competence Center*, https://www.bmf.gv.at/themen/betrugsbekaempfung/einheiten-betrugsbekaempfung/Predictive-Analytics-Competence-Center.html. [32]

beEU (2024), *A Citizens' View of Artificial Intelligence within the EU*, https://glassroots.com/wp-content/uploads/2024/09/Rapport-IA-EN.pdf. [90]

Berryhill, J. et al. (2019), "Hello, World: Artificial intelligence and its use in the public sector", *OECD Working Papers on Public Governance*, No. 36, OECD Publishing, Paris, https://doi.org/10.1787/726fd39d-en. [69]

BOSA (n.d.), *AI4Belgium*, https://bosa.belgium.be/fr/AI4Belgium. [91]

BOSA (n.d.), *L'IA dans le secteur public (AI4GOV)*, https://bosa.belgium.be/fr/AI4Belgium/AI4GOV. [92]

Brazilian Secretariat of Digital Government (2024), *Data Maturity Model (MMB)*, https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/maturidade-de-dados/arquivos/modelo-maturidade-de-dados-mmd.pdf. [35]

Bright, J. et al. (2024), *Generative AI is already widespread in the public sector*, https://arxiv.org/abs/2401.01291. [71]

Brizuela, A. et al. (2025), *Analysis of the generative AI landscape in the European public sector*, European Commission, https://op.europa.eu/s/z4XY. [9]

Cabinet Office of Japan (2026), *Human-Centered AI Society Principles Conference*. [66]

Chile's Ministry of Science, Technology, Knowledge and Innovation (2024), *Política Nacional de Inteligencia Artificial*, https://drive.google.com/file/d/11OLxLp8NyKgpeRFLe45X0zStY7SFEJIC/edit?pli=1. [74]

Chile's Ministry of Science, Technology, Knowledge and Innovation (2023), *Lineamientos para el uso de Inteligencia Artificial*, https://minciencia.gob.cl/uploads/filer_public/ae/9a/ae9a7ce7-807b-4781-9ac3-9b253bfbe735/of_n711_2023_dis_lin_ia_minciencia.pdf. [75]

Congress of the Republic of Peru (2025), *Law No. 32270: Amendment to the Organic Law on Elections introducing digital voting*. [54]

Consejo Nacional de Política Económica y Social (2025), *Política Nacional de Inteligencia Artificial (CONPES 4144)*, Departamento Nacional de Planeación, https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf. [67]

Danish Agency for Digital Government (n.d.), *Signature projects with artificial intelligence in municipalities and regions*, https://digst.dk/kunstig-intelligens/signaturprojekter. [24]

Danish Agency for Digital Government (n.d.), *The Grant Pool for New Technologies*, https://digst.dk/digital-transformation/tilskudspuljen-for-nye-teknologier. [25]

Danish Centre for AI Innovation (DCAI) (2024), *Denmark's first AI supercomputer is now operational*, https://dcai.dk/news/denmark-s-first-ai-supercomputer-is-now-operational. [34]

Department for Science, Innovation & Technology (2026), *Consultation outcome, Guidance for using the AI Management Essentials tool: government response*, https://www.gov.uk/government/consultations/ai-management-essentials-tool/outcome/guidance-for-using-the-ai-management-essentials-tool-government-response. [95]

Department of Public Expenditure NDP Delivery and Reform (2024), *Interim Guidelines for Use of Artificial Intelligence in the Public Service*. [80]

Digital Agency of Japan (2025), *Advanced AI Utilization Advisory Board*, https://www.digital.go.jp/en/councils/ai-advisory-board. [68]

Digital Agency of Japan (2025), *The Guideline for Japanese Governments' Procurements and Utilizations of Generative AI for the sake of Evolution and Innovation of Public Administration*, https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/6e45a64f/20250527_resources_standard_guidelines_guideline_04.pdf. [52]

Digital Island (n.d.), website, https://island.is/en/o/digital-iceland/island-is. [5]

Digital Transformation Agency of Australia (n.d.), *Policy for the responsible use of AI in government*, https://www.digital.gov.au/ai/ai-in-government-policy/strategy-and-oversight. [57]

Dutch Government (n.d.), *Algoritmeregister (Algorithm Register of the Dutch Government)*, https://algoritmes.overheid.nl/en. [59]

European Union (2024), *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, https://eur-lex.europa.eu/eli/reg/2024/1689/oj. [3]

Federal Public Service (FPS), Public Social Security Institutions (IPSS) and ICT organisations (n.d.), *G-CLOUD, the common cloud of the public sector*. [31]

Gartner (2025), *Gartner Survey Finds 45% of Organizations With High AI Maturity Keep AI Projects Operational for at Least Three Years*, https://www.gartner.com/en/newsroom/press-releases/2025-06-30-gartner-survey-finds-forty-five-percent-of-organizations-with-high-artificial-intelligence-maturity-keep-artificial-intelligence-projects-operational-for-at-least-three-years. [84]

Giesecke, O. (2024), *Generative AI Use In US Public Sector On The Rise, Survey By Hoover Fellow Suggests*, https://www.hoover.org/generative-ai-use-us-public-sector-rise-survey-hoover-fellow-suggests. [70]

Government of Canada (2026), *Algorithmic Impact Assessment tool*, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html. [47]

Government of Canada (2025), *Consultations on the AI Strategy for the Federal Public Service: What We Heard*, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/consultations-ai-strategy-federal-public-service-what-we-heard.html. [93]

Government of Colombia (2026), *Guía Ética para la Implementación, Desarrollo y Uso de Sistemas de Inteligencia Artificial en Entidades Públicas de Colombia*, https://www.mintic.gov.co/portal/715/articles-425888_recurso_1.pdf (accessed on 8 June 2026). [62]

Government of Colombia (2025), "Colombia estrena Directiva para garantizar la transparencia de los algoritmos del Estado", Procuraduría General de la Nación, https://www.procuraduria.gov.co/Pages/colombia-estrena-directiva-garantizar-transparencia-algoritmos-estado.aspx. [61]

Government of Estonia (2026), *AI use cases: Examples of artificial intelligent applications in the Estonian public sector*. [60]

Government of France (2024), *Produits incubés en 2024*, https://alliance.numerique.gouv.fr/produit/les-produits-incub%C3%A9s-2024. [23]

Government of France (n.d.), *Code des relations entre le public et l'administration*, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000031366350/LEGISCTA000031367696/?anchor=LEGIARTI000033205535. [56]

Government of Greece (2024), *Blueprint for Greece's AI Transformation*, https://foresight.gov.gr/en/studies/A-Blueprint-for-Greece-s-AI-Transformation/. [45]

Government of Ireland (2025), *Guidelines for the Responsible Use of AI in the Public Service*, Department of Public Expenditure, Infrastructure, Public Service Reform and Digitalisation, https://assets.gov.ie/static/documents/09fe3ad4/Guidelines_for_the_Responsible_Use_of_AI_in_the_Public_Service_20250918.pdf. [64]

Government of Luxembourg - Ministry of Digitalization (n.d.), *The AI4Gov initiative*, https://mindigital.gouvernement.lu/en/dossiers.gouv2024_mindigital+fr+dossiers+2021+AI4Gov.html. [50]

Government of Peru (2023), *Law No. 31814*. [46]

Government of Portugal (2025), *Despacho n.º 749/2025, Diário da República, 16 January*, https://diariodarepublica.pt/dr/detalhe/despacho/749-2025-903770555. [96]

Government of Portugal (2024), *Resolução do Conselho de Ministros n.º 201/2024, Diário da República, 30 December*, https://diariodarepublica.pt/dr/analise-juridica/resolucao-conselho-ministros/201-2024-901536075. [97]

Government of the Netherlands (2026), *Algoritmekader (Algorithmic Framework)*, https://minbzk.github.io/Algoritmekader. [77]

Government of the Republic of Türkiye (n.d.), *1711 - Artificial Intelligence Ecosystem Call*, Scientific and Technological Research Council of Türkiye – TÜBİTAK, https://tubitak.gov.tr/tr/destekler/sanayi/ulusal-destek-programlari/1711-yapay-zeka-ekosistem-cagrisi. [26]

Government of the United Kingdom (2025), *Evaluation of the M365 Copilot pilot in the Department for Business and Trade*, Department for Business and Trade, https://www.gov.uk/government/publications/microsoft-365-copilot-pilot-dbt-evaluation-report. [86]

IMY (2025), *National guidelines for generative AI in public administration are launched*, Swedish Authority for Privacy Protection, https://www.imy.se/en/news/national-guidelines-for-generative-ai-in-public-administration-are-launched/. [65]

Inspector General of Colombia and Ombudsman of Colombia (2025), *Estándares de transparencia algorítmica para los sistemas utilizados por el Estado*, https://www.defensoria.gov.co/documents/20123/3407303/300925DirectivaConjunta007.pdf/c47e1175-6f60-058a-3e0b-3dfaf82d5f23?t=1759261267112 (accessed on 8 June 2026). [63]

Israel National Digital Agency (2025), *Setting the Standard: Israel Unveils First-Ever Responsible AI Guide for the Public Sector*, https://www.gov.il/en/pages/ai-guide. [94]

Israel Privacy Protection Authority (2025), *Guide on Implementing Privacy-Enhancing Technologies in Artificial Intelligence Systems*, https://www.gov.il/BlobFolder/generalpage/pets_ai/en/PETs_AI_english_accessable.pdf. [41]

Korea Internet & Security Agency (KISA) (n.d.), *AI Threat Detection and Response*, https://academy.kisa.or.kr/cont/programInfo/eduIntroAI.do. [17]

Korean Public Procurement Service (2022), *Launch of AI-Based Public Software Project Ordering Support System*, https://www.pps.go.kr/kor/bbs/view.do?bbsSn=2208010006&key=00318. [8]

LINC (2025), *We tested homomorphic encryption!*, https://linc.cnil.fr/teste-le-chiffrement-homomorphe. [42]

Ministry of Industry and Trade, Czech Republic (2024), *National Artificial Intelligence Strategy 2030*, https://mpo.gov.cz/assets/cz/podnikani/digitalni-ekonomika/umela-inteligence/2024/7/Narodni-strategie-umele-inteligence-2030.pdf. [14]

Ministry of Information Technologies and Communications (MinTIC) (2025), *Registration is open for the free diploma in Artificial Intelligence for public servants*, https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/406073:Abiertas-inscripciones-para-diplomado-gratuito-en-Inteligencia-Artificial-para-servidores-publico. [20]

Ministry of the Economy and Innovation (2025), *AI Training Platform*, https://eimin.lrv.lt/lt/veiklos-sritys/skaitmenine-politika/dirbtinis-intelektas/di-viesajame-sektoriuje/di-mokymu-platforma. [22]

Ministry of the Interior and Kingdom Relations (2025), *Responsible Use of Generative AI: Government-Wide Guide*, https://www.government.nl/documents/2025/01/31/responsible-use-of-generative-ai. [82]

Ministry of Transformation and Civil Service (2024), *Towards a strategy to use Artificial Intelligence (AI) in French civil service HRM*. [89]

MIT NANDA (2025), *The GenAI Divide: State of AI in Business 2025*, MIT Networked AI Agents in Decentralized Architecture, https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf. [73]

New Zealand Digital Government (2025), *Responsible AI guidance for the Public Service: Generative AI – Customer experience and Privacy*, https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/artificial-intelligence/responsible-ai-guidance-for-the-public-service-genai/customer-experience/privacy. [78]

New Zealand Government (n.d.), *Data standards toolkit*, https://data.govt.nz/toolkit/data-standards. [79]

NHS Digital (n.d.), *Artificial data pilot*, https://digital.nhs.uk/services/artificial-data. [43]

OECD (2026), *Building an AI-ready public workforce: Implications and strategies*, OECD Publishing, Paris, https://doi.org/10.1787/b89244c7-en. [72]

OECD (2025), "AI openness: A primer for policymakers", *OECD Artificial Intelligence Papers*, No. 44, OECD Publishing, Paris, https://doi.org/10.1787/02f73362-en. [10]

OECD (2025), *Digital Government Review of Korea: Harnessing Digital and Data to Transform Government*, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/9defc197-en. [4]

OECD (2025), *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*, OECD Publishing, Paris, https://doi.org/10.1787/795de142-en. [2]

OECD (2025), "Sharing trustworthy AI models with privacy-enhancing technologies", *OECD Artificial Intelligence Papers*, No. 38, OECD Publishing, Paris, https://doi.org/10.1787/a266160b-en. [30]

OECD (2024), "AI, data governance and privacy: Synergies and areas of international co-operation", *OECD Artificial Intelligence Papers*, No. 22, OECD Publishing, Paris, https://doi.org/10.1787/2476b1a4-en. [28]

OECD (2024), "Framework for Anticipatory Governance of Emerging Technologies", *OECD Science, Technology and Industry Policy Papers*, No. 165, OECD Publishing, Paris, https://doi.org/10.1787/0248ead5-en. [88]

OECD (2024), "Recommendation of the Council on Artificial Intelligence", *OECD Legal Instruments*, OECD/LEGAL/0449, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [1]

OECD (2023), "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", *OECD Digital Economy Papers*, No. 351, OECD Publishing, Paris, https://doi.org/10.1787/bf121be4-en. [29]

OECD (2023), *Global Trends in Government Innovation 2023*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/0655b570-en. [55]

OECD (forthcoming), *Governing with Artificial Intelligence: Measuring impact and demonstrating returns on AI investments*. [87]

OECD Observatory of Public Sector Innovation (OPSI) (n.d.), *Robot Alice – Bid, Contract and Notice Analyser*, https://oecd-opsi.org/innovations/robot-alice-bid-contract-and-notice-analyser/ (accessed on 1 June 2026). [7]

Office for National Statistics (ONS) - Data Science Campus (2023), *Synthesising the linked 2011 Census and deaths dataset while preserving its confidentiality*, https://datasciencecampus.ons.gov.uk/synthesising-the-linked-2011-census-and-deaths-dataset-while-preserving-its-confidentiality/. [38]

Ramos, L. and R. Kandaswamy (2023), *Capture AI Value With These 5 Benefit Realization Best Practices*, Gartner, https://static1.squarespace.com/static/5530dddfe4b0679504639dc1/t/66040dae666c427d843c6de6/1711541693913/Capture+AI+Value+With+These+5+Benefit+Realization+Best+-+Gartner.pdf. [83]

Republic Portuguesa (2023), *Virtual assistant with Artificial Intelligence will support citizens in ePortugal*, https://www2.gov.pt/en/noticias/assistente-virtual-com-inteligencia-artificial-vai-apoiar-os-cidadaos-no-eportugal. [33]

Secretariat of Digital Government of Brazil (2025), *Cartilha de Inteligência Artificial Generativa (Generative AI Guide)*, https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/inteligencia-artificial-1/publicacoes/cartilha-ia-generativa. [76]

Spanish Agency for the Supervision of Artificial Intelligence (AESIA) (n.d.), *Ensuring ethical and responsible AI*, https://aesia.digital.gob.es. [81]

