

Smarter guide to information management in the public sector with OpenText

Expected business outcomes of information management



Contents

Introduction: The current state of global government	3
Key challenges facing the public sector	3
Key trends in the public sector	4
The role of information management in the public sector	4
About this guide	5
1. Information management in the public sector	6
2. The digital citizen	9
3. Data-driven government	11
4. IT optimization and modernization	13
5. The modern workforce	16
6. Cybersecurity	19
7. Defense and intelligence agencies	22
8. Educational Institutions	24
9. Selecting your technology partner	26
10. 7 top tips for digital transformation in government	27

Three key OpenText public sector solutions have achieved fully authorized status on the FedRAMP marketplace:

- [OpenText Cloud for Government](#)
- [OpenText™ Fortify™ on Demand](#)
- [OpenText IT Management Platform \(ITMX\)](#)

In addition, OpenText™ Content Management (Extended ECM) has achieved Protected B authorization, providing central government agencies in Canada assurance that it meets their cloud security standards.

Introduction: The current state of global government

With the increase in government directives related to digital technology, and rising citizen expectations due to private sector innovations, global governments are feeling the pressure to modernize citizen services.

Regulations, laws, and policies set the standards and requirements for cloud security in the public sector. Examples include FedRAMP in the United States, Protected B in Canada, and the Information Security Registered Assessors program in Australia.

Other government policies related to cybersecurity have been implemented in recent years, including [Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure in the US](#), [Canada's National Cyber Security Strategy](#), and the [2023-2030 Australian Cyber Security Strategy](#).

Governments must also meet records mandates such as the [NARA memorandum](#) to transition US federal agencies to electronic records, while public health agencies have regulations they must meet to protect sensitive patient data.

More recently, governments have published policies and guidance governing the use of AI, including the European Union's [AI Act](#), [Executive Order 13960: Promoting the Use of Trustworthy AI in the Federal Government](#) in the US, and the [Artificial Intelligence and Data Act \(AIDA\)](#) in Canada.

These policies, mandates, and regulations place significant pressure on government organizations to modernize their IT stack. Many governments are making strides towards modernization and digital transformation, but there is still progress to be made.

Key challenges facing the public sector

The public sector is faced with [several key challenges](#) when it comes to delivering modern citizen services. The pandemic has fundamentally changed the way public sector agencies do business, and governments have adapted to accommodate a hybrid workforce.

Continued remote workforce structures are driving the need for improved information access and employee productivity tools. Many public sector agencies are also facing a worker shortage and challenges attracting and retaining top talent, especially in ever-changing areas like cybersecurity, data analytics, and AI.

Many government departments worldwide continue to depend on outdated technology and applications. These legacy systems often result in disaggregated or siloed data, which can present significant challenges to modernization initiatives. Custom-built legacy applications also cannot be easily modified to accommodate larger volumes, were not designed for remote workers, and are not secure. These legacy systems are also hindering progress indirectly: they are absorbing all the IT money.

Governments are spending significant amounts of their budget on the operations and maintenance of IT investments, including legacy systems. In the US, federal government spends more than [\\$100 billion on IT and cyber-related investments](#), 80 percent of which is allocated to maintaining existing IT. It is near-impossible to innovate when 80 percent of your budget is going to maintenance with just 20 percent left for modernization efforts.



The security challenges associated with legacy systems and the increase in cybersecurity threats to governments in recent years also make modernization initiatives both more important and more difficult.

Faced with these challenges, public sector agencies need a strategic technology partner that can help them modernize citizen services in a comprehensive way.

Key trends in the public sector

Several key trends are driving modernization in the public sector:

- **Migration to the cloud:** Driven by Cloud Smart policies and other government cloud mandates, there is a push to migrate agencies to the cloud. This increases public sector reliance on sensitive content discovery and remediation.
- **Artificial intelligence (AI):** AI is quickly becoming ubiquitous in the public sector, although many agencies are careful about which data sets should be incorporated. [Generative AI](#) (GenAI) has the potential to make governments more efficient and effective with increased automation, AI-driven insights, and more.
- **Total Citizen Experience:** The public sector must keep pace with the private sector in providing citizens with a personalized, frictionless experience.

Total Citizen Experience takes a holistic approach to citizen experience by incorporating external user experience (such as mobile apps, web portals, and online data collection) with internal operational experience. After all, a slick front-end system paired with a legacy back-end system is destined to fail any customer satisfaction survey.

The role of information management in the public sector

[Information management](#) is the practice of capturing, governing, exchanging, and using information to its full potential while keeping it secure. Early studies estimated that knowledge workers spend 20 percent or more of their time searching for information in their own internal IT environment.¹ A recent Gartner study shows that this trend hasn't changed: as many as 47 percent of workers struggle to find the information they need to complete their jobs.²

Time spent searching for internal information means sacrificing mission-critical work. Modern information management solutions and best practices make it possible to work smarter by organizing, integrating, and protecting data as it flows through business processes across the organization and beyond.

¹ Hubbion, *Document Management Statistics*, 2019

² Gartner, *Gartner Survey Reveals 47% of Digital Workers Struggle to Find the Information Needed to Effectively Perform Their Jobs*, 2023

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the US and internationally and is used herein with permission. All rights reserved.

A modern information management system can ease all the challenges government faces—from improving cybersecurity and cloud migrations, to providing AI-fueled analytics, and improving citizen (and employee) satisfaction. It also ensures that public sector agencies remain fully compliant with all records management and data protection mandates.

OpenText information management solutions deliver enterprise-wide content services that automate workflows and manage all forms of content throughout their entire lifecycle—digitizing documents, creating a content ecosystem, and providing a complete view of the customer across all channels.