Sweden Agency for Digital Government (DIGG) (n.d.), *Ena – Sweden's digital infrastructure*, https://www.digg.se/styrning-och-samordning/ena---sveriges-digitala-infrastruktur. [36]

TSE Global (n.d.), *Sistem Belgelendirme (System Certification Services)*, https://www.tseglobal.com.tr/sistem-belgelendirme?num=38%3Flg%3Den. [51]

Turkish Standards Institution (TSE) (2026), *Ayna Komiteler (Mirror Technical Committees)*, https://intweb.tse.org.tr/standard/aynakomite/aynakomiteler.aspx. [49]

Türkiye Digital Transformation Office and Ministry of Industry and Technology (2021), *National Artificial Intelligence Strategy 2021–2025*, https://wp.oecd.ai/app/uploads/2021/12/Turkey_National_Artificial_Intelligence_Strategy_2021-2025.pdf. [48]

UK Cabinet Office (2025), *One Big Thing 2025: 'AI for All' - A Modern Civil Service Blog,*, https://moderncivilservice.blog.gov.uk/2025/10/14/one-big-thing-ai-for-all-is-live/. [18]

UK Department for Science, Innovation and Technology (2026), *AI Opportunities Action Plan: One Year On*, https://www.gov.uk/government/publications/ai-opportunities-action-plan-one-year-on/ai-opportunities-action-plan-one-year-on. [44]

UK Department of Science, Innovation and Technology (2023), *The UK-US Blog Series on Privacy-Preserving Federated Learning: Introduction*, https://rtau.blog.gov.uk/2023/12/07/the-uk-us-blog-series-on-privacy-preserving-federated-learning-introduction/. [39]

UK Government (n.d.), *Find out how algorithmic tools are used in public organisations*, https://www.gov.uk/algorithmic-transparency-records. [58]

UK Government (n.d.), *Government – AI Incubator for Artificial Intelligence (i.AI)*, https://ai.gov.uk/our-work/government/ (accessed on 1 June 2026). [6]

UK Government (n.d.), *Service Standard*, https://www.gov.uk/service-manual/service-standard. [37]

UK Government Digital Service (n.d.), *Making the Algorithmic Transparency Recording Standard (ATRS) mandatory across government*, https://dataingovernment.blog.gov.uk/2025/05/08/making-the-algorithmic-transparency-recording-standard-atrs-mandatory-across-government. [53]

UNESCO (2025), *Strengthening Digital Resilience: Costa Rica's AI Push After a Massive Cyberattack*, https://www.unesco.org/es/articles/fortalecer-la-resiliencia-digital-el-impulso-de-costa-rica-por-la-ia-tras-un-ciberataque-masivo. [21]

University of Helsinki and MinnaLearn (n.d.), *Elements of AI – Free online course on artificial intelligence*, https://www.elementsofai.com. [15]

NOTES

[1] For more information on AI in Government, see https://oecd.ai/gov.

[2] The OECD.AI Policy Navigator is available at https://oecd.ai/dashboards. More specifically, AI use cases in the public sector can be found at https://oecd.ai/dashboards/policy-initiatives?initiativeTypeIds=123.

[3] For more information, see https://www.oecd.org/en/topics/sub-issues/privacy-enhancing-technologies.html.

[4] Portugal's National Agenda on Artificial Intelligence, as part of the National Digital Strategy: Resolution 749/2025 (Government of Portugal, 2025[94]) and Legal Analysis of Resolution 201/2024 (Government of Portugal, 2024[95]).

[5] Acteurs Publics (2026), IA : David Amiel veut faire aboutir le dialogue social à un accord d'ici l'automne (AI: David Amiel aims to reach a social dialogue agreement by autumn).

[6] The rates among OECD accession candidate countries are: public sector organisations (50%); civil servants (17%); broader ecosystem (33%); service users (17%); and cross-border actors (17%).

[7] See Estonia's guidelines for digital public services (https://digiriik.eesti.ee/protsess/kasutuselevott/tagasiside-kogumine) and the Estonian Tax and Customs Board's online feedback form (https://www.emta.ee/en/private-client/board-news-and-contacts/contacts/feedback).


03
04
05
06
65
72
snlutions thatc
H proud pt zkva
pgrjfe wi jre
AI
do eiusmod uf mo
t nluptate velit es
Lorem ipsum
10
20
30
40
50
00

5 Building human-centred and proactive government services in the digital age

Public services are one of the most direct ways in which governments are experienced by people. Making them work well is therefore as much an implementation challenge as a matter of policy or design. Drawing on the 2025 Digital Government Index, this chapter examines how governments can move beyond strategies and standards to deliver services that are reliable, joined-up and easy to navigate. It shows that service standards are widespread but inconsistently applied; user engagement is improving yet remains narrow and ad hoc; reliable delivery requires joined-up channels, digital identity and trusted data; proactive services depend on shared foundations, not isolated efforts; and continuous improvement needs measurement systems that genuinely inform frontline decisions. Across all of these elements, the evidence points to a common conclusion: closing the gap between ambition and delivery is the key challenge, and doing so requires sustained attention to governance, capability and accountability, not technology alone.

Key messages

- **The core challenge in public administrative services is implementation**. Many governments have strategies, service standards and tools, and yet users still experience friction when accessing services due to fragmented entry points, poorly coordinated journeys across agencies and levels of government, and inconsistent quality depending on which part of government they deal with. The gap between policy ambition and what people actually experience is the defining implementation challenge for public service delivery today.
- **Whole-of-government service standards are widespread, but their value depends on whether they shape everyday decisions.** The issue is not whether standards exist, but whether they shape routine decisions (e.g. investment approval, delivery gates, procurement and service reviews) and help improve the delivery and commitments of the administration towards users. Closing the gap between having standards and their application in practice requires both practical support and governance mechanisms that make standards hard to ignore.
- **User engagement is improving but needs to be more consistent, involve a wider range of users and continue throughout the service lifecycle.** Governments are doing more to involve people in service design, and co-design tools are now widely available. But engagement still too often reaches the most accessible users rather than those with the greatest needs, takes place at the start of projects rather than throughout their lifecycle, and stops short of making testing a routine expectation. Engagement that is embedded as a regular practice, and that deliberately reaches people who face higher barriers to access, produces better services and reduces the risk of costly problems emerging after launch.
- **Reliable service delivery depends on joined-up channels, shared infrastructure and trusted data sharing.** Ministries have made progress integrating data and services within their own policy areas, but these efforts rarely extend across organisational boundaries. Services need to work consistently across agencies and levels of government, regardless of how people access them, and users should be able to move between channels without repeating information. This depends on three things working together: a clear approach to how channels relate to one another, digital identity systems that are widely used across services, and the ability to share data between agencies in ways that are governed and trusted in practice.
- **Proactive services reduce burdens and improve fairness, but require shared foundations to scale.** When government anticipates needs and acts before people have to ask, it reduces the effort required to access support and helps ensure entitlements reach those who need them, not only those best placed to navigate bureaucracy. Achieving this requires making the once-only principle an operational default, shifting data use from planning into service delivery, and applying automation and AI with appropriate oversight and safeguards. Automating routine, rules-based tasks like eligibility checks can make services faster, more accurate and more equitable, while freeing staff for cases requiring judgement or support.
- **Stronger feedback loops are critical to continuous improvement.** Most governments monitor services to some degree, but measurement of actual service performance and what services cost people in time and effort remains limited and inconsistent. Only 28% of OECD countries have standardised ways of measuring the burdens services impose on users. Without reliable, consistent measurement connected to the decisions that shape services, improvement tends to be exceptional rather than routine.

5.1. Introduction

Public services are perhaps the most direct expression of what government does for people. When they work well – when they are easy to navigate, reliably available and responsive to individual circumstances – they build confidence in government. When they do not, they erode it. OECD evidence shows that people's satisfaction with public administrative services is strongly shaped by whether services are fast and easy to use, and that nearly half of people (46%) do not feel confident they can access support when they need it (OECD, 2024[1]). Only 31% of people, on average across OECD countries, feel they could easily receive public benefits if they needed them, and 28% say they think the application process would be simple and quick (OECD, 2025[2]). As expectations rise and people's needs become more complex, governments' ability to deliver services that are simple, dependable and joined up becomes increasingly important for trust. In some service journeys, the stakes also go beyond convenience, as public services can affect people's ability to understand, claim or exercise their rights.

People's needs rarely fit neatly within a single government organisation. A person seeking support may simultaneously be a worker, a caregiver, a student and a small-business owner. Yet public services are still frequently organised around institutional boundaries rather than people's actual situations. The result is duplication, repeated requests for the same information and fragmented handovers between agencies, making services difficult to navigate, particularly for people already dealing with difficult circumstances such as job loss, health challenges or displacement. These challenges can be particularly consequential where service journeys affect rights, obligations or access to remedies, for example in relation to legal aid, victim support services or protective measures. The OECD Recommendations on Human-Centred Public Administrative Services and on Access to Justice and People-Centred Justice Systems recognise these challenges and call for services that place people's needs at the centre of design and delivery, while ensuring reliability, fairness, transparency and trust (OECD, 2025[3]; OECD, 2023[4]). The Recommendations underscore that delivering on this ambition requires not only good intentions but reliable digital infrastructure, effective data governance and the organisational capacity to coordinate across institutional boundaries (Box 5.1).

Many governments have made real progress. Strategies, standards and tools for human-centred service design are now widespread. But the central challenge today is not whether service frameworks exist: it is whether they shape what happens in practice. In many countries, services are still experienced as a collection of disconnected entry points across ministries, agencies and levels of government, rather than a joined-up system. Governance is fragmented, accountability for cross-cutting journeys is unclear, and technical and organisational capabilities vary significantly across agencies and levels of government. Furthermore, line ministries have advanced in designing and delivering services that meet user needs, but face issues when integrating with other sectors to deliver more complex services such as life events (OECD, 2024[5]; OECD, 2023[6]). As a result, users experience inconsistency, duplication and unnecessary complexity, not because governments lack ambition, but because they have not yet solved this implementation problem.

This chapter looks at the implementation challenges of delivering human-centred public administrative services. It explores how governments organise, steer and improve services so that people experience them as reliable, easy to navigate and responsive, both in ordinary circumstances and when conditions change. It is organised around where service delivery most often succeeds or fails in practice:

- **Service standards:** whether they exist is less the question than whether they shape day-to-day decisions about design, investment and delivery.
- **User engagement**: whether it involves a sufficiently wide range of people and is embedded throughout the service life rather than concentrated at the start.
- **Reliability**: whether services remain coherent and accessible as needs shift, demand changes and circumstances evolve.
- **Proactive services**: whether governments can anticipate needs and act before people have to ask.
- **Feedback and measurement**: whether governments have the information they need to improve continuously and steer performance over time,

Box 5.1. OECD Recommendation on Human-Centred Public Administrative Services

The Recommendation provides a policy framework for the development and implementation of public administrative services (PAS) that put people's needs at the centre of policy design and delivery. PAS are the administrative processes that people use to comply with laws and regulations, access government programmes, and use their rights. These include familiar processes that many people use regularly, such as renewing passports or identity documents, paying taxes, or managing their benefits like public pensions. Other PAS are processes that an individual may use only occasionally but at important points in their lives, such as applying for a driving license; registering a birth, marriage or death; or getting the deed on a home

The Recommendation has four pillars:

Pillar 1: Strategic vision, values and rights

- **Whole-of-government strategy:** develop services aligned with government-wide goals.
- **Foster a human-centred culture:** prioritise user needs and public engagement.
- **Protect rights:** respect the rule of law, providing procedural guarantees and transparency.

Pillar 2: Core foundations

- **Leadership and roles:** clearly define leadership and co-ordination responsibilities.
- **Skills and competencies:** build public servants' capacity to design and deliver services.
- **Digital infrastructure:** develop scalable, secure and interoperable digital infrastructure to support service delivery.

Pillar 3: Seamless and accessible services

- **User-centred design:** based on user needs, ensuring inclusiveness and accessibility.
- **Omni-channel approach:** provide consistent, high-quality service across all channels.
- **Simplified services:** streamline processes, reduce administrative burdens, anticipate needs.

Pillar 4: Measurement, engagement, improvement

- **Measure user experience:** track user satisfaction and service performance.
- **Data-driven improvement:** use data and feedback to continuously enhance services.
- **Public engagement:** involve users in the co-design and evaluation of services.

Source: (OECD, 2025[3])

5.2. Service standards are widespread, but applying them consistently remains a challenge

Having clear expectations for how public services should be designed and delivered is an important foundation for consistency. Service standards – which are frameworks that set out what good service looks like - help agencies work to a common benchmark, reduce fragmentation and give teams practical guidance for design and delivery decisions. Such principles will usually provide the basis for setting expectations with delivery partners (whether those are public servants or non-governmental suppliers), and in some cases may also be the criteria against which formal assessments of performance are carried out.

Box 5.2. An example of service standard: the United Kingdom

The United Kingdom's Service Standard sets out a clear definition of what good services look like. It translates high-level principles into a practical checklist for teams, covering:

1. Understand users and their needs
2. Solve a whole problem for users
3. Provide a joined up experience across all channels
4. Make the service simple to use
5. Make sure everyone can use the service
6. Have a multidisciplinary team
7. Use agile ways of working
8. Iterate and improve frequently
9. Create a secure service which protects users' privacy
10. Define what success looks like and publish performance data
11. Choose the right tools and technology
12. Make new source code open
13. Use and contribute to open standards, common components and patterns
14. Operate a reliable service

By stating these expectations in one place, the standard helps make service quality more consistent across organisations and supports assurance and review conversations with a shared reference point.