About this guide

This guide examines how functions across the public sector can leverage information management technologies and best practices to achieve their strategic initiatives. The chapters are broken down into key topics and functional areas in the public sector.

Each chapter includes:

- Trends in the functional area.
- Key business challenges.
- How OpenText information management solutions can help.

Inc. and/or its affiliates in the US and internationally and is used herein with permission. All rights reserved.





1. Information management in the public sector

In this chapter:

- Learn what information management means to the public sector
- Compare your agency against an information management readiness checklist
- Understand how to establish a smarter public sector approach to information management

Information management is one of the key challenges facing the public sector—and one of the greatest areas for opportunity. But what is information management, and why does it matter to the public sector?

Gartner [defines information management](#) as “a method of using technology to collect, process and condense information with a goal of efficient management.”

Information management solutions help public sector agencies to [work smarter](#) by organizing, integrating, and protecting data as it flows through business processes.

Public sector agencies work with a significant amount of data—including sensitive citizen and business data—which must be properly and securely managed to deliver an exceptional citizen experience while protecting against cyberthreats.

While much of that data is “structured,” i.e., collected using standardized forms, other data stored by government is considered “unstructured” (e.g., videos, photos, and captured images). Unstructured data poses different challenges in deriving insights and analysis as well as simply connecting it to relevant workflows.

Information management solutions can help public sector agencies easily and securely capture, govern, and exchange information to gain the [information advantage](#).

Benefits of information management in the public sector

There are several benefits to implementing a robust information management strategy in the public sector.

Connect data across the agency

Integrating systems, people, and data across the agency enriches information and enables it to be delivered in context, wherever it’s needed. This is key to delivering timely, accurate, and tailored citizen experiences.

Provide a single source of truth

Having the correct information at the right time is essential to employee satisfaction. A robust information management strategy—with solutions that integrate into existing systems and data—breaks down silos and provides employees with a single source of truth.

3 Gartner, *Adapting to the Customer Service Preferences of Gen Z and Millennials*. October 30, 2023.

Improve citizen and employee experience

A strong information management strategy can improve both citizen and employee experience. This is especially true in hybrid work environments.

When employees don't have to spend significant time searching for the information they need, they can focus more attention on delivering an exceptional experience. A robust information management strategy can also enable self-serve options for citizens, which is the preferred delivery mechanism for Millennials and Generation Z users.

Increase cybersecurity

Including robust cybersecurity solutions in an agency's information management strategy can increase overall cyber resiliency by detecting and remediating threats as well as protecting against data loss to ensure business continuity.

Improve operational efficiency and sustainability

Information management solutions enable public sector organizations to automate paper-based and manual processes, which not only improve operational efficiency but also contribute to sustainability and environmental, social, and governance targets.

Find insights faster

AI is quickly becoming a key component of a strong information management strategy. From improving decision-making across government, to monitoring cybersecurity threats, to searching through vast amounts of content, AI can help. Public sector agencies are equipped to find insights faster, reduce risk, and improve operational efficiency to deliver against their mission much more effectively.

Information management readiness checklist

The information management readiness checklist is a tool to help you identify how ready your agency is to take the next step on your information management journey. Whether your agency is just beginning an information management journey or working to refine and optimize its current approach, this checklist can help.

Questions to assess information management maturity in the public sector:

- ☒ Do you have an agency-wide information management strategy?
- ☒ How many of your records are on paper?
- ☒ What percentage of your records are categorized using metadata?
- ☒ How often is the data in question used?
- ☒ Is the data located in one repository, or is it siloed across different IT systems?
- ☒ Is your agency committed to hiring and training employees to implement or expand an information management strategy?
- ☒ Has your agency established a commitment to identifying and empowering information management leaders?
- ☒ How are your agency's records archived? Do you have automated tools for compliance, or is this primarily a manual process?
- ☒ Do you have an archiving strategy to reduce costs and complexity?
- ☒ What legislation, regulations, or directives need to be considered when developing or defining your agency's information management strategy?

Information management with OpenText

OpenText provides the world's most comprehensive set of modern information management solutions to help the public sector manage its structured and unstructured information end to end.

[OpenText Cloud for Government](#) is a FedRAMP®-authorized government cloud solution providing a low-risk, highly secure content management cloud option for the public sector.

Total Citizen Experience is an end-to-end solution that combines the industry-leading capability of OpenText Customer Experience and Content Management solutions. It provides a single source of truth for the entire customer journey, from onboarding to case management, to archiving.

[OpenText IT Management Platform \(ITMX\)](#) is a FedRAMP-authorized set of cloud-native tools that centralizes security, tracking, and project and portfolio management services into one environment. ITMX is hosted within the AWS GovCloud infrastructure for the United States Public Sector.

[OpenText Content Management for Government](#) (Extended ECM for Government) provides the digital file and case management for modern administration in central, local, and municipal government. The solution is FedRAMP authorized, Protected B certified, and the only public sector enterprise content management solution that has undergone rigorous validation by SAP® to ensure the highest quality standards.

The **OpenText AI Platform**, [OpenText™ Aviator](#), provides predictive AI-led analytics, AI-powered conversational search, and generative AI to help public sector agencies get the most out of their information.

OpenText Cybersecurity includes a full stack of tools covering prevention, detection and response, recovery, investigation, and compliance. It also enables end-to-end security protection and helps public sector agencies reduce risk, maintain trust, minimize disruption, and increase cyber resilience.



2. The digital citizen

Citizens today have a broad appetite for digital services from the public sector. Whether they want to learn about planned developments in their neighborhood, apply for a permit, or receive relevant and localized emergency alerts, their expectations have risen dramatically.

[A Deloitte 2023 survey](#) of 5,800 individuals across 13 countries⁴ found that customer satisfaction from digital government services is 21 percentage points lower than private sector services.

Today's citizens are digital citizens, and the public sector needs to prioritize delivering an exceptional digital service to keep citizens engaged and satisfied.

What is the digital citizen?

The digital citizen is always-on, always-connected, and expects prompt, fast, seamless experiences. They expect to be able to connect with the public sector services they need—when, where, and how they need them.

It's important for public sector agencies to remember that digital citizens' expectations are guided by the experiences they receive in the private sector. Companies like Amazon, Apple®, and Uber® are setting the bar for what constitutes a good digital experience. These companies focus on total transparency, easy payments, and personalization while being fully secure.

The digital citizen has no patience for endless wait times on hold or looking through confusing websites to find the information they need. Instead, they are inclined to self-service options, preferring to log on to a portal to manage their account, access information, or take care of other requirements.

AI is set to accelerate this trend, putting even greater pressure on government to keep up.

Benefits of delivering a better digital service to citizens

Every touchpoint with the public is an opportunity to positively connect, enhance citizen engagement, and make interactions more efficient and relevant. Here are three key benefits to delivering a better digital service to citizens.

Increased trust

Public customers are nine times more likely to trust a government agency if they are satisfied with the service they receive.⁵ A 2023 McKinsey survey further revealed that an increase in customer satisfaction correlates with both increased trust and decreased anxiety with government services.⁶

The [Forrester 2024 US Customer Experience Index](#) ranks government at 13th out of 13 measured industries. Delivering easy-to-navigate, frictionless digital services is a clear way to increase public trust.

⁴ Deloitte Insights, *Digital government and citizen experience survey*, 2023

⁵ McKinsey Quarterly Report, *The public sector gets serious about customer experience*, August 2019

⁶ McKinsey, *How US government leaders can deliver a better customer experience*, 2023

GenAI is set to transform every industry, including government. In fact, 91 percent of governments surveyed by IDC anticipate that generative AI will have an impact on work transformation.⁸

Boosted engagement

Investing in a seamless digital experience can boost engagement with citizens while simplifying operations. For example, sending citizens proactive, personalized, and secure communications based on their unique government interactions.

Improved employee satisfaction

Having the tools needed to deliver an exceptional citizen experience, no matter where they log in from, frees up employees to focus on core business and improves employee experience.

The new generation of digital citizen services

The digital citizen wants the ability to handle minor problems or queries through a self-service portal.

This expectation has only increased since the pandemic, after many countries allowed citizens to access their vaccination status online whenever they needed to.

Today, citizens expect to be able to access services via a self-service portal, such as filing and paying their taxes online, accessing their driving record, updating their address and contact information, and more. This is especially true for millennial and Gen Z citizens.⁷

GenAI will accelerate digital citizen experience initiatives. AI tools like real-time virtual assistants, and AI-driven analytics, insights, and call summarization can help enable the self-service options the digital citizen expects.

Meeting the digital citizen's needs with Total Citizen Experience

Over the past several years, agencies have invested in modernization efforts to centralize information so they can deliver a better citizen experience.

Faced with today's challenges, governments need to deliver a Total Citizen Experience. This strategy combines externally facing applications with back-end operations in a compliant environment supported by robust cybersecurity solutions. By doing so, the public sector can improve both employee and citizen experiences in a secure way—all of which increases public trust.

How to deliver a better digital citizen experience

OpenText provides solutions designed to help governments create and deliver citizen experiences that are optimized, personalized, and highly efficient.

Total Citizen Experience builds a 360-degree view of customer information and serves as a single source of trust for the entire customer journey. Combining customer experience and content management solutions, it drives future employee productivity and citizen satisfaction improvement.

⁷ Gartner, *Adapting to the Customer Service Preferences of Gen Z and Millennials*. October 30, 2023.



3. Data-driven government

Data drives everything that government does, yet data-driven government organizations have yet to be realized.

Achieving data-driven government goals requires running at digital speed through information, automation, and the cloud.

GenAI is set to transform every industry, including government. In fact, 91 percent of governments surveyed by IDC anticipate that generative AI will have an impact on work transformation.⁸

Set to reshape our future in fundamental ways, AI is a new ontology for how we look at data, how we create, and how we put trust at the forefront of everything.

By employing GenAI in a secure way, governments can better serve their citizens.

Effective AI needs effective information management

Having a robust information management strategy builds a strong foundation to successfully apply AI and gain the AI advantage. Solid results can only be achieved when the underlying data is reliable.

Modern information management helps government agencies:

- Find information easily.
- Define data-governance standards.
- Automate always-on data integration.
- Secure information flows.

AI that customers can trust requires curated, structured data, and content that are accurate, clean, and timely. To be effective, that data must be enriched and tagged with metadata.

With a modern information management strategy, governments can build a strong foundation to successfully gain the AI advantage.

Considerations for AI use in government

AI has the potential to revolutionize the way we work. However, it must be used responsibly, otherwise governments risk exacerbating social harms, displacing workers, or even posing risks to national security.

There are several considerations when implementing AI in government, including:

- **Privacy and compliance:** Governments must ensure their use of AI complies with legislation, policy, and guidelines that govern the consent, collection, storage, use, and retention of personal information.
- **Security:** AI systems must comply with relevant security and data protection legislation, executive orders, and directives. For third-party AI systems, security needs to be considered throughout the supply chain and should ensure access to data is restricted by role.
- **Transparency:** Citizens need to have clear insights into how their data is used by AI. They also need to know when they are interacting with AI via self-service options.

⁸ IDC, *Governments Anticipate That Generative AI Will Impact Employee Work Transformation*, 2023

To address these concerns, governments are implementing executive orders, directives, and frameworks on the safe and ethical use of AI.