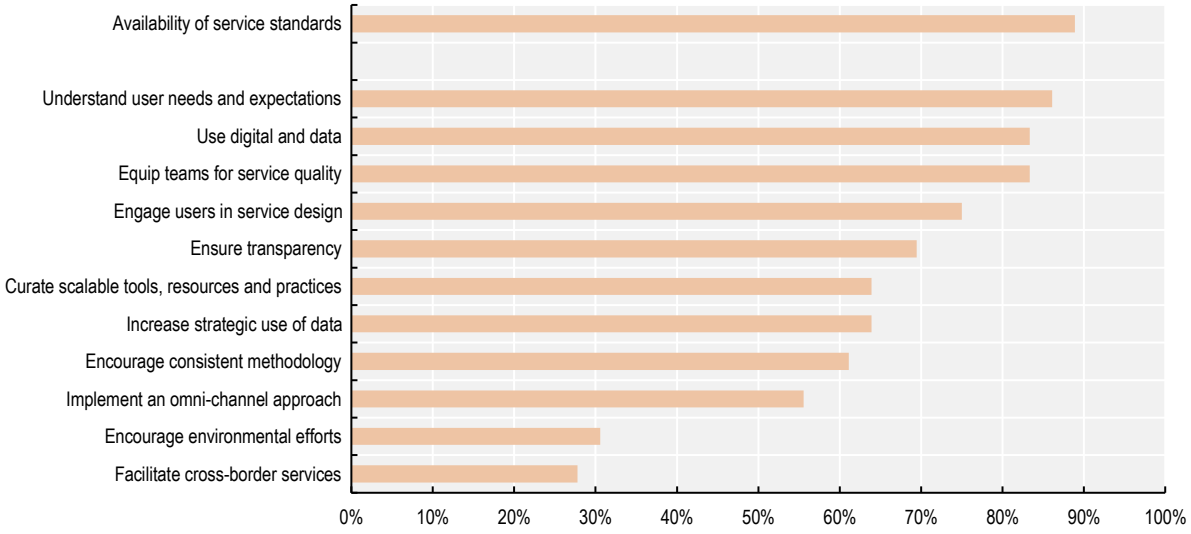
Source: (GOV.UK, 2019[7])

5.2.1. Service standards as shared principles are widely in place

Service standards are now in place in 32 out of 36 OECD countries (89%), reflecting broad recognition that coherent service delivery requires shared expectations across government. Standards typically focus on service quality, user engagement and a consistent, whole-of-government approach to design and delivery. However, the 2025 DGI results show that some important dimensions are less consistently covered (Figure 5.1). Omni-channel approaches, which ensures services work consistently across digital, telephone, in-person and other channels, are included in standards in only 20 out of 36 countries. Cross-border service delivery features in standards in just 10 out of 36. As people increasingly expect services that work across channels and jurisdictions, these gaps are worth addressing.

Figure 5.1. Whole-of-government service standards are widespread across OECD countries, primarily targeting service design and use of digital and data, but significantly less supporting cross-border service delivery

Percentage of OECD countries with availability of government-wide service standards and associated goals, 2025



Note: Data not available for Germany or the United States. Refer to Annex Table 5.A.1 for comprehensive OECD and Accession country data.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/wta2ri

The OECD Good Practice Principles for Public Service Design and Delivery in the Digital Age provide a reference point for this shared understanding. They emphasise designing services around real user needs, delivering coherent omni-channel journeys, ensuring that multidisciplinary teams can do high-quality work, and promoting accountability and transparency throughout design and delivery (OECD, 2022[8]). These principles help administrations articulate a common benchmark for quality, supporting alignment across agencies and reducing fragmentation.

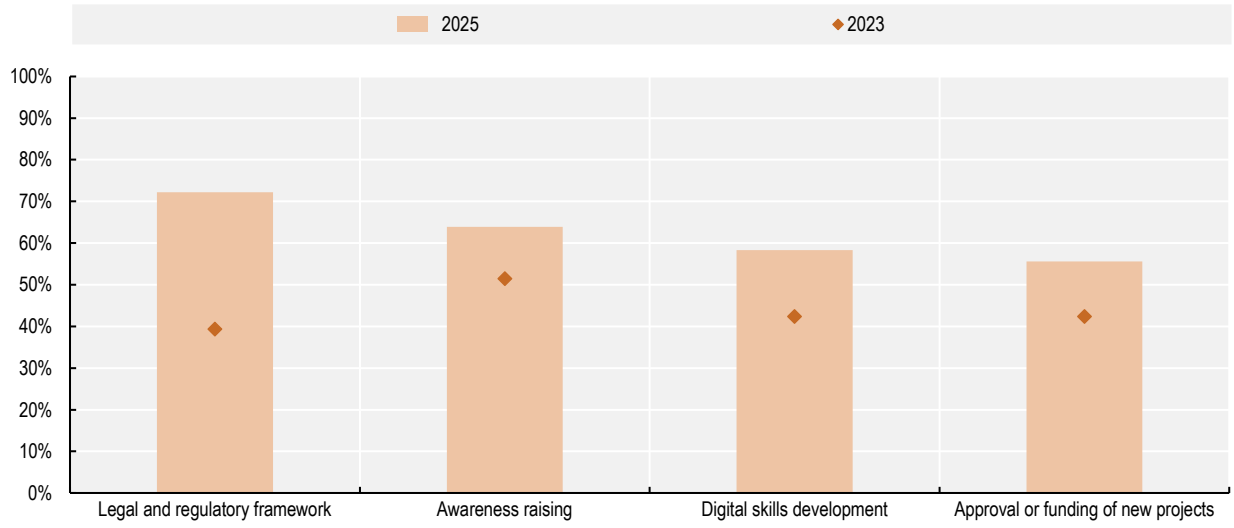
5.2.2. Consistent application of service standards remains the challenge

However, the central challenge is not whether standards exist, it is whether they change how services are actually built and delivered. Human centred design for digital services depends both on standards that are practical to use and on governance mechanisms that support consistent application. A standard only has impact if it shapes the decisions that matter: how services are prioritised, how funding is approved, how delivery teams work day to day, and how services are reviewed and improved over time. Without this, standards risk remaining aspirational documents that teams are aware of but not consistently guided by. Furthermore, it remains essential to promote their adoption and use consistently across government functions to avoid duplication of efforts and promote a more consistent, unified experience to users.

The 2025 DGI results point to an important implementation gap: while many countries report having service standards, formal requirements to use standards are limited, with only 16 out of 36 countries (44%) reporting that following the service standard is mandatory at both central/federal and sub-national levels. The use of mechanisms to support their application – ranging from hard levers, such as legal or regulatory requirements and links to project approval or funding, to softer supports, such as awareness-raising activities and investment in digital skills – are also moderate (Figure 5.2). This matters because consistency does not emerge automatically across ministries, agencies and levels of government. Where standards are optional or unevenly applied, the quality of services people receive can depend more on which agency they deal with, or which team happens to be responsible, than on any government-wide commitment to good design.

Figure 5.2. While legal requirements to adopt service standards are adopted in most OECD countries, more can be done to embed them in digital investments decision-making

Percentage of OECD countries reporting mechanisms to support the application of service standards, by type, 2023 and 2025



Note: 2025 data not available for Germany and the United States. 2023 data not available for Germany, Greece, Slovak Republic, Switzerland and the United States. Refer to Annex Table 5.A.1 for comprehensive OECD and Accession country data.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/gb0wno

Strengthening implementation requires at least two things working together. First, governments need to make standards easier to use, providing clear guidance, templates and practical tools that help teams translate standards into concrete design and delivery decisions. Second, governments need to make standards harder to ignore, by embedding them in the governance and management processes that shape services. This includes checking compliance at key stages such as project approval and service launch, and linking adherence to standards to funding and procurement decisions. When these mechanisms are in place alongside shared platforms and common infrastructure, they can shift service delivery away from fragmented, one-off solutions towards reusable, consistent approaches that benefit users across government (Box 5.3).

Box 5.3. Making service standards work in practice

Some OECD countries combine legal requirements, investment governance and practical support to turn service standards into everyday delivery tools:

- **Portugal's** Decree-Law 49/2024 makes MOSAICO (a common model for designing digital public services centred on people and businesses) mandatory from August 2024. Implementation is linked to project governance requirements, and agencies are supported through published toolkits and capacity-building activities led by LabX.
- **Australia** connects investment oversight to service standards: the Digital and ICT Investment Oversight Framework links funding decisions to compliance with whole-of-government standards under the Digital Experience Policy, including the Digital Service Standard, Digital Inclusion Standard, Digital Access

Standard and Digital Performance Standard. Practical tools and guidance support teams in applying these standards consistently.

- **Italy** anchors service design in law: Design Guidelines for government websites and digital services are required under the Digital Administration Code, with clear distinctions between mandatory requirements and recommended approaches.
- **Switzerland** reinforces service delivery and interoperability expectations through a legal and standards framework anchored in the Public Procurement Act (BöB) and the Federal ICT Strategy. Associated eCH standards specify whether they are mandatory or recommended and for whom, providing clarity for teams implementing them.

Source: (OECD, 2023[9]; Portuguese Republic, 2026[10]; Designers Italy, 2025[11]; L'Assemblée fédérale de la Confédération suisse, 2024[12]; Confédération suisse, 2026[13]; DTA, 2025[14])

Even where standards are mandatory, teams need the right conditions to apply them, particularly for complex service journeys that span multiple organisations and channels. This is as much a capability and organisational challenge as a governance one. The conditions that make standards work in practice typically include:

- A central team in charge of disseminating and monitoring how the standards are applied across the administration;
- A named person with clear accountability for the quality and ongoing improvement of each service;
- Stable, multi-disciplinary teams, combining policy, design, technology and operations skills — with the time, funding and mandate to design and run services rather than deliver one-off projects;
- Delegated decision-making authority, so teams can resolve trade-offs and improve services without having to escalate every decision; and
- Practical, accessible support, shared templates, reusable design components, peer learning, networks of experts and light-touch expert guidance that makes it straightforward to apply standards well.

The OECD Good Practice Principles for Public Service Design and Delivery in the Digital Age makes these conditions explicit, emphasising clear accountability for each service, sustained multidisciplinary teams and consistent delivery methods supported by practical tools and training (OECD, 2022[8]). Putting these conditions into practice is hard, particularly in complex, resource-constrained settings. Strengthening implementation requires deliberate workforce planning, sustained investment in capability and senior leadership engagement. Some OECD countries are already acting: New Zealand is improving senior leadership decision-making to bring authority closer to multidisciplinary teams, while Israel is reviewing recruitment, career development and mobility pathways to support more collaborative ways of working.

Overall, the 2025 DGI results suggest that the challenge has shifted. Most OECD governments have defined what good services looks like. The harder and more pressing task is embedding those expectations in the decisions and routines that actually shape services, from investment approval and procurement choices to delivery stage reviews and ongoing improvement. Standards become useful when they are built into these processes and when teams have the support to apply them consistently.

5.3. User engagement in service design shows promise but needs to be more systemic

5.3.1. User engagement is progressing but remains uneven and fragile

Public services work best when they are designed around the people who actually use them. This sounds obvious, but it requires deliberate effort: the people who design and deliver services are rarely the same people who depend on them, and the assumptions that seem reasonable inside government often do not match the reality of people's lives. User engagement - systematically involving people in how services are designed, tested and improved - is how governments close this gap. It helps teams understand what people actually need rather than what they assume is needed, identify where services create unnecessary complexity or exclude certain groups, and make improvements based on evidence rather than guesswork. When engagement is done well and done consistently, it reduces the risk of building services that do not work for the people they are meant to serve, and increases the likelihood that digital investment delivers real improvements in people's experience of government.

Involving people in the design of public services has shifted from an unfamiliar idea to a recognised practice across OECD governments. Tools and methods for working with users – from interview and usability testing to co-design workshops and online consultations - are now widely available, and their use has grown significantly. This is an important step forward: without practical methods, engagement tends to remain rhetorical, limited to one-off consultations that happen too late to influence design choices. The widespread availability of these tools signals a more hands-on, evidence-based approach to service design.

However, having the tools is not the same as using them consistently. The harder challenge is turning user engagement from an occasional exercise into a regular part of how services are designed, run and improved – something that happens throughout the life of a service, not just at the start. The 2025 DGI results suggest that engagement is advancing on some dimensions but remains less consistently embedded in the ways that matter most for human-centred delivery.

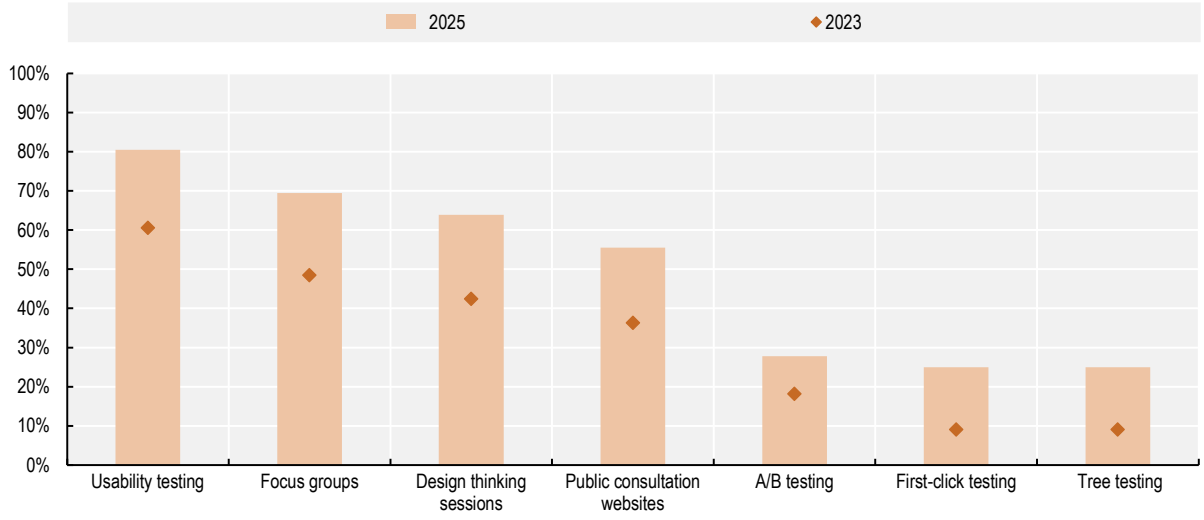
Who is involved is one gap**.** Methods to understand and involve users broadly are relatively widespread, but targeted engagement with people who face higher barriers to access, including illiterate people (11 of 36 countries, 31%), asylum seekers or refugees (11 of 36, 31%), indigenous communities (12 of 36, 33%) and low-income population groups (14 of 36, 39%), is less consistently in place. These are often the groups whose experience of services differs most from the average, and whose needs are most likely to be missed if engagement is not deliberately designed to include them.

Whether testing is routine is another. The 2025 DGI shows only moderate use of formal requirements or recommendations to test services with users (12 of 36, 33%) and/or service providers (12 of 36, 33%) before and after launch. Testing methods such as usability sessions, focus groups and online consultation tools are more widely available than they were in 2023, but they remain unevenly used across government (Figure 5.3). Where testing is not routine, problems with services, confusing navigation, inaccessible language, steps that work for some users but not others, tend to surface only after launch, when they are more costly and disruptive to fix.

Whether needs are tracked over time is a third gap. Engagement that happens only at the start of a project captures a snapshot of user needs rather than how those needs evolve as services are used, circumstances change and new issues emerge**.** Systematic tracking of user needs across the service lifecycle remains moderate (21 of 36, 58%).

Figure 5.3. Methods to test digital government services are not evenly used across OECD countries

Percentage of OECD countries reporting methods to test digital government services, by type, 2023 and 2025



Note: 2025 data not available for Germany and the United States. 2023 data not available for Germany, Greece, Slovak Republic, Switzerland and the United States. Refer to Annex Table 5.A.1 for comprehensive OECD and Accession country data. "A/B testing" refers to a user experience testing technique based on the comparison between two versions of a same product or service. "First-click testing" refers to a testing method for websites, apps or platforms which examines the 'first click' of the users when interacting the system, aiming to verify the success of completing a task. "Tree testing" is a user-research method used to check whether people can find information easily in a service, website, or app based on its structure and labels, not its visual design.

Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/6hxztj

These gaps become particularly important as governments introduce AI-enabled services. The 2025 DGI shows that user engagement is not yet consistently embedded in AI development: only 15 out of 35 OECD countries (42%) report engaging service users when developing AI policies or deploying AI in public services. This matters because feedback from real users is essential for ensuring that AI-enabled interactions are usable, accessible and trusted, and because problems with AI systems, such as bias or exclusion of certain groups, may only become visible through sustained engagement with a wide range of people. International engagement with AI is also limited: only 13 out of 36 OECD countries (36%) engage with counterparts in other countries on AI-related work beyond participation in international fora. Since AI standards, data practices and risks frequently cross borders, purely domestic approaches to engagement leave important gaps.

5.3.2. Making engagement repeatable requires shared enablers

A practical route to make engagement more consistent is to provide government-wide digital participation tools that any ministry or agency can use repeatedly when designing policies and services, standardising the basic process of involving users and reducing the effort to do it well (OECD, 2025[15]). The 2025 DGI results suggest that this enabling layer is only partly in place: only 17 out of 36 OECD countries (47%) report requirements to use digital participation tools when policies are being designed, and government-wide initiatives to encourage their use score at a moderate level.

Making engagement systemic require three connected shifts: setting clear expectations for user research and testing at key stages in service development; making participation practically feasible through shared recruitment, accessible formats and reusable research protocols; and providing enough specialist support that teams can plan and run engagement that reaches a wide range of people, translate findings into design decisions and repeat this process as a matter of routine rather than exceptional effort (Box 5.4).

Box 5.4. Making user engagement more consistent and effective

Several governments are moving from ad-hoc consultations toward more repeatable engagement practices – setting clearer expectations, making participation feasible at scale and reaching a wider range of people:

- The **United Kingdom** operationalise expectations for user research through published standards and guidance, backed by central governance arrangements including publicly available service standard assessment reports. This helps embed user research and testing as a routine part of service work rather than an optional extra.
- **Iceland** supports assessment of user needs at different stages of the service life through different resources, including at launch and throughout design and delivery. The Ísland.is Influencers initiative provides a structured way to recruit and involve users in testing before services are launched, and signposts multiple testing methods including usability testing, A/B testing, first-click testing and tree testing – making participation feasible at scale.
- **Canada** requires departments to maximise public engagement under the Policy and Directive on Communications and Federal Identity, alongside consultation requirements in specific legislative frameworks. Departments also draw on practical design guidance for engagement where no single standardised framework applies.
- The **Netherlands** supports participation and inclusion through the Alliance Digital Society, a sustained collaboration model that works directly with groups who face higher barriers to digital access. Practical measures include distributing refurbished devices, a free helpline for digital questions, and physical information points – helping engagement remain feasible and meaningful for people who might otherwise be left out.

Source: (GOV.UK, 2025[16]; GOV.UK, 2026[17]; Digital Iceland, n.d.[18]; island.is, 2024[19]; Government of Canada, 2025[20]; Government of Canada, 2026[21]; Alliance for Digital Living, 2026[22]).

Overall, the results suggest that user engagement is advancing in terms of available methods and stated commitments, but has not yet become consistently embedded in the ways that most shape service quality: reaching those who face higher barriers to access, making testing a routine expectation and tracking needs throughout the full life of a service.

5.4. Reliable services need joined-up delivery across channels, infrastructure and data sharing

Public services need to work reliably not just when everything goes as planned, but when people's circumstances change, demand increases or a channel becomes unavailable. A parent dealing with a sudden job loss, a family navigating a health crisis, or a business facing an unexpected regulatory change all depend on services remaining accessible, coherent and responsive precisely when the need is greatest. Reliability in these moments is not a bonus feature, it is what distinguishes a service that people can genuinely count on from one that works only in ideal conditions.

This kind of reliable, joined-up service delivery depends on three things working together: an approach to service delivery that works consistently across different channels; digital infrastructure that underpins continuity when circumstances change; and the ability to share data across agencies so that people do not have to repeat themselves as they move through service journeys.

5.4.1. Joined-up service delivery across channels

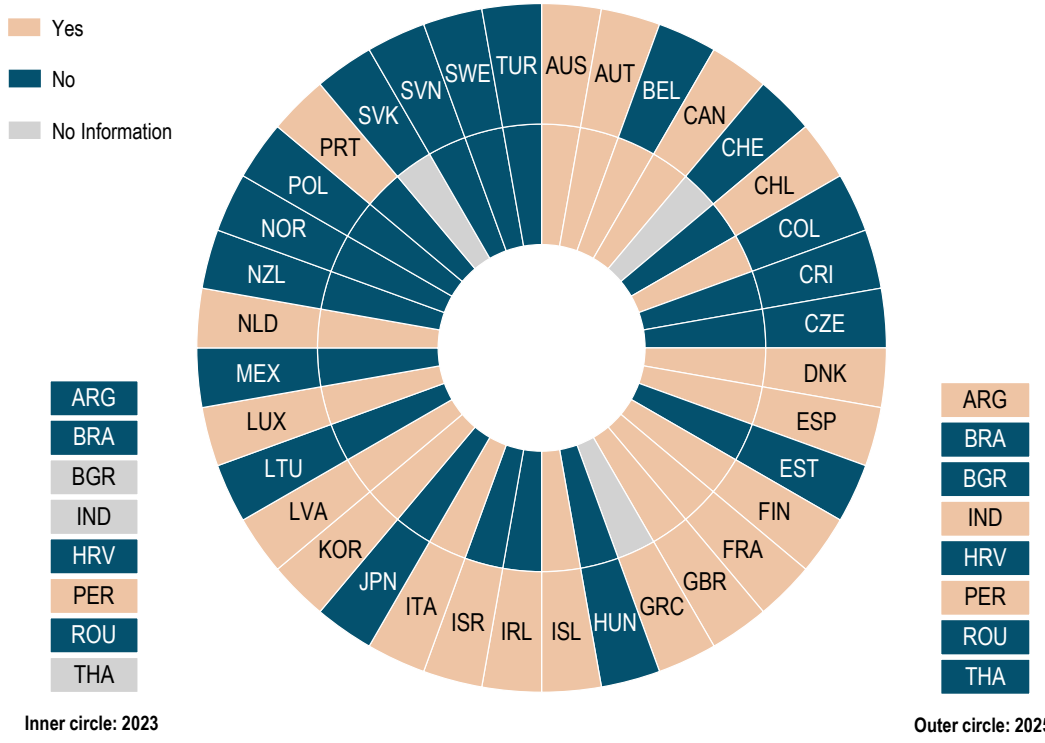
Most governments now offer services through multiple channels - online, by telephone, in person and increasingly through apps and assisted digital support. This gives people more options depending on how they prefer to access services. The OECD Risk That Matter Survey 2024 data show that while just over half of respondents report using digital tools to access

government services most of the time, four in ten say they would prefer in-person or paper-based options (OECD, 2025[2]). But offering multiple channels is not the same as delivering a joined-up experience across them. The real test is whether someone can start a process in one channel and continue it in another without losing their place, repeating information or having to navigate a system that cannot recognise them. This matters because, even where service delivery is principally online, a significant share of people still relies on, or prefer, human and paper-based channels. This is particularly important for services that affect rights, entitlements or legal status, where a failed handover can have consequences beyond inconvenience, including missed deadlines, loss of access to support or difficulties exercising rights. Designing services that truly work across channels is therefore not a transitional issue, but a core requirement for human-centred service delivery.

Many governments have strengthened the entry points to their services: service catalogues are more widely available (31 of 36 countries, 86%) – often complemented by single information and/or service delivery platforms – and channel options are more clearly signposted (26 of 31 countries with service catalogues, 83%). But the 2025 DGI results suggest that a clear, government-wide approach to managing how channels relate to one another - what is often called an omni-channel strategy - is still missing in many countries. An omni-channel approach means designing services so that all channels work together as a coherent system: users can move between them smoothly, the quality of the experience is consistent regardless of how they access a service, and no channel is treated as secondary or disconnected. Only 19 out of 36 OECD countries (53%) have such an omni-channel strategy (Figure 5.4).

Figure 5.4. Only half of OECD countries have a government-wide omni-channel strategy

Countries reporting government strategy for omni-channel service delivery approaches, 2023 and 2025



Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023. An omni-channel approach is defined as one in which all channels for services work together as a coherent system: users can move between them smoothly, the quality of the experience is consistent regardless of how they access a service, and no channel is treated as secondary or disconnected.

Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/4m1pos

Even where an omni-channel approach exists, the practical details of how channels are organised and positioned are not consistently defined across government, e.g. which services can be completed fully online, where telephone or in-person support is needed, how national and sub-national channels are aligned, and how channels and services across different sectors of the public administration are connected and interoperable. Without this clarity, expanding the number of channels can actually make things harder for users, adding more entry points without reducing the complexity of navigating between them.

Building a joined-up approach across channels requires at least three practical commitments. First, treating priority service journeys as end-to-end experiences that span multiple organisations and channels, rather than as separate transactions owned by individual agencies or specific sectors. Second, being explicit about what the channel is for (e.g. what can be completed digitally from start to finish, what requires assisted support, and what requires an in person interaction) and designing clear handovers between them. Third, putting in place continuity mechanisms so that people do not have to start over when they switch channels: this includes identity systems that work across touchpoints, appropriate data sharing between agencies and clear accountability for who takes over when an interaction moves from one channel or organisation to another (Box 5.5).

Box 5.5. Designing joined-up service journeys across channels

Several governments are making their approach to channel delivery more explicit, helping people move between channels without losing progress or having to repeat information:

- **Australia** positions its omni-channel approach within the Data and Digital Government Strategy, with expectations for non-digital access reflected in standards including the Digital Service Standard and Digital Inclusion Standard. myGov serves as a primary entry point, with guidance and standards supporting consistent service delivery patterns across channels.
- **Portugal's** Decree-Law 49/2024 defines how public service channels should be integrated to support an omni-channel approach, enabling citizens and businesses to start a service through one channel and continue it through another according to their needs, while supporting a unified customer service experience.
- **Korea's** Government24 (Gov.kr) is an integrated channel for government services, linked to the Electronic Government Act's provisions on integrated service windows. It provides clear guidance on which services can be completed online and which require in-person steps, supporting clear handovers between channels.
- **Israel's** GOV.IL and MyGov.il consolidate government services and information through a unified digital entry point, with structured routes for different service types and clear signposting for contact and assistance.

Source: (DTA, 2025[14]; Presidency of the Council of Ministers (Portugal), 2024[23]; gov.pt, 2026[24]; Ministry of the Interior and Safety (Republic of Korea), 2026[25]; Government of Israel, 2026[26])

5.4.2. Digital public infrastructure as a foundation for continuity

Joined-up channel delivery depends on the digital infrastructure that sits behind it. When someone moves from one channel to another, or from one agency to another, the systems that support those interactions need to be able to recognise them, reuse the information they have already provided and maintain continuity of their service journey. Without this, even a well-designed omni-channel approach breaks down at the handover.

Digital identity is particularly important here. A widely used digital identity system allows services to recognise the same person across channels and agencies, so users do not have to re-establish who they are or re-submit information they have already provided. Where digital identity is widely adopted, agencies can reuse verified information for eligibility checks and case continuity, supporting simpler journeys and faster resolution of requests. As shown in chapter 2, most OECD countries have a digital identity strategy and the key governance arrangements in place, but the share of services that can actually be accessed using digital identity, and the share of the population that uses it, remain more limited. This gap matters in practice: where digital identity does not reach most services and users, the continuity it could provide cannot be realised. Addressing this gap requires shifting focus from formal frameworks to widespread use in practice, by embedding digital identity across service portfolios, improving user experience and trust, and creating clearer incentives for both institutions and users to rely on digital identity in routine service interactions (see Chapter 2, Section 2.3 on the governance of digital identity).

Other components of DPI also contribute to continuity and responsiveness. Authoritative data registries – official records of key information such as population data, business details and addresses – help agencies access core data in consistent ways, reducing the need for manual checks or duplicate requests when a case moves between organisations. Common notification and messaging tools allow agencies to communicate reliably with people through alternative channels when primary channels are unavailable. Shared payment systems support faster and more reliable delivery of financial support. Taken together, these components make it easier to reroute service journeys when needed, reducing single points of failure and enabling faster, more reliable handovers (see Chapter 2, Section 2.1 on DPI building blocks).

5.4.3. Data sharing to support joined-up journeys

The third element of reliable, joined-up service delivery is the ability to link and share data across government institutions and sectors — including, where appropriate, personally identifiable information that allows organisations to recognise the same user across different line ministries or agencies. Many public services involve interactions with multiple entities, each of which may require the same supporting information, such as proof of identity, household details, or income. Without effective data sharing, users are asked to re-submit evidence at each step that government already holds elsewhere. When data can be linked and shared securely, with appropriate governance and safeguards, the experience becomes simpler and more coherent, allowing people to progress through a service journey without unnecessary duplication — and enabling governments to identify needs, verify eligibility, and coordinate responses across organisational boundaries.

The 2025 DGI results suggest that the enabling conditions are partly in place but actual use lags behind formal requirements. Requirements to share data across public sector institutions are relatively strong, with 79% of OECD countries reporting such requirements. But in practice, on average only 63% of central government institutions and 58% of subnational governments institutions in countries with a data sharing system are actively using it. Chapter 2 previously identified the challenge that, while legal frameworks and strategies are in place, incentives, operational integration, skills and accountability mechanisms to embed interoperability in day-to-day service delivery remain uneven. This gap between having a system and using it matters: when handovers depend on data sharing that is technically available but not consistently used in practice, the burden falls back on the person accessing the service, who must re-submit evidence and navigate a system that cannot join up what it knows (see Chapter 2, Section 2.5 on interoperability). Some governments are also embedding consent management into their digital public infrastructure, enabling individuals to authorise, monitor and revoke data sharing in ways that can facilitate trusted data reuse across interconnected services (OECD, forthcoming[27]).

Taken together, these three elements - joined-up channel design, widely used digital infrastructure and trusted data-sharing arrangements - are mutually reinforcing. Strengthening any one of them without the others produces only partial improvement. A clear channel strategy without digital identity means users still have to re-identify themselves at each touchpoint. Digital identity without data sharing means agencies can recognise a person but cannot act on what they know. Data sharing without clear channel design means information flows but the user experience may remain fragmented. Where services are genuinely proactive, anticipating needs and reaching people directly, the choice of channel or access mechanism becomes less critical, as the burden of navigating the system shifts from the user to the state.

5.5. Proactive services: Reducing burdens by anticipating needs

Most public services today are reactive: people must know what they are entitled to and how to apply for it. This places the burden of navigating government on people or business, and it does not fall equally. People who are less familiar with government systems, who face language barriers, who are under stress or who simply do not know what support is available may not apply at all, apply too late or give up partway through (OECD, 2024[5]). The result is avoidable non-take-up: support that exists but does not reach the people who need it.