In the US, the [Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence](#) was announced by the Biden Administration in October 2023.

The [EU Artificial Intelligence Act](#), which establishes a common regulatory and legal framework for AI within the European Union, came into force Aug. 1, 2024.

The Canadian Government has released the [Responsible use of artificial intelligence in government](#).

Australian state and territory governments released the joint [National framework for the assurance of artificial intelligence in government](#) in June 2024.

These executive orders, directives, and frameworks make clear that while AI presents great opportunities to transform public service delivery, government use of AI must be safe and responsible.

AI use cases in the public sector

AI can be used with complex events, taking on structured and unstructured data and allowing customers to feed image recognition and machine vision into AI. In Auckland, New Zealand, [AI is being used](#) to identify traffic patterns from real-time video sources to enhance public safety and ease congestion.

AI can also be used against data warehouses and data lakes. Applying it against text, voice, video, and audio can drive voice-to-text and enterprise search. AI can also be applied to visualization and data discovery. Another example includes auto-categorizing paper records and attaching them to workflows where needed.

In the cybersecurity space, machine learning can be used for predictive models, deep learning, and reinforcement learning.

Understanding the importance of sharing use cases across government at this stage of AI adoption, the US CIO Council has set up the [Federal AI Use Case Inventory](#), populated by federal agencies.

AI with OpenText

As technology drives into the realm of artificial general intelligence—where we're automating not just calculations, but decisions—AI trust, risk, and security become critical.

OpenText has been [working in AI for decades](#), with innovations ranging from natural language processing to helping customers extract information, organize it, and use it to make decisions.

OpenText recently launched [OpenText Aviator](#), a generative AI tool embedded into our content management, business network, cybersecurity, customer experience, and IT operations software. It supports prompt engineering, vector databases, and large language models.

Interested in AI for government, but don't know where to start? OpenText has created a guide to help you identify which OpenText AI business tools are right for your organization. Play the [AI match game](#) to learn more.



4. IT optimization and modernization

Governments continue to depend on outdated technology and legacy applications that can be many decades old. With the increase in government directives related to digital technology (e.g., NARA's mandate to preserve all US Government permanent records digitally), IT modernization is top of mind for many public sector agencies.

Unfortunately, getting there is far from easy.

Much of government IT budgets worldwide are tied to maintaining legacy systems. For example, the US federal government spends more than [\\$120 billion on IT and cyber-related investments each year](#), 80 percent of which goes to the operations and maintenance of existing IT investments, including legacy systems.

Not only are there budget challenges to IT optimization and modernization initiatives, but the lights must be kept on during the transition. Addressing both challenges requires that governments optimize their current operations while charting a path to modernization—especially cloud-based systems.

Here are three case studies that demonstrate how governments can optimize existing operations while making strides in their modernization journey.

Paper-based processes

The public sector continues to rely heavily on paper-based processes. By transitioning from paper-based to digital workflows, governments can make significant improvements in employee and citizen experience. This can help them meet environmental, social and governance (ESG) targets while reducing costs and increasing operational efficiencies.

[Harris County](#) is the most populous county in Texas and the third largest county in the US by population, with more than 4.7 million residents. Content management was a key challenge for them. In the past, departments relied on their own systems and processes to manage records, including warehouses to store paper documents and shared drives for digital information. Records were siloed and it was costly and time-consuming for departments to manage their own document archives.

Harris County was also challenged with manual, time-consuming, paper-based process for budget requests. Relying on paper increased the risk of important information getting lost in the shuffle.

The County increased its investment in digital technology to enhance and accelerate the services it delivers to residents and businesses. They worked with OpenText to implement a centralized enterprise content management platform for records management across departments. The solution helps ensure consistent records retention and disposition policies while delivering faster access to information.

OpenText Content Management provides Harris County with a central platform to manage key records, as well as digital workflows to automate previously manual processes. With the OpenText solution, Harris County has streamlined invoice payments and significantly cut records management efforts by reducing the human resources involved in filing records by 50 percent.

Funding and grants

The [National Bank for Agriculture and Rural Development \(NABARD\)](#), a government-owned bank in India, processes thousands of cases each year, including funding applications for agriculture and rural development projects. NABARD helps local communities and non-governmental organizations secure funding for projects to implement climate-resilient agriculture practices, develop robust and sustainable food value chains, promote agricultural mechanization, and more.

Assessing and approving cases involves a multi-stage review process that includes several departments.

The organization relied heavily on paper to manage cases and process thousands of applications each year, often mailing records between offices and departments. Application approval times were delayed by these manual, paper-based processes, and there was an increased risk of losing information as documents moved from desk to desk.

NABARD worked with OpenText to implement efficient digital workflows, reducing time to approve projects. They have accelerated approval times by initiating and processing more than 120,000 digital cases, saving time and physical storage space.

Transitioning to digital workflows has also significantly reduced NABARD's carbon footprint. By working on cases digitally, NABARD has saved approximately 2.4 million pages of paper, which equates to almost 10 tons of CO₂ emissions.

Digital records management

Digital records management can also significantly impact employees and citizens by eliminating data silos, reducing time spent searching for data and ensuring regulatory compliance.

In May 2023, the US Department of Defense (DoD) released a [records modernization strategy](#) that outlines the Department's direction for well-managed records.

The first-ever DoD Records Strategy treats electronic records as a strategic asset, seeking to employ technology such as AI and cloud-based services to reduce the administrative burden associated with records management. The goal of the strategy is to ensure DoD records are curated, records management processes are automated, and governance accountability is clear.

The [DoD Records Strategy](#) provides several key lessons that can be applied to any government records digitization initiative, including:

- Connect digital recordkeeping to the mission.
- State your goals simply and succinctly.
- Incorporate the latest technological advancements.
- Embed security at each step of the records management lifecycle.
- One size does not fit all.
- Use digital recordkeeping to address weaknesses (re: IG or GAO findings).
- Involve all the interested parties.

IT optimization and modernization tools and technologies

Whether your agency is looking to up-level its existing digital modernization program by incorporating AI or are still struggling to get a handle on mountains of paper documents, OpenText can help.

[Government cloud solutions that are FedRAMP-certified](#) help the public sector digitize and modernize its IT environments. OpenText Cloud for Government enables public sector organizations to digitize paper-based processes, securely and seamlessly manage records, and automate grants and funding processes.

[OpenText™ Process Automation \(AppWorks\)](#) is a low-code development platform that helps government agencies build engaging, smart, and easy-to-deploy process automation and dynamic records management applications. Through this solution, agencies can achieve operational efficiencies and innovate on demand while maintaining compliance.

OpenText Process Automation delivers the tools to digitize, automate, and integrate processes across functions, systems, machines, and clouds. It enables public sector agencies to quickly create applications at a low cost with low-code, drag-and-drop modeling, reusable building blocks, and accelerators.





5. The modern workforce

The COVID-19 pandemic, recent technological developments, and globalization have all had a significant impact on the way we work. These challenges have also resulted in a skills gap crisis across all industries.

According to IDC, the public sector is disproportionately impacted by the global shortage of technical skills.⁹ Compounding this crisis is the fact that many government workers are nearing retirement. The share of full-time workers in the US federal workforce over 54 years old is 29 percent.¹⁰

Technology such as AI is creating new work opportunities, but employers need skilled workers to fill these roles. Governments must work with businesses and academic institutions to address the growing skills gap and help students and workers transition into new digital careers in government and beyond.

The public sector can leverage AI and other technology to upskill staff, source skilled workers, and automate manual, repeatable tasks.

Trends impacting the skills gap

The [Digital Skills Gap Index 2021](#) shows that most economies are failing to bridge the gap. The capacity of economies' policymakers to respond to the talent deficit as well as education institutions' and corporate trainers' ability to deliver needed skills is lagging. Out of 132 countries reviewed for the index, Canada is ranked at No. 23, the United States at No. 26, and Australia at No. 33.

By 2030, [90 percent](#) of the jobs in the United States will require digital skills—yet one-third of American workers lack them. The US Government is seeking IT skillsets, with [five of the top seven](#) fastest-growing jobs involving some type of computer or statistical background.

The Canadian government is in a similar bind when it comes to attracting technical workers: it faces an estimated [30-percent shortage](#) for its IT positions.

For the Australian government, the [cybersecurity skills gap](#), which could see up to 30,000 unfilled positions in four years—is nearly twice the figure forecasted by AustCyber before the pandemic.

A 2023 [McKinsey Global Institute survey](#) found that 87 percent of companies worldwide reported either experiencing skill gaps now or expected to within the next five years. This not only impacts productivity and competitiveness at corporate and national levels, but also affects governments as they compete with the private sector to attract skilled workers.

9 IDC PlanScape: Leveraging AI to Address the Skills Gap in Federal Agencies, June 2023, IDC #US50308423

10 USA Facts, *How old is the federal workforce?*, 2023

Why is there a skills gap?

There are several challenges that have led to the skills gap crisis in the public sector. These include:

- **Legacy systems:** Legacy systems that are cumbersome and difficult to maintain and use impact employee experience and present major challenges to government agencies.
- **Slow and lengthy recruitment processes:** In the race for talent, cumbersome recruitment processes mean that governments can miss out on skilled workers who may be scooped up by the private sector's nimbler approach to hiring.
- **Aging populations:** More government workers are nearing retirement. This leaves more positions needing to be filled.
- **Rapid technological advancements:** AI, automation, and the cloud are changing the way we work and the jobs that need to be done. The pace of technological development is increasing, and governments are struggling to keep up.

Case studies: Governments close the gap

Singapore's SkillsFuture Program

The Singapore government aims to increase the number of digitally skilled workers by 55 percent, from the current 2.2 million in the workforce. The [SkillsFuture program](#) is designed to provide Singaporeans with the skills they need, with an emphasis in four key areas: automation, cybersecurity risk, data analytics, and in-demand digital tools.

The program is a collaboration between the government, education, and training providers, employers, and unions. In 2023, more than 660,000 people used the program to increase their skillset.

United States Digital Service

The [U.S. Digital Service](#) was founded to bring together the best engineering, design, and government talent to change the US Government's approach to technology.

Through the program, top designers, engineers, product managers, and digital policy experts are recruited and paired with civil servants to address some of the most critical government services. The U.S. Digital Service has worked with more than 20 federal agencies to build their digital abilities.

Saudi Arabia FutureX

Saudi Arabia has launched FutureX, an initiative that prepares students, professionals, and job seekers to compete in the modern labor market by teaching them emerging technical skills.

The initiative brings together local and global education providers into one national platform to provide online learning to Saudi residents.

New York State Department of Labor reskilling and upskilling program

During the pandemic, which cost New York State more than [1.7 million private sector jobs](#), the New York State Department of Labor (NYSDOL) provided [free access to skills training on Coursera](#).

The program includes learning courses for ten economic regions, including finance and manufacturing, and incorporates micro-credentials and entry-level professional certificates from companies such as Google and Meta.

To date, learners have completed more than 1.5 million lessons in fields such as business, technology, and data science.