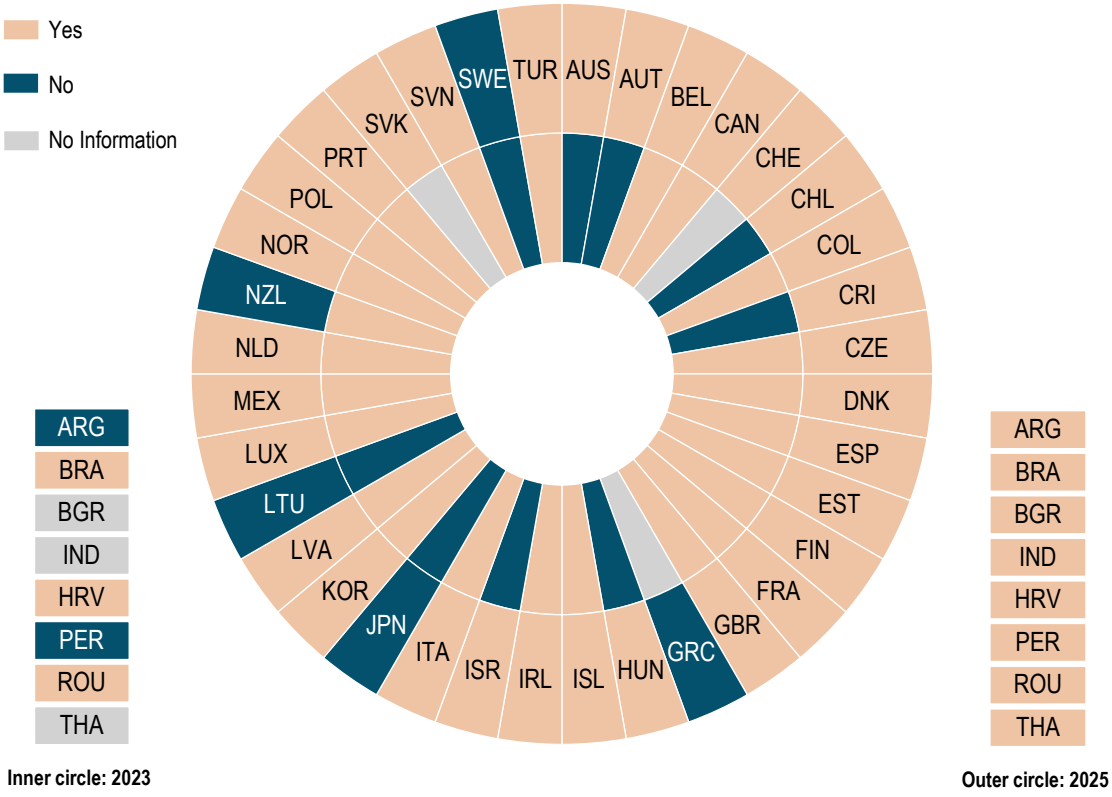
Proactive services address this by shifting the default. Rather than waiting for people to come forward, government acts on what it already knows - identifying likely eligibility, pre-filling information, sending timely reminders or delivering benefits automatically when conditions are met. This is not simply a convenience improvement. It is a matter of fairness: proactive approaches help ensure that support reaches those who need it, not just those who successfully navigate the system.

Proactivity also reduces unnecessary work on both sides. When services rely on repeated form-filling and manual verification, government incurs avoidable workload through incomplete applications, duplicate checks and administrative back-and-forth. When services can reuse information, anticipate needs and automate routine steps where appropriate, both people and government save time and effort.

The 2025 DGI results show that proactiveness ranks fifth among the six dimensions of the Digital Government Policy Framework, indicating that many governments remain stronger at strategy and digital delivery foundations than at enabling services to anticipate needs or simplify interactions by default (Figure 5.5). The reason is not primarily lack of ambition, it is (in part) that proactivity depends on capabilities that are hard to scale through isolated projects: shared systems, interoperable infrastructure and the ability to reuse data safely across agencies. In addition, more proactive models can have significant fiscal implications: when governments actively identify and reach all individuals who are eligible for a service or benefit, take-up increases by design, requiring budgets and funding models to anticipate and absorb higher, more visible demand.

Figure 5.5. Most governments recognise proactive service delivery as an operational goal

Countries acknowledging proactive service delivery as an operational goal, 2023 and 2025



Note: "Yes" includes either a stand-alone strategy or inclusion in a wider strategy. 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/vo6dnh

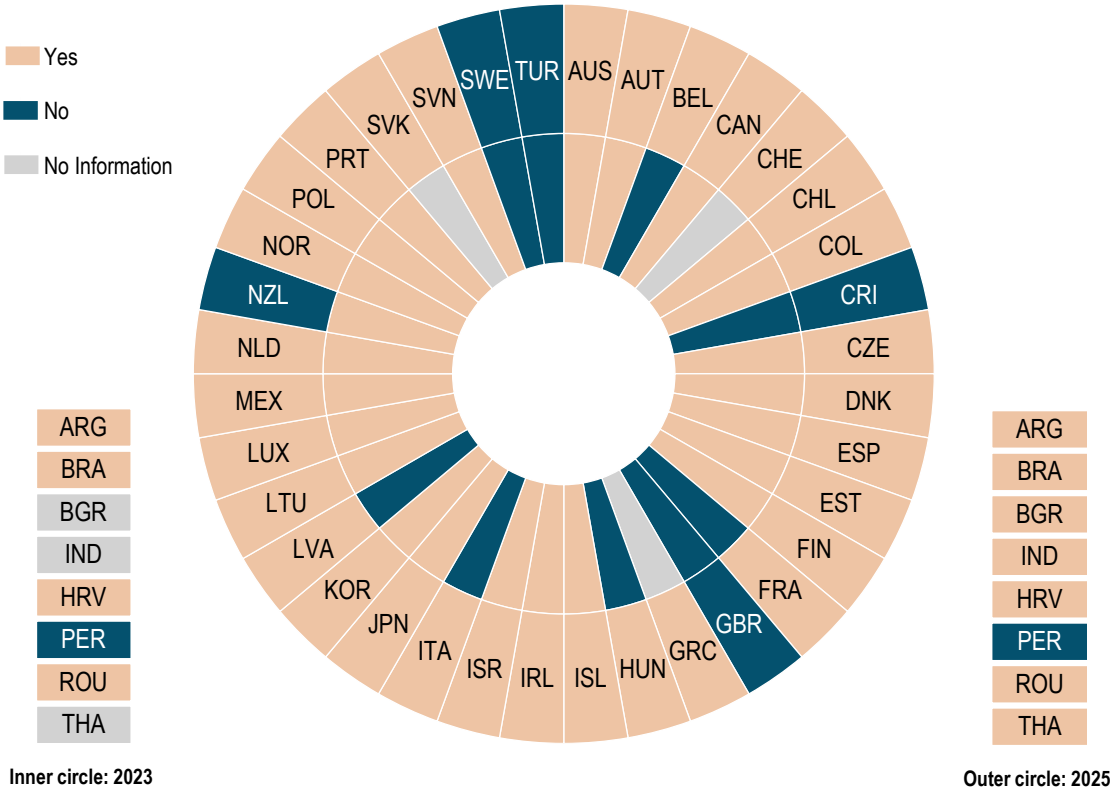
Three practical levers can help governments make meaningful progress.

5.5.1. Moving the once-only principle from policy to practice

The once-only principle - the commitment that government should not ask people to provide the same information more than once - is widely recognised across OECD countries and referenced in many national strategies (Figure 5.6). But recognition in a strategy document is a long way from embedding it as a routine feature of how services are delivered.

Figure 5.6. Wide recognition of the "once-only" principle has yet to translate into routine practice

Countries recognising the "once-only" principle, 2023 and 2025



Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/g4qpfo

Making the "once-only" principle work in practice requires a set of operational practices that many governments have not yet made consistently: which information can be reused and under what legal basis; what safeguards and consent arrangements apply; which technical mechanisms – shared data registries, data exchange platform, standardised verification processes – will handle the reuse; and how compliance will be checked when new services are designed. Without these foundations, service teams are left to negotiate case-by-case data sharing arrangements or rely on manual workarounds, both of which reintroduce the burden and fragmentation that the once-only principle is meant to eliminate.

The goal is to make once-only the default, not the exception: where information can be reused, it should be; where it cannot not, the reason should be clear and the technical pathway for verification and reuse should be available as a shred resource rather than something each team has to build from scratch (Box 5.6).

Box 5.6. Making the once-only principle operational

Several governments are moving from recognising the once-only principle to embedding it as a delivery requirement:

- **Belgium**'s Only Once Act requires federal public services to reuse information already held in official registers such as the National Register and the Crossroads Bank for Enterprises - rather than asking people to provide it again. New forms must be reviewed before use by a simplification service that can require changes. People and businesses can report non-compliant forms for review.
- **Greece** supports once-only delivery through a dedicated Once-Only Technical System and the Once-Only Hub. New digital services are expected to address compliance with interoperability and once-only requirements as part of project approval, aligned with the gov.gr development frameworks.
- **Spain** enables cross agency verification through a Data Intermediation Platform, used under collaboration agreements between administrations. This is linked to the legal framework for administrative procedure, allowing public bodies to verify information directly rather than asking people to submit it again.
- **Korea** anchors its once-only approach in the Electronic Government Act and links it to project approval and budget governance, including reviews under the Framework Act on Intelligent Informatization – creating a direct connection between the once-only principle and how digital projects are approved and funded.

Source: (FPS BOSA, 2024[28]; Ministry of Digital Governance (Greece), 2022[29]; Ministry of Digital Governance (Greece), 2024[30]; Head of State (Spain), 2015[31]; Ministry of Government Legislation (Korea), 2026[32])

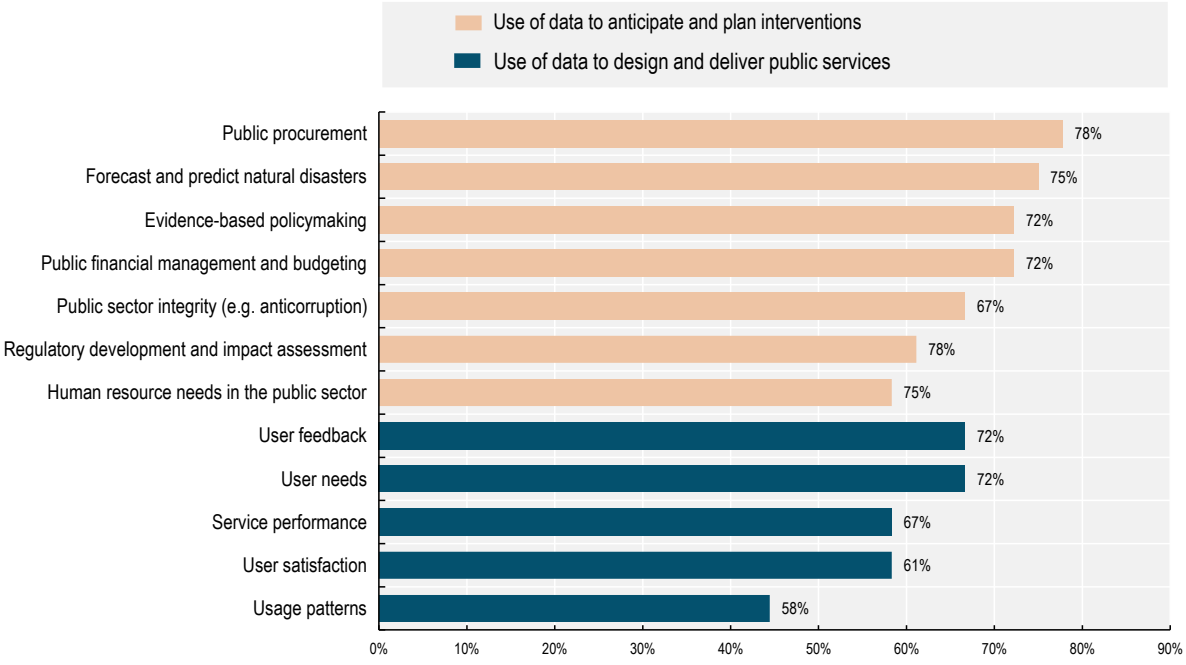
5.5.2. Using data to improve service delivery

Governments collect and analyse large amounts of data about how services are used, who accesses them and what outcomes they produce. But there is an important difference between using data to understand what is happening and using data to change what happens at the point of service delivery. Proactivity becomes real when information shapes the actual decisions made in service operations - eligibility checks, case transitions, notifications, targeted outreach - not just the reports that managers read afterwards.

The 2025 DGI results point to a mixed progress here. Governments report relatively stronger use of data to anticipate and plan government interventions at a strategic level – informing budgeting, policy design and resource allocation. But the operational use of data to design and deliver services – using real time information to route people faster, identify emerging needs or trigger proactive support – remains less mature, albeit still fairly common (Figure 5.7). This gap is partly structural: strategic uses of data can be developed centrally by analytical teams, while operational uses require data to be integrated into the systems, processes and day-to-day workflows of the people delivering services.

Figure 5.7. Governments are better at using data for strategy than for day-to-day service delivery

Percentage of OECD countries reporting government-wide initiatives to use data to anticipate and plan interventions and making government-wide use of data to design and deliver public services, by area, 2025



Note: Data not available for Germany or the United States. Refer to Annex Table 5.A.1 and Annex Table 5.A.2 for comprehensive OECD and Accession country data.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/e04y1i

Shifting data use from reporting and planning into service operations requires investment in the tools, skills and governance arrangements that make operational data accessible and actionable. It also requires clear safeguards: data used to identify eligible people, predict needs or tailor communication must be governed transparently, with appropriate protections against bias, inappropriate inference or exclusion of particular groups. Proactivity built on skewed data risks causing harm rather than reducing burden (Box 5.7).

Box 5.7. Using data to anticipate needs and improve planning

Proactivity often starts with responding to early signals. Several governments therefore strengthened how they use data to anticipate needs and plan interventions, including:

- **Australia** uses linked and longitudinal data to support targeted interventions and planning, including through the Life Course Data Initiative and place-based initiatives. Evaluation reporting supports evidence-informed decisions about where to prioritise action.
- **Estonia** uses a smart text search solution to support preparation of policy decisions. Legislative drafting rules also require explanatory notes to include an assessment of the expected impact of proposed legislation, reinforcing an evidence-based approach to policy design.
- **Greece** is developing a central hub for managing and analysing large datasets under the Greece 2.0 recovery plan, supporting strategic decision-making and strengthening the evidence base for regulation and policy analysis.
- **Finland** uses government-wide information management approaches to support better decisions in complex environments, including the Tietokiri tool and structured approaches to impact assessment when drafting legislation.
- **United Kingdom (London).** Five local authorities collaborated through the InnOvaTe Programme to apply real-time sensor data for earlier and more targeted local interventions. Across 47 trials, more than 2 900 sensors fed into a shared platform generating actionable insights, supporting use cases such as early flood alerts, identifying under-used buildings and reducing fly-tipping.

Source: (Australian Bureau of Statistics, 2026[33]; Australian Department of Social Services, 2025[34]; Australian Department of the Treasury, 2025[35]; Government Office of Estonia, 2026[36]; Ministry of Digital Governance (Greece), 2022[37]; Ministry of Finance (Finland), n.d.[38]; Finnish State Treasury, 2024[39]; OECD, 2024[40])

5.5.3. Using AI to make timely support the default

AI can help governments move from reactive to proactive service delivery in practical ways (OECD, 2025[41]; OECD, 2025[42]) (see also Chapter 4):

- improving triage and routing, so people are guided to the right pathway earlier (for example, by identifying the most relevant service, channel or follow-up step);
- supporting more personalised and timely communication, such as targeted reminders, nudges or status updates that reduce missed deadlines and prevent avoidable drop-out while maintaining fairness, accessibility and clear explanation;
- helping administrations identify patterns that indicate emerging needs or service frictions, including spikes in unresolved cases, bottlenecks, repeated contacts or signals of exclusion risks.

Used well, AI can make timely, targeted support the default rather than something people must find and request themselves. Delivering more timely support means aligning AI capability-building with changes to how work is organised, integrating AI into operations, clarifying responsibilities between people and systems, and empowering staff to act on AI outputs. At the same time, AI can introduce real risks such as opacity, skewed data and inappropriate automation. Where AI is used for a clear public purpose with human oversight and safeguards that are proportionate to risk, it can help reimagine how proactive public service looks: strengthening the responsiveness of service operations by turning data signals into earlier action and helping staff focus attention where it is needed most (Box 5.8).

Box 5.8. Applying AI to strengthen proactive services

- **France**'s Compar: IA enables comparison of AI language models in French, collecting user preferences that are turned into open datasets. This supports public bodies in evaluating and selecting AI models that meet national requirements, building the evidence base for responsible AI adoption in government.
- **Luxembourg** uses AI through its AI4Gov portfolio for two types of proactive support: identifying unusual patterns in municipal financial data to flag potential irregularities, and profiling to help employment advisers assess which jobseekers are likely to need which type of support to access employment.
- **Spain** uses AI in forest fire management: the Arbaria system uses AI and historical fire data to predict fire behaviour and inform both preventive and reactive decisions, helping authorities act earlier and more effectively.
- **Korea**'s Ministry of the Interior and Safety (MOIS) has piloted an AI-based telephone monitoring system that proactively contacts potentially vulnerable people, analyses responses to identify signs of risk and triggers rapid human follow-up. The initiative aims to reduce routine administrative workload while improving early detection for groups such as older people living alone and low-income households. (OECD, 2025[43])

Source: (Ministry of Culture (France), 2025[44]; Ministry of Digitalization (Luxembourg), 2025[45]; Government of Spain, 2022[46]; OECD, 2025[43])

Proactivity is not a single programme or technology, it is a shift in how service delivery is organised. Governments can make the most progress by focusing on three connected moves: turning once-only from a principle into a practical delivery default that service teams can apply consistently; shifting data use from reporting and planning into the operational processes where services are delivered; and using AI as a tool to make timely, targeted support the norm rather than something people must find and request on their own.

5.6. Stronger feedback loops are needed to drive continuous improvement

Everything described in this chapter - consistent service standards, meaningful user engagement, joined-up channel delivery, proactive services - depends on governments having reliable information about whether their services are actually working. Without this, it is difficult to know where improvements are most needed, whether changes are making a difference, or whether digital investment is delivering real benefits for people. Feedback loops - the mechanisms that connect evidence about service performance to the decisions that shape services - are what make improvement sustainable rather than occasional

The 2025 DGI results suggests that this remains a weak link for many governments. Most OECD countries include monitoring of user experience in their national digital government strategy – 26 out of 36 OECD countries (72%). But including it in a strategy is different from measuring it systematically and acting on what is found. The evidence points to measurement that is often partial, inconsistent and not sufficiently connected to the decisions that matter, with 21 out of 36 countries (58%) doing systematic tracking of user needs across the service lifecycle.

5.6.1. Monitoring is common, but what is being measured matters

Tracking whether services are meeting their objectives is a basic management function, and most OECD governments have some form of service monitoring in place. But two important questions are whether monitoring captures the right things and whether it is connected to improvement.

Much current monitoring focuses on process and output, whether a service launched on time, whether a milestone was met, whether a form was completed. This kind of information is useful for basic accountability but does not tell governments much about whether services are working well for the people who use them.

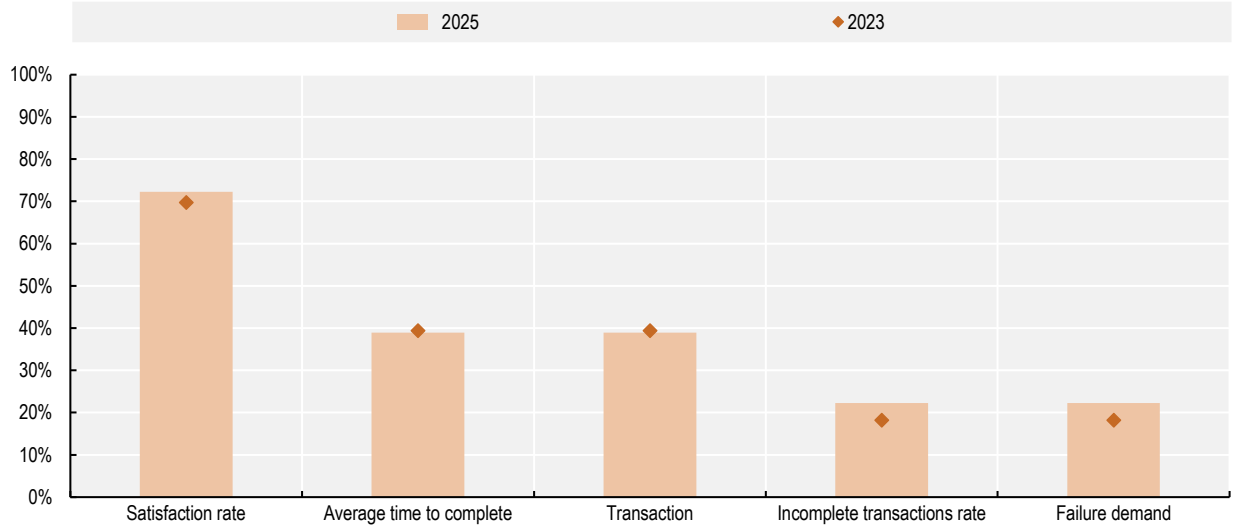
Monitoring that captures user experience - how easy a service was to use, where people got stuck, whether they found what they needed - provides a much more useful basis for improvement.

The 2025 DGI results show that the use of indicators to measure service performance remains low across OECD countries (Figure 5.8). This is a significant gap: without consistent measurement of service performance, governments are operating with limited visibility when they try to prioritise improvements, allocate resources or make the case for investment in service transformation.

Additionally, OECD Serving Citizens Survey results show that only around one third of countries require delivery targets across central government, while a similar share report having no such targets at all (OECD, 2025[47]; OECD, forthcoming[48]). Taken together, the results suggest that measurement is often partial, uneven and insufficiently standardised to support comparison, targeting and decision-making across government. Nonetheless, countries are advancing in government-wide efforts to measure satisfaction with public services, as noted in Box 5.9.

Figure 5.8. Service monitoring is widespread, but meaningful performance measurement remains limited

Percentage of OECD countries reporting measurement of digital service performance and transaction costs, by type, 2023 and 2025



Note: 2025 data not available for Germany and the United States. 2023 data not available for Germany, Greece, Slovak Republic, Switzerland and the United States. Refer to Annex Table 5.A.1. for comprehensive OECD and Accession country data.
Source: OECD (2025) Survey on Digital Government 3.0.

StatLink https://stat.link/r1ojs3

Public transparency about service performance is also limited. Only 17 out of 36 countries (48%) publish progress or monitoring data about digital project online – up from 39% in 2023, which is a positive trend, but still meaning that in more than half of OECD countries, there is no routine public window onto how major services are performing. Greater transparency would support external scrutiny, encourage shared learning across government and strengthen public accountability for service quality.

Box 5.9. Government-wide efforts to measure user satisfaction with public services across OECD countries

Chile's User Satisfaction Survey (MESU) is one of the largest user experience surveys across OECD countries. Overseen by the Ministry of Finance, it is mandatory for a broad set of public institutions — 68 agencies participated in 2024, with around 60,000 users responding. MESU produces an overall satisfaction score for each agency and captures experiences across specific dimensions such as accessibility, infrastructure quality, and treatment of users. Chile is progressively strengthening the link between survey results and service improvement: many agencies are required to develop satisfaction improvement plans informed by MESU, and performance-related pay is available to those that meet agreed targets, reinforcing the role of citizen feedback in driving organisational change.

Australia's Trust in Australian Public Services (TAPS) survey measures public satisfaction, trust, and experiences with public services. Led by the Australian Public Service Commission, the 2024 wave collected more than 11,000 responses and found that trust in the public service remained stable at 58%. A distinctive feature of TAPS is its emphasis on demographic disaggregation, revealing systematic differences in trust by gender and age — for example, higher trust among men (63%) than women (53%), and among younger and older adults compared with middle-aged cohorts. The survey also examines five core dimensions of service experience: staff, information, access, process, and outcomes.

Source: (OECD, forthcoming[48]; OECD, 2025[49])

5.6.2. Measuring what services cost people, not just what they cost government

One of the most informative — and underused — forms of service measurement is tracking the costs that services impose on the people who use them. These transaction costs include the time spent completing a service, the number of steps required, the documents that need to be gathered, the handovers between agencies and the occasions when people have to contact government again because something went wrong the first time. A service can appear efficient from the inside while still imposing significant burdens on users.

Only 10 out of 36 OECD countries (28%) report standardised mechanisms or guidance for measuring transaction costs. This is a genuinely low figure — and it means that in most OECD countries, governments do not have a consistent way of knowing where burdens concentrate, which groups are most affected, or which parts of a service journey create the most avoidable frustration or dropout.

Measuring transaction costs systematically has three benefits. It reveals where services impose the highest burdens, helping governments prioritise where to focus improvement efforts. It identifies which user groups are most affected, supporting more equitable service design. And it provides a common metric that can be tracked over time, making it possible to demonstrate the impact of simplification and digitalisation in terms that are meaningful to both decision-makers and the public (Box 5.10).

Box 5.10. Measuring what services cost people

Several governments have developed standardised approaches to measuring the costs and burdens that services impose on users, making improvements more targeted and demonstrable.

- The **United Kingdom** requires central government service teams to calculate cost per transaction across all available channels – including assisted digital support – and publish this data regularly. This creates a consistent, comparable measure of efficiency and burden that connects to service improvement decisions.
- **Portugal** provides guidance and a practical tool that support public bodies in calculating the benefits and savings linked to digital transformation and service simplification. This makes transaction cost measurement more feasible and repeatable across organisations of different seizes and capacities.
- **Colombia** calculates "citizen savings" from the simplification of administrative procedures using a defined methodology, drawing on data from its national system for tracking administrative requirements. Savings are weighted depending on the type of simplification action taken, producing a quantified estimate of the burden reduction achieved.
- **Iceland** uses a standardised approach (*Ávinningur af stafrænum ferlum*) to calculate the benefits of digital processes, focusing on changes in efficiency and cost. Agencies are encouraged to use a dedicated tool and report a standard indicator, supporting a consistent measurement across government.

Source: (GOV.UK, 2021[50]; ARTE, n.d.[51]; Administrative Department of the Public Service (Colombia), 2022[52]; Digital Iceland, n.d.[53])

5.6.3. Connecting measurement to decisions

Measurement only improves services when it changes what people decide. The risk with any monitoring or reporting system is that it becomes something that is observed but not acted upon, for example dashboards that exist but do not drive change, reports that are filed but not discussed. The core challenge is the lack of incentives for civil servants to act on the evidence they gather. The OECD Serving Citizens Survey results indicate that only half of countries incorporate user experience and performance data into their decision-making process to improve services (OECD, 2025[47]). Avoiding this requires explicit pathways from evidence to action.

Practically, this means building measurement into the decision points that shape services. Service performance data should be reviewed alongside investment proposals, so that evidence of how existing services are performing informs decisions about where to invest next. It should trigger service redesign when performance falls below acceptable levels, depending on the outcomes for users, or when user burdens, drop off or accessibility issues are identified. It should feed into assurance processes and go-live decisions for major services, so that new services are not launched without a clear plan for how their performance will be tracked.

It also means designing measurement as a tool for learning rather than a compliance exercise. When teams see measurement as something done for them rather than to them, as a source of insight that helps them improve their work rather than a reporting burden imposed from outside, they are more likely to engage with it seriously and use it well. This requires measurement to be proportionate, accessible and connected to issues that teams can actually act on. A simple, regular user experience survey for a high-volume service is more useful than an elaborate measurement framework that takes months to produce and arrives too late to influence decisions.

Finally, measurement needs to be connected to the governance and accountability structures that give it force. If service teams know that evidence of poor performance will prompt support and improvement rather than punishment, they are more likely to collect honest data and report it accurately. Building a culture where measurement is valued as a management tool, rather than feared as a means of blame, is as important as having the right indicators and systems in place.

Ultimately, stronger feedback loops make continuous improvement possible rather than exceptional. When evidence about outcomes, user experience and transaction costs is collected consistently, reported transparently and connected to the decisions that shape services, improvement becomes part of how governments operate, not a special initiative that depends on exceptional teams or circumstances. This is what it means for service transformation to be sustainable: not a series of one-off projects, but a system that learn, adapts and gets better over time.