How to address the skills gap in government

As these case studies show, there are several key ways governments can help address the digital skills gap in the public sector. In addition to the examples above, governments can focus on the following areas:

Reskilling and upskilling existing employees

Training and retaining existing employees are critical to addressing the skills gap in government. By focusing on non-degree, skill-building programs and [micro-credentials](#), governments can reskill and upskill existing employees. Investing in employees' skillsets will also increase retention.

Investing in technology

According to IDC,¹¹ new technology, such as AI, can help agencies combat skills challenges by:

- Automating manual, repeatable tasks.
- Providing next-generation training and skills development.
- Improving analytics and decision-making with AI insights.

Investing in technology helps improve the employee experience and frees up time to focus on core work activities, which can also impact retention.

Adopting flexible work models to attract and retain talent

The pandemic changed the way we work. According to [Forrester](#), one-third of global civil servants will become permanent hybrid workers. Although the pendulum may be swinging back toward on-site workplaces,¹² hybrid work models are now table stakes for attracting and retaining top talent. The public sector must adapt its work models to remain competitive.

¹¹ IDC PlanScape: Leveraging AI to Address the Skills Gap in Federal Agencies, June 2023, IDC #US50308423

¹² BBC, *Amazon tells staff to get back to office five days a week*, 2024



6. Cybersecurity

Government computers and networks are a critical path to sensitive data and are central to operations. Malicious access and unauthorized changes to these systems can have a significant impact on an agency's operations and, potentially, that of the country.

The global cybersecurity market has been growing at a rate of 11-12 percent over the past several years.¹³ This is in direct correlation to an increase in threats.

The public sector is a top target of malicious actors. According to PwC, [11 percent of cyberattacks](#) in Canada last year targeted the public sector, ranking third behind telecom and healthcare organizations.

Smarter governments are taking a holistic approach to cybersecurity, leaning on tools that provide detection, response, and remediation in a zero trust environment.

What is zero trust?

In a zero trust environment, cybersecurity no longer focuses on protecting static, network-based perimeters but rather focuses on users, assets, and resources. In February 2020, the National Institute of Standards and Technology (NIST) updated its Special Publication 800-207 to help to make the case for zero trust in government. The DoD has publicly stated a goal to operate in a total zero trust cybersecurity environment by the end of fiscal year 2027.¹⁴

According to the NIST, [zero trust](#) is a cybersecurity paradigm that assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location.

In the US, the President's Executive Order (EO)14028, "[Improving the Nation's Cybersecurity](#)," calls for eight technology mandates to enhance cybersecurity, including implementing a NIST-oriented zero trust architecture, enhancing software supply chain security, and improving vulnerability detection on federal networks.

The zero trust security model is now in its fourth year since the NIST's Special Publication 800-207. Today, zero trust is widely adopted globally and is a solid framework to secure government data and infrastructure.

Cybersecurity challenges facing government

According to the US Government Accountability Office (GAO), the public sector faces [four cybersecurity challenges](#). Although the GAO's report is specific to the US, these insights can be applied globally to help strengthen cybersecurity in the public sector.

First, national cybersecurity strategies aren't as strong as they could be. The GAO notes that governments need to have outcome-oriented performance measures, ensure monitoring of the global supply chain, recruit more employees highly skilled in cybersecurity, and address the risks associated with emerging technologies such as AI.

¹³ Wall Street Journal, *Cybersecurity Budgets Grow, But at a Slower Pace*, 2023

¹⁴ DOD Cyber Officials Detail Progress on Zero Trust Framework Roadmap > U.S. Department of Defense > Defense Department News

The risks of not having a strong cybersecurity strategy are high. NIST warned that users coming from another trusted network or location—where their credentials had already been verified—are normally given full access to data and agency resources without any further review, even though they could be a potential threat.

This is exactly what happened in the SolarWinds attack: malicious, trojan-ized updates to SolarWinds' Orion® network management software made their way into approximately 18,000 enterprises, government agencies, and other organizations around the globe. With a strong cybersecurity strategy that implemented a zero trust framework, this kind of attack might have been avoided.

Second, agencies are limited in their ability to improve the security of federal systems and information. Federal agencies rely on information systems for their day-to-day activities, and these systems often hold sensitive citizen data. Ineffective security controls not only leave systems vulnerable but can also delay responses to attacks.

Third, critical infrastructure sectors such as healthcare and defense remain vulnerable to disruptive attacks. These sectors present unique cybersecurity challenges to government as critical infrastructure sectors house sensitive citizen and national security information. As attacks on critical infrastructure sectors continue to grow, governments will need to take concrete steps to enhance cybersecurity.

Fourth, efforts to protect citizens' personal privacy face limitations. As the amount of citizen data collected by corporations continues to increase, governments will need to create and implement privacy laws like the GDPR to manage its collection and use.

Governments are also facing [cybersecurity challenges](#) related to the increase in ransomware and supply chain attacks, as well as a lack of skilled cybersecurity professionals. According to [WatchGuard](#), ransomware attacks targeting the public sector increased by 95 percent in 2022 compared to the same period the year before.

The demand for skilled cybersecurity professionals is being felt throughout industry as well as in the public sector. To combat these resource challenges, governments can turn to trusted managed security service providers like OpenText to help fill the skills gap.

Applying zero trust to government

OpenText has several offerings that can help the public sector in their journey to zero trust.

[OpenText™ Advanced Authentication \(NetIQ™\)](#) provides security solutions that help organizations with workforce and consumer identity and access management at enterprise-scale. By providing secure access, effective governance, scalable automation, and actionable insight, OpenText customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

[OpenText™ Application Security \(Fortify™\)](#), which is FedRAMP authorized, includes a suite of cybersecurity products for application security (AppSec) testing. Products include

- **OpenText™ Core Application Security (Fortify™ On Demand)**, an AppSec as a Service offering.
- **OpenText™ Dynamic Application Security Testing (Fortify™ WebInspect)**, a dynamic application security testing (DAST) offering.
- **OpenText™ Static Application Security Testing (Fortify™ Static Code Analyzer)**, which can pinpoint the root cause of security vulnerabilities in the source code.
- **OpenText™ Fortify™ Aviator**, an AI code security tool that executes fast auditing, identification, and automated code fix suggestions for SAST vulnerabilities with the power of AI.