Annex 5.A. Additional tables with country data

Annex Table 5.A.1. Availability of service standards (*) and selected associated goals, 2025

Availability of whole-of-government service standard or guidelines on service design and delivery at the central/federal level (*); and if yes, associated goals these common guidelines or the service standard

Country	Availability of service standards*	Understand user needs or expectations	Equip teams for service quality	Engage users in service design	Ensure transparency	Use digital and data	Increase strategic use of data	Implement an omni-channel approach	Facilitate cross-border services	Encourage greening efforts	Encourage consistent methodology	Curate scalable tools, resources and practices
Australia	●	●	●	●	●	●	●	●	●	●	●	○
Austria	●	○	●	○	○	○	○	○	○	●	○	○
Belgium	●	●	●	●	●	●	○	○	○	○	○	●
Canada	●	●	●	●	●	●	●	●	○	●	●	●
Chile	●	●	●	●	●	●	●	●	○	●	○	●
Colombia	●	●	●	●	●	●	●	●	○	●	●	●
Costa Rica	○	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Czechia	●	●	●	●	●	●	●	●	○	●	○	●
Denmark	●	●	●	●	○	○	○	○	●	●	○	●
Estonia	●	●	●	●	●	●	●	●	●	●	●	●
Finland	●	●	●	●	○	●	●	○	○	●	○	●
France	●	●	●	●	●	●	○	○	○	●	○	●
Greece	●	●	●	●	●	●	●	●	●	●	○	●
Hungary	●	●	●	●	●	●	●	●	○	●	○	●
Iceland	●	●	●	●	○	●	○	●	○	●	●	●
Ireland	●	●	●	●	●	●	●	○	○	●	○	●
Israel	●	●	●	○	●	●	●	●	○	●	●	●
Italy	●	●	●	●	●	●	●	●	●	●	○	●
Japan	●	●	●	●	●	●	●	●	○	●	○	●
Korea	●	●	●	●	●	●	●	●	○	●	●	●
Latvia	●	●	●	●	●	●	○	●	●	●	○	○
Lithuania	○	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Luxembourg	○	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Mexico	●	●	●	○	●	●	●	○	○	●	○	●
Netherlands	●	●	●	●	○	●	○	●	○	●	○	○
New Zealand	●	●	●	●	●	●	●	○	○	○	○	○
Norway	●	●	●	●	●	●	●	●	●	●	●	●
Poland	○	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Portugal	●	●	●	●	●	●	●	●	●	●	○	●
Slovak Republic	●	●	●	●	●	●	●	●	○	●	○	●
Slovenia	●	●	●	●	●	●	●	○	○	○	○	○
Spain	●	●	●	○	○	●	○	○	○	○	●	○
Sweden	●	●	○	●	●	●	●	○	●	○	○	○
Switzerland	●	●	●	●	●	●	●	●	○	●	●	●
Türkiye	●	●	○	○	○	●	○	○	○	●	○	○

Country	Availability of service standards*	Understand user needs or expectations	Equip teams for service quality	Engage users in service design	Ensure transparency	Use digital and data	Increase strategic use of data	Implement an omni-channel approach	Facilitate cross-border services	Encourage greening efforts	Encourage consistent methodology	Curate scalable tools, resources and practices
United Kingdom	●	●	●	●	●	●	●	●	●	●	●	●
OECD Total												
● Yes	32	31	30	27	25	30	23	20	10	27	11	23
○ No	4	1	2	5	7	2	9	12	22	5	21	9
No information	0	4	4	4	4	4	4	4	4	4	4	4
Argentina	●	●	●	○	●	●	○	○	○	●	○	●
Brazil	●	●	●	●	●	●	●	●	●	○	●	●
Bulgaria	○	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Croatia	●	●	●	●	○	●	●	○	●	○	○	○
Indonesia	●	●	○	●	●	●	○	○	○	●	○	○
Peru	●	●	●	●	●	●	●	●	●	●	●	●
Romania	○	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Thailand	○	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Note: 2025 data not available for Germany and the United States.
Source: OECD (2025) Survey on Digital Government 3.0.

Annex Table 5.A.2. Countries reporting support mechanisms for application of service standards, by type

What mechanisms are in place to support the application of these common guidelines or service standards?

Country	Legal and regulatory framework		Approval or funding of new projects		Awareness raising		Digital skills development	
	2023	2025	2023	2025	2023	2025	2023	2025
Australia	○	●	●	●	○	●	●	●
Austria	●	●	○	○	○	○	○	○
Belgium	○	○	○	○	●	●	●	●
Canada	●	●	●	●	●	●	●	●
Chile	○	●	●	●	●	●	○	●
Colombia	●	●	○	○	●	●	●	●
Costa Rica	○	○	○	○	○	○	○	○
Czechia	●	●	●	●	○	●	○	●
Denmark	○	○	●	●	●	●	●	●
Estonia	●	●	○	●	○	○	●	●
Finland	●	●	○	○	●	●	○	○
France	○	●	●	●	○	●	○	●
Greece	N/A	●	N/A	●	N/A	●	N/A	●
Hungary	○	●	○	○	○	○	○	○
Iceland	○	○	●	●	●	●	●	●
Ireland	○	●	○	●	●	●	●	●
Israel	●	●	○	○	○	○	○	○
Italy	●	●	○	●	○	○	○	○
Japan	○	●	●	●	●	●	●	●
Korea	●	●	●	●	●	●	●	●
Latvia	●	●	○	○	○	○	○	○

Country	Legal and regulatory framework		Approval or funding of new projects		Awareness raising		Digital skills development	
	2023	2025	2023	2025	2023	2025	2023	2025
Lithuania	○	○	●	○	○	○	○	○
Luxembourg	●	●	○	○	○	○	○	○
Mexico	●	●	●	●	●	●	●	●
Netherlands	○	○	○	○	○	○	○	○
New Zealand	○	○	○	○	●	○	○	○
Norway	●	●	●	●	●	●	●	●
Poland	○	○	○	○	○	○	○	○
Portugal	○	●	○	●	●	●	○	○
Slovak Republic	N/A	●	N/A	●	N/A	●	N/A	●
Slovenia	○	○	●	●	●	●	●	●
Spain	○	●	○	○	○	●	○	●
Sweden	○	○	○	○	●	●	○	○
Switzerland	N/A	●	N/A	●	N/A	●	N/A	●
Türkiye	○	●	○	○	○	○	○	○
United Kingdom	○	●	●	●	●	●	●	●
OECD Total								
● Yes	13	26	14	20	17	23	14	21
○ No	20	10	19	16	16	13	19	15
No information	3	0	3	0	3	0	3	0
Argentina	○	●	○	○	●	●	●	●
Brazil	●	●	○	●	○	●	●	●
Bulgaria	N/A	○	N/A	○	N/A	○	N/A	○
Indonesia	○		○		○		○	
Croatia	N/A	○	N/A	○	N/A	○	N/A	○
Peru	●	●	●	●	●	●	●	●
Romania	○	○	○	○	○	○	○	○
Thailand	N/A		N/A		N/A		N/A	

Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

Annex Table 5.A.3. Countries using methods to test digital government services

Methods used to test digital government services

Country	Usability testing		Focus groups		Design thinking sessions		Public consultation websites		A/B testing		First-click testing		Tree testing	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
Australia	●	●	●	●	●	●	●	●	●	●	○	●	●	●
Austria	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Belgium	●	●	●	●	●	●	●	○	○	●	○	●	○	●
Canada	●	●	●	●	●	●	●	●	○	○	○	○	○	○
Chile	○	●	●	●	●	●	○	●	○	○	○	○	○	○
Colombia	●	●	○	○	○	○	●	●	○	○	○	○	○	○
Costa Rica	○	○	○	●	○	●	○	●	○	○	○	○	○	○
Czechia	●	●	●	●	●	●	○	○	○	○	○	○	○	○

Country	Usability testing		Focus groups		Design thinking sessions		Public consultation websites		A/B testing		First-click testing		Tree testing	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
Denmark	●	●	●	●	●	●	○	○	○	○	●	●	○	○
Estonia	●	●	●	●	●	●	●	●	●	●	○	○	○	○
Finland	●	●	●	●	○	○	○	○	○	○	○	○	○	○
France	●	●	●	●	●	●	●	○	○	○	○	○	○	○
Greece	N/A	●	N/A	●	N/A	●	N/A	●	N/A	○	N/A	○	N/A	○
Hungary	○	●	○	○	○	●	○	○	○	○	○	○	○	●
Iceland	○	●	○	●	○	●	○	●	○	●	○	●	○	●
Ireland	○	●	○	●	○	●	○	●	○	○	○	○	○	○
Israel	○	○	○	●	○	●	○	●	○	●	○	●	○	●
Italy	●	●	○	○	○	○	●	●	●	●	○	○	○	○
Japan	●	●	○	○	●	●	○	○	●	●	○	○	○	○
Korea	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Latvia	●	●	○	○	○	○	○	○	○	○	○	○	○	○
Lithuania	●	●	●	●	○	○	○	○	○	○	○	○	○	○
Luxembourg	●	●	○	○	●	●	○	○	○	○	○	○	○	○
Mexico	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Netherlands	○	●	○	●	○	●	○	●	○	○	○	●	○	○
New Zealand	●	●	●	●	○	○	●	●	○	○	○	○	○	○
Norway	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Poland	●	●	●	●	○	○	●	●	○	○	○	○	○	○
Portugal	○	●	○	●	○	●	○	●	○	○	○	○	○	●
Slovak Republic	N/A	●	N/A	●	N/A	●	N/A	○	N/A	●	N/A	○	N/A	○
Slovenia	○	○	●	●	●	●	●	●	○	○	○	○	○	○
Spain	●	●	○	●	○	○	○	●	○	○	○	○	○	○
Sweden	●	●	●	●	●	○	○	○	○	○	○	○	○	○
Switzerland	N/A	●	N/A	○	N/A	●	N/A	●	N/A	○	N/A	●	N/A	●
Türkiye	○	○	○	○	○	○	○	○	○	○	○	○	○	○
United Kingdom	●	●	●	●	●	●	●	●	●	●	●	●	●	●
OECD Total														
● Yes	20	29	16	25	14	23	12	20	6	10	3	9	3	9
○ No	13	7	17	11	19	13	21	16	27	26	30	27	30	27
No information	3	0	3	0	3	0	3	0	3	0	3	0	3	0
Argentina	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Brazil	●	●	●	●	●	○	●	●	●	○	●	○	●	○
Bulgaria	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○
Croatia	●	○	○	○	○	○	○	○	○	○	○	○	○	○
Indonesia	N/A	○	N/A	●	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○
Peru	●	○	●	●	●	●	●	●	●	○	●	○	○	○
Romania	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Thailand	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○

Note: "Usability testing" refers to a testing technique based on the evaluation of a system by its users, ensuring effectiveness and efficiency, and measuring the degree to which the system is adapted to the user needs. "Focus groups" refers to a group involving a small number of participants with similar experience gathered together to address and discuss and specific issue. "Design thinking sessions" refers to organized meetings to identify and overcome issues by using the 'design thinking methodology' which consists of matching the needs with feasible solutions to create value in a ordered and systematic way. "Public consultation websites" refers to a web tool to collect opinions of interested and affected groups for particular issues in order to improve transparency, efficiency and effectiveness of public regulation. "A/B testing" refers to a user experience testing

technique based on the comparison between two versions of a same product or service. "First-click testing" refers to a testing method for websites, apps or platforms which examines the 'first click' of the users when interacting the system, aiming to verify the success of completing a task. 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

Annex Table 5.A.4. Government-wide initiatives to use data to anticipate and plan interventions

Government-wide initiatives by the central/federal government to use data to anticipate and plan government interventions, by area

Country	Evidence-based policymaking	Regulatory development and impact assessment	Public financial management and budgeting	Public sector integrity	Forecast and predict natural disasters	Public procurement	Human resource needs in the public sector
Australia	●	●	●	●	●	●	●
Austria	○	○	○	●	●	●	○
Belgium	●	●	●	●	●	●	●
Canada	●	●	●	●	●	●	●
Chile	●	○	○	●	●	●	○
Colombia	●	●	●	●	●	●	●
Costa Rica	○	○	●	●	○	○	○
Czechia	●	●	●	○	●	●	○
Denmark	●	○	●	○	●	○	○
Estonia	●	●	●	●	●	●	●
Finland	●	●	●	●	●	●	●
France	●	●	●	●	●	○	○
Greece	●	●	●	●	●	●	●
Hungary	●	○	○	○	○	○	○
Iceland	●	○	●	●	●	●	●
Ireland	●	●	●	○	●	●	●
Israel	○	○	●	○	○	●	●
Italy	○	○	○	○	○	○	○
Japan	●	●	●	○	●	●	●
Korea	●	●	●	●	●	●	●
Latvia	●	○	○	●	●	●	○
Lithuania	○	●	●	●	○	●	●
Luxembourg	●	●	○	●	●	●	●
Mexico	●	●	○	●	○	●	○
Netherlands	○	○	○	○	○	○	○
New Zealand	●	●	●	●	●	●	○
Norway	●	●	●	●	●	●	●
Poland	○						
Portugal	●	○	●	●	●	●	●
Slovak Republic	●	○	○	○	○	○	○
Slovenia	●	○	●	●	●	●	●
Spain	○	●	●	●	●	●	●
Sweden	●	●	●	●	●	●	○
Switzerland	○	●	●	○	●	●	●
Türkiye	●	●	●	○	●	●	●
United Kingdom	○	●	●	●	●	●	●

Country	Evidence-based policymaking	Regulatory development and impact assessment	Public financial management and budgeting	Public sector integrity	Forecast and predict natural disasters	Public procurement	Human resource needs in the public sector
OECD Total							
● Yes	26	22	26	24	27	28	21
○ No	10	13	9	11	8	7	14
No information	0	0	0	0	0	0	0
Argentina	○	○	○	○	○	○	○
Brazil	●	○	●	●	●	●	●
Bulgaria	○	○	○	○	○	○	○
Croatia	○	○	○	○	○	○	○
Indonesia	○	○	●	●	●	●	●
Peru	●	●	●	●	●	●	●
Romania	○	○	○	○	○	○	○
Thailand	○	○	●	●	●	●	○

Note: Data not available for Germany and the United States. Data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

Annex Table 5.A.5. Government-wide use of data to design and deliver public services

Government-wide initiatives by the central/federal government to design and deliver government services according to the use of data, by area

Country	User needs		User feedback		Usage patterns		User satisfaction		Service performance	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
Australia	●	●	●	●	●	●	●	●	●	●
Austria	●	●	●	○	●	○	●	○	●	○
Belgium	●	●	●	●	●	●	●	○	○	○
Canada	●	●	●	●	●	●	●	●	●	●
Chile	○	○	○	●	○	○	●	●	●	●
Colombia	○	●	○	●	●	●	○	●	○	●
Costa Rica	○	●	○	○	○	○	○	○	○	○
Czechia	○	○	○	●	○	○	○	○	○	●
Denmark	●	●	●	●	●	●	●	●	●	●
Estonia	●	●	●	●	○	○	●	●	○	○
Finland	●	●	○	○	○	○	○	○	●	○
France	●	●	○	●	○	●	○	●	●	●
Greece	N/A	●	N/A	●	N/A	○	N/A	●	N/A	○
Hungary	○	●	○	●	○	●	○	●	○	●
Iceland	●	●	●	●	○	○	●	●	●	●
Ireland	○	●	○	●	○	●	○	●	○	●
Israel	○	●	○	●	○	●	○	●	○	●
Italy	●	○	●	○	○	○	●	○	●	○
Japan	○	○	○	●	○	●	○	●	●	●
Korea	●	●	●	●	●	●	●	●	●	●
Latvia	●	●	●	●	○	○	○	○	●	●
Lithuania	●	●	●	●	●	●	●	●	●	●
Luxembourg	●	●	●	●	○	○	○	●	○	○
Mexico	●	○	○	○	●	○	●	○	●	●
Netherlands	●	○	●	○	●	○	●	○	●	○