Read more about OpenText's zero trust capabilities in our cybersecurity ebook, [Zeroing in on Zero Trust: Why federal agencies must take a threat-informed defense approach](#).





7. Defense and intelligence agencies

The stakes are higher in the defense sector; lives are literally on the line if defense organizations do not keep pace with their adversaries.

Unfortunately, digital transformation in global defense has been slow. Defense and Intelligence agencies are burdened with unstructured content, legacy technology, and manual processes. As much as 90 percent of collected data is never used,¹⁵ which can contribute to mission failure.

For many defense agencies, systems, and organizational processes are siloed and inefficient, struggling to keep up with the required pace of operations.

Defense and intelligence agencies need to connect, access, and leverage information to sharpen decision-making and improve mission effectiveness. AI and other emerging technologies can help, but national security agencies need a secure content management solution to optimize data usage and mitigate risk.

By implementing a strong information management strategy, agencies can enhance information availability, bridge process gaps, and create a single source of operating truth.

Defense modernization

Highly complex operations and budgetary pressures have placed a spotlight on defense modernization. Finding innovative ways to manage information improves frontline and back-end operations. By embracing digital process automation of workflows and automating where possible, agencies can save significant costs.

Information management can help agencies digitize and automate critical support functions, such as personnel changes, finance, and HR, while increasing the value of information available. By connecting content across existing enterprise applications, such as SAP®, Microsoft®, ServiceNow®, Oracle®, and Salesforce®, warfighters gain access to current information when and where it's needed. OpenText also enables the automation of key tasks and processes, while providing a flexible platform for rapidly building user-centric applications.

The Dutch Ministry of Defence

With more than 78,000 employees, the Ministry of Defence is one of the largest employers in the Netherlands. To manage all its operating processes, the Ministry's existing IT architecture was big and broad, consisting of more than 3,000 applications. Each application supported only a small part of a process.

The ministry wanted a single platform that could support complete processes to reduce complexity and maintenance costs. With OpenText, the organization gained a single integrated platform to connect processes across departments, including HR, logistics, and finance, reducing cost and complexity while optimizing business processes.

¹⁵ Forbes, *The Unseen Data Conundrum*, February 2022

Intelligence, analysis, and insight

Defense and intelligence agencies manage massive amounts of data. Processing, analyzing, and taking action on intelligence become increasingly difficult due to the sheer volume.

OpenText enables agencies to access and collect structured and unstructured information from virtually any source. This data can then be fed into AI and machine learning solutions to quickly produce useful, actionable analysis from all content types, including text, audio, and video.

By combining AI with advanced analytics, agencies can identify and manage the most vital data quickly and accurately, enabling real-time intelligence for better decision-making, situational readiness, and performance.

United States Air Force

The [United States Air Force's](#) (USAF) mission is to preserve the peace and security, and provide for the defense, of the United States. Technology plays a key role, particularly with innovations in AI and cybersecurity. As a leading-edge organization within the DoD, USAF is ideally positioned to take a leadership role by delivering applications rapidly and in a secure manner.

By centrally creating and maintaining DevSecOps platforms, rather than just DevOps processes, the USAF found they could avoid each DoD service building their own stack and reinventing the wheel.

Through OpenText Fortify, the central DevSecOps platform, called Platform One, allows users to deploy a DevSecOps platform for shorter development cycles, baked-in runtime security, and more focus on mission software.

The modular approach uses a secure Kubernetes platform for hosting microservices. This flexible structure means that development teams can define their exact criteria to determine when an application is ready for release.

Supply chain traceability

With evolving threats, hazards, and disruption risks, the defense sector faces significant supply chain challenges. On top of these challenges, understanding and tracking the origin of raw materials and components is critical to national security, driving a need for end-to-end traceability of items throughout the supply chain.

Modernization and digitization are critical to ensuring supply chain traceability—and doing so can bring significant cost savings. In fact, McKinsey estimates that advancing digital maturity along the aerospace and defense value chain could unlock \$20 billion in annual value.¹⁶

OpenText helps defense organizations streamline, connect, and automate supply chain processes, gaining end-to-end visibility of shipments and assets across extended ecosystems.

By leveraging the world's largest B2B integration network, agencies can connect everyone involved in the supply chain, drawing together disparate systems and partner networks to ensure that information can flow whenever and wherever it's needed.

¹⁶ McKinsey Digital, *The next horizon for global aerospace and defense*, March 2021



8. Educational Institutions

Academic institutions use a plethora of information to recruit new students, drive funding, and engage with current students, faculty, staff, and alumni.

Unfortunately, disconnected systems across departments and individual schools make it difficult to find the correct files, adhere to brand guidelines, and ensure the appropriate security and governance rules are applied.

Universities are increasingly investing in digital transformation, with 33 percent employing a senior technology officer whose primary responsibility is overseeing innovation. Additionally, 42 percent of university CIOs say digital transformation is “essential” or a “high priority.”¹⁷

Information management puts content at the core of operations, helping schools reduce repetitive tasks; eliminate information silos; maintain compliance; and improve how HR, finance, marketing, and advancement departments operate.

Key challenges and trends

Secure information management

Educational institutions need lifecycle content management solutions with automated workflows to boost productivity and enable seamless collaboration within a secure and compliant environment.

For example, the [University of Texas at Austin \(UT Austin\)](#) had disparate methods for managing content across departments. The University retained paper records dating back many years in large storage warehouses, and had current documents filed in cabinets in offices. Administrative staff devoted considerable time to finding and retrieving documents.

Some departmental teams had implemented their own digital document management systems, while others relied on digital copies held on shared drives or public cloud services. However, maintaining effective security and compliance oversight of these multiple, isolated systems presented significant challenges.

With OpenText™ Documentum™ Content Management D2, UT Austin is transforming administrative staff productivity, streamlining content management, and providing students and faculty with easier access to information. This transformation has resulted in a 38 percent improvement in administration productivity.

Compliance

Data breaches are doing more harm in higher education than other sectors. In higher ed, data breaches cost \$200 per record, compared to \$141 in other sectors.¹⁸ This is partly because education institutions have strict compliance regulations to adhere to, highlighting the need for enhanced information protection.

¹⁷ Inside Higher Ed., *2022 Survey of Campus Chief Technology/Information Officers, 2022*

¹⁸ Ponemon Institute, *Cost of a Data Breach Report 2021*

The [Metropolitan School District of Wayne Township](#) educates a large student body spread across a broad area. To keep the system working, everyone in the district needs to communicate quickly and effectively while maintaining compliance with the Family Education Rights Privacy Act (FERPA) law.

The district's communications infrastructure needed to be rebuilt to make its team more accessible and better equipped to support students and their families. OpenText™ CX-E Voice and OpenText™ XM Fax™ gave MSD Wayne employees the ability to send and access voicemails anywhere, secure faxing, a multilingual automated attendant, and 24/7 coverage without redundancy. The improved communications ease FERPA compliance while increasing efficiency.

Budget cuts and legacy infrastructure

Colleges and universities continue to reduce funding in legacy infrastructure and data center technologies, shifting budgets to focus on accelerating their cloud migration.

Many higher education CIOs have either invested in or are considering AI (53%) and machine learning (47%), underscoring the move to modernization. However, this transition to emerging technology presents new challenges.

The [University of Pretoria](#) in South Africa sought to implement an AI-powered service desk to meet the needs of its staff, faculty, and students. They were challenged with addressing the need for a scalable solution due to resource strain, bridging gaps in device access and connectivity, overcoming resistance, and aligning diverse departments for non-IT adaptation.

Information management in higher education

When institutions bridge information silos they can drive loyalty across students, faculty, staff, and alumni with more powerful and enjoyable experiences.

With information management, educational institutions can:

- **Empower human resources:** By automating and digitizing HR processes, schools can bring together information across applications to gain a single, secure source of operational truth and boost HR productivity.
- **Fuel finance and procurement:** By automating complex processes and connecting finance- and procurement-related information, schools can bring efficiency to these processes, including accounts payable, accounts receivable, invoice processing, expense reimbursement, and vendor management.
- **Engage donors and accelerate advancement:** By sunseting slow and outdated paper-based processes in favor of modernized digital experiences that integrate content across multiple systems. This allows personalizing engagement, increases agility and scalability, and accelerates time-to-funding.

Schools can increase donor interest, revenue and long-term loyalty which, in turn, allows them to focus on their primary missions of teaching, research, and student support.

Learn more about OpenText education solutions by visiting our [Education webpage](#).



9. Selecting your technology partner

Governments are facing significant challenges when it comes to information management, and new technologies such as AI and the cloud. The partner you select should be a clear leader in the information management domain.

Here are some considerations to think about:

1. Scalability

Your partner should be able to support you as you scale across departments, business units, ecosystems, and more. As your business scales, your information management solutions should scale as well.

2. Public sector experience

Public sector agencies face specific challenges and having a technology partner who understands these challenges, and is FedRAMP authorized, can give you peace of mind.

3. Integration expertise

To get the most out of your information management journey, you need to ensure that your technology partner has deep integration capabilities that match your existing technology investments.

4. Breadth of solutions

Having one technology partner with the breadth of solutions you need can help save costs and the complexity of having multiple technology partners.

5. Information management leadership

Successful AI deployments in the public sector demand superior information management for reliability, accuracy, and security.



10. 7 top tips for digital transformation in government

Here are seven handy tips to help public sector agencies as they embark on their information management journey.

1. Digitize paper-based processes

Digitizing paper-based workflows allows governments to make significant improvements in employee and citizen experience. It also helps governments meet ESG targets, reduce costs, and increase operational efficiencies.

2. Modernize legacy systems

Modernizing legacy systems with low-code or no-code development enables agencies to flexibly adapt to changes in circumstances, reduce downtime, and mitigate risk.

3. Archive information while retiring systems

Properly modernizing legacy systems and digitizing paper-based workflows includes retiring legacy systems and archiving information. With increases in government directives related to digital technology (e.g., reducing technical debt across the public sector), compliant archival strategies are now top of mind.

4. Enable Total Citizen Experience

The public sector needs to deliver superior digital experiences to keep citizens satisfied. Improving both employee and citizen experience in a secure way increases public trust.

5. Adopt new technologies

New technologies, such as the cloud and AI, have the potential to make governments more efficient and effective with increased automation, insights, and more.

6. Adopt a zero trust framework

Shift the focus of cybersecurity from protecting static, network-based perimeters to focus on users, assets, and resources. Adopting a zero trust framework allows governments to secure their data and infrastructure.

7. Partner with an information management leader

A modern information management system can help with all areas of government, from cybersecurity to cloud migrations to AI-fueled analytics to citizen experience. Partnering with an information management leader gives public sector agencies a competitive edge in their digital transformation journey.

OpenText provides the world's most comprehensive set of modern information management solutions to help the public sector manage structured and unstructured information end to end.