Country	User needs		User feedback		Usage patterns		User satisfaction		Service performance	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
New Zealand	○	●	○	○	○	○	○	○	○	○
Norway	●	●	●	●	●	●	●	●	●	●
Poland	○	○	○	○	○	○	○	○	○	○
Portugal	○	○	○	●	○	●	○	●	○	●
Slovak Republic	N/A	●	N/A	●	N/A	●	N/A	●	N/A	●
Slovenia	○	○	○	○	○	○	○	○	○	○
Spain	○	○	○	○	○	○	○	○	○	○
Sweden	○	○	○	○	○	○	○	○	○	○
Switzerland	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○
Türkiye	●	●	●	●	●	○	●	●	●	●
United Kingdom	●	●	●	●	●	●	●	●	●	●
OECD Total										
● Yes	19	24	16	24	13	16	16	21	18	21
○ No	14	12	17	12	20	20	17	15	15	15
No information	3	0	3	0	3	0	3	0	3	0
Argentina	●	○	○	●	●	○	●	●	●	○
Brazil	●	●	●	●	○	○	●	●	○	●
Bulgaria	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○
Croatia	○	○	○	○	○	○	○	○	○	○
Indonesia	N/A	○	N/A	○	N/A	○	N/A	●	N/A	○
Peru	●	○	●	●	●	○	●	●	●	○
Romania	○	○	○	○	○	○	○	○	○	○
Thailand	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○

Note: 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

Annex Table 5.A.6. Measurement of service performance and transaction costs

Metrics used to measure performance of digital government services

Country	Average time to complete		Satisfaction rate		Incomplete transactions rate		Failure demand		Transaction	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
Australia	○	●	●	●	○	●	○	●	●	●
Austria	○	○	●	●	○	○	○	○	○	○
Belgium	●	●	●	●	○	○	○	○	○	○
Canada	●	●	●	●	○	●	○	○	○	○
Chile	●	●	●	●	○	○	○	○	○	○
Colombia	●	●	●	●	○	○	●	●	●	●
Costa Rica	○	○	○	○	○	○	○	○	○	○
Czechia	○	○	○	○	○	○	○	○	○	○
Denmark	●	○	●	●	●	○	○	○	●	●
Estonia	●	●	●	●	○	○	○	○	○	○
Finland	○	○	○	○	○	○	○	○	●	●
France	●	●	●	●	○	○	○	○	○	○
Greece	N/A	●	N/A	●	N/A	●	N/A	○	N/A	●

Country	Average time to complete		Satisfaction rate		Incomplete transactions rate		Failure demand		Transaction	
	2023	2025	2023	2025	2023	2025	2023	2025	2023	2025
Hungary	○	○	●	●	○	○	●	●	○	○
Iceland	○	○	●	●	○	●	○	○	○	●
Ireland	●	●	●	○	●	○	○	○	○	○
Israel	●	●	○	●	●	●	●	●	○	○
Italy	○	○	●	●	○	○	○	○	○	○
Japan	○	○	●	●	○	○	○	○	●	○
Korea	●	●	●	●	○	○	●	●	●	●
Latvia	○	○	●	●	○	○	○	○	○	○
Lithuania	●	○	○	○	○	○	○	○	○	○
Luxembourg	○	○	○	●	○	○	○	○	○	○
Mexico	○	○	●	●	○	○	○	○	●	○
Netherlands	○	○	○	○	○	○	○	○	○	●
New Zealand	○	○	○	○	○	○	○	○	○	○
Norway	○	○	●	●	○	○	○	○	●	●
Poland	○	○	○	○	○	○	○	○	○	○
Portugal	○	●	●	●	●	●	○	●	●	●
Slovak Republic	N/A	●	N/A	●	N/A	○	N/A	○	N/A	○
Slovenia	○	○	○	○	○	○	○	○	●	●
Spain	○	○	●	●	○	○	○	○	●	●
Sweden	●	○	●	○	○	○	○	○	●	○
Switzerland	N/A	○	N/A	●	N/A	○	N/A	○	N/A	○
Türkiye	●	●	●	●	●	●	●	●	●	●
United Kingdom	○	○	●	●	●	●	●	●	○	●
OECD Total										
● Yes	13	14	23	26	6	8	6	8	13	14
○ No	20	22	10	10	27	28	27	28	20	22
No information	3	0	3	0	3	0	3	0	3	0
Argentina	○	○	●	●	●	○	○	○	○	○
Brazil	●	●	●	●	○	○	○	○	●	●
Bulgaria	N/A	○	N/A	○	N/A	○	N/A	○	N/A	○
Croatia	○	○	○	○	○	○	○	○	○	○
Indonesia	N/A	○	N/A	●	N/A	○	N/A	○	N/A	●
Peru	●	●	●	●	●	○	○	●	●	●
Romania	○	○	○	○	○	○	○	○	○	○
Thailand	N/A	○	N/A	●	N/A	○	N/A	○	N/A	○

Note: "Failure demand" refers to inquiries caused by failures, poor services or inconveniences when providing services. 2025 data not available for Germany and the United States. 2023 data not available for Bulgaria, Germany, Greece, Indonesia, Slovak Republic, Switzerland, Thailand and the United States. 2025 data for Indonesia and Thailand cover the period from 1 January 2022 to 31 December 2023.
Source: OECD (2025) Survey on Digital Government 3.0.

REFERENCES

Administrative Department of the Public Service (Colombia) (2022), *Documento metodológico operación estadística: Cálculo de ahorros ciudadanos por racionalización de trámites*, https://www1.funcionpublica.gov.co/documents/34645357/34703525/Documento_metodologico_operacion_estadistica_calculo_ahorros_ciudadanos_racionalizacion_tramites_v2.pdf/003a321b-17e6-f7df-7923-cdbcfb66f0ce?t=1670346246908. [52]

Alliance for Digital Living (2026), *Alliance for Digital Living*, https://digitaalsamenleven.nl/. [22]

ARTE (n.d.), *Manual de Apoio à Quantificação de Benefícios Económicos*. [51]

Australian Bureau of Statistics (2026), *Life Course Data Initiative*, https://www.abs.gov.au/about/key-priorities/life-course-data-initiative. [33]

Australian Department of Social Services (2025), *Partnerships for Local Action and Community Empowerment*, https://www.dss.gov.au/supporting-community-change/partnerships-local-action-and-community-empowerment. [34]

Australian Department of the Treasury (2025), *State of Evaluation in the Australian Government 2025*, https://evaluation.treasury.gov.au/publications/state-evaluation-australian-government-2025. [35]

Conféderation suisse (2026), *Modèle de gouvernance de la transformation numérique*, https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bereichdti/organisation.html. [13]

Designers Italy (2025), *Designers Italy*, https://designers.italia.it/. [11]

Digital Iceland (n.d.), *Benefits of digital processes*, https://island.is/s/stafraent-island/avinningur-af-stafraenum-ferlum. [53]

Digital Iceland (n.d.), *Influencers*, https://island.is/en/o/digital-iceland/influencers. [18]

DTA (2025), *Digital Experience Policy*, https://www.digital.gov.au/policy/digital-experience. [14]

Finnish State Treasury (2024), *Fact sheet*, https://www.valtiokonttori.fi/palvelu/tietokiri/. [39]

FPS BOSA (2024), *Only Once: the one-time collection of data*, https://bosa.belgium.be/nl/themas/digitale-overheid/administratieve-vereenvoudiging/only-once-de-eenmalige-inzameling-van. [28]

gov.pt (2026), *The Portuguese public services portal*, https://www.gov.pt/servicos. [24]

GOV.UK (2026), *Service Standard Reports*, https://www.gov.uk/service-standard-reports. [17]

GOV.UK (2025), *User research*, https://www.gov.uk/service-manual/user-research. [16]

GOV.UK (2021), *Measuring cost per transaction*, https://www.gov.uk/service-manual/measuring-success/measuring-cost-per-transaction. [50]

GOV.UK (2019), *Service Standard*, https://www.gov.uk/service-manual/service-standard. [7]

Government of Canada (2026), *Impact Assessment Agency of Canada*, https://www.canada.ca/en/impact-assessment-agency.html. [21]

Government of Canada (2025), *Policy on Communications and Federal Identity*, https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=30683. [20]

Government of Israel (2026), *gov.il – Services and Government Information Website*, https://www.gov.il/he. [26]

Government of Spain (2022), *Wildfires in Spain: News Update*, https://www.miteco.gob.es/content/dam/miteco/es/biodiversidad/temas/incendios-forestales/avance_1_enero_31_diciembre_2022_tcm30-560521.pdf. [46]

Government Office of Estonia (2026), *A smart text data search solution supporting the preparation of policy-making decisions*, https://www.riigikantselei.ee/poliitikakujundamise-otsuste-ettevalmistamist-toetav-tekstiandmete-targa-otsingu-lahendus. [36]

Head of State (Spain) (2015), *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.*, https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10565. [31]

island.is (2024), *Project Management*, https://docs.devland.is/technical-overview/project-management. [19]

L'Assemblée fédérale de la Confédération suisse (2024), *Loi fédérale sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités*, https://www.fedlex.admin.ch/eli/oc/2023/682/fr. [12]

Ministry of Culture (France) (2025), *compar:IA*, https://comparia.beta.gouv.fr/. [44]

Ministry of Digital Governance (Greece) (2024), *OOTSHUB Greece*, https://ootshub.mindigital.gr/. [30]

Ministry of Digital Governance (Greece) (2022), *Implementation of a Central Hub for the Management & Analysis of Multidimensional Big Data*, https://greece20.gov.gr/?projects=kentrikos-komvos-diacheirisis-kai-analysis-polydiastaton-dedomenon-megaloy-ogkoy-big-data-16842. [37]

Ministry of Digital Governance (Greece) (2022), *Once-Only Hub - The future of the single market*, https://digi.gov.gr/once-only-hub-to-mellon-tis-eniaias-agoras/. [29]

Ministry of Digitalization (Luxembourg) (2025), *L'initiative AI4Gov*, https://gouvernement.lu/fr/dossiers.gouv2024_mindigital+fr+dossiers+2021+AI4Gov.html. [45]

Ministry of Finance (Finland) (n.d.), *Knowledge management*, https://vm.fi/tietojohtaminen. [38]

Ministry of Government Legislation (Korea) (2026), *Korean Law Information Center*, https://www.law.go.kr/LSW/eng/engMain.do. [32]

Ministry of the Interior and Safety (Republic of Korea) (2026), *Government24+*, https://plus.gov.kr/. [25]

OECD (2025), *Digital Government Review of Korea: Harnessing Digital and Data to Transform Government*, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/9defc197-en. [43]

OECD (2025), "Effectively Managing Investments in Digital Government: An OECD Framework", *OECD Public Governance Policy Papers*, No. 76, OECD Publishing, Paris, https://doi.org/10.1787/5c324e91-en. [49]

OECD (2025), *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*, OECD Publishing, Paris, https://doi.org/10.1787/795de142-en. [41]

OECD (2025), *Government at a Glance 2025*, OECD Publishing, Paris, https://doi.org/10.1787/0efd0bcd-en. [47]

OECD (2025), *Harnessing Artificial Intelligence in Social Security: Use Cases, Governance and Workforce Readiness*, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/b52405c1-en. [42]

OECD (2025), *More Effective Social Protection for Stronger Economic Growth: Main Findings from the 2024 OECD Risks that Matter Survey*, OECD Publishing, Paris, https://doi.org/10.1787/3947946a-en. [2]

OECD (2025), "Recommendation of the Council on Human-Centred Public Administrative Services", *OECD Legal Instruments*, OECD/LEGAL/503, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0503 (accessed on 9 January 2026). [3]

OECD (2025), "Tackling civic participation challenges with emerging technologies: Beyond the hype", *OECD Public Governance Policy Papers*, No. 72, OECD Publishing, Paris, https://doi.org/10.1787/ec2ca9a2-en. [15]

OECD (2024), *Global Trends in Government Innovation 2024: Fostering Human-Centred Public Services*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/c1bc19c3-en. [40]

OECD (2024), *Modernising Access to Social Protection: Strategies, Technologies and Data Advances in OECD Countries*, OECD Publishing, Paris, https://doi.org/10.1787/af31746d-en. [5]

OECD (2024), *OECD Survey on Drivers of Trust in Public Institutions – 2024 Results: Building Trust in a Complex Policy Environment*, OECD Publishing, Paris, https://doi.org/10.1787/9a20554b-en. [1]

OECD (2023), *Civic Space Review of Portugal: Towards People-Centred, Rights-Based Public Services*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/8241c5e3-en. [9]

OECD (2023), *OECD Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem*, OECD Publishing, Paris, https://doi.org/10.1787/c74f03de-en. [6]

OECD (2023), "Recommendation on Access to Justice and People-Centred Justice Systems", *OECD Legal Instruments*, OECD/LEGAL/0498, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0498. [4]

OECD (2022), "OECD Good Practice Principles for Public Service Design and Delivery in the Digital Age", *OECD Public Governance Policy Papers*, No. 23, OECD Publishing, Paris, https://doi.org/10.1787/2ade500b-en. [8]

OECD (forthcoming), *Operationalising consent in the digital ecosystem: mapping challenges and technical innovations, and exploring the opportunities of AI*, OECD Publishing, Paris. [27]

OECD (forthcoming), *Serving Citizens*, OECD Publishing, Paris. [48]

Portuguese Republic (2026), *MOSAICO*, https://mosaico.gov.pt/. [10]

Presidency of the Council of Ministers (Portugal) (2024), *Decreto-Lei n.º 49/2024, de 8 de agosto*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/49-2024-875899341. [23]

Digital Government Outlook 2026

From Foundations to Transformational Impact

Governments today face a growing disconnect between rising expectations for speed, adaptability and responsiveness, and institutional systems that have not kept pace. Digital technologies and data are no longer optional enablers; they have become core infrastructure for addressing today's policy and service delivery challenges. The 2025 OECD Digital Government Index (DGI) and Open, Useful and Re-usable Data (OURdata) Index confirm that governments have made meaningful progress, particularly in establishing strategies, frameworks and enabling conditions. The challenge now is to move beyond these foundations to deliver transformational impact for people and businesses: strengthening data governance for greater coherence and reuse, increasing uptake of digital public infrastructure, modernising investment and procurement approaches, building robust trust frameworks for AI, and designing more proactive, human-centred services.

The OECD *Digital Government Outlook* provides a comprehensive, forward-looking assessment of these dynamics across 36 OECD Members and 8 accession candidate countries. Drawing on the results of the 2025 DGI and OURdata, it evaluates both progress and persistent gaps across key areas of digital transformation, identifying what governments need to do to move from digital ambition to public sector performance in an environment of rapid technological change, fiscal constraints and limited public trust.

PRINT ISBN 978-92-64-97814-0
PDF ISBN 978-92-64-88028-3