

# Modernizing sovereign cloud workloads with OpenText and AWS

How federal agencies can manage, secure, and scale FedRAMP, Protected B, and IRAP workloads across systems



---

## Contents

|                                                                                         |    |
|-----------------------------------------------------------------------------------------|----|
| Executive summary                                                                       | 3  |
| Modernizing FedRAMP workloads for federal agencies                                      | 4  |
| Supporting mission outcomes in FedRAMP environments                                     | 5  |
| OpenText on AWS: Content management, IT asset management,<br>and cybersecurity together | 6  |
| How OpenText and AWS work together                                                      | 7  |
| Key federal use cases                                                                   | 9  |
| Sovereign cloud: Local control at global scale                                          | 10 |
| Roadmap and future investments                                                          | 11 |
| Getting started with OpenText and AWS                                                   | 13 |

---

## Executive summary

Federal agencies are under pressure to modernize faster, operate more securely, and deliver better services with constrained resources. Cloud adoption has accelerated that shift, but moving workloads to FedRAMP-authorized infrastructure is only the first step. Agencies still need to manage large volumes of regulated content, automate complex processes, and maintain consistent security controls across systems that were never designed to work together.

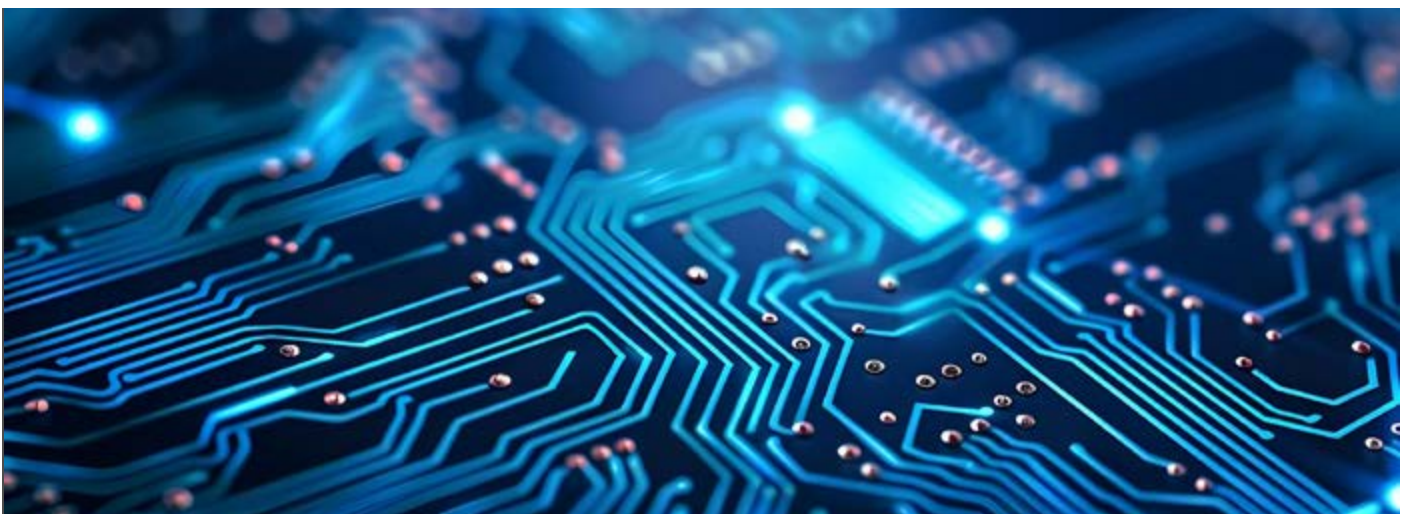
The gap between cloud infrastructure and operational readiness is where missions stall.

OpenText, an AWS Partner, closes that gap. Its FedRAMP-authorized solutions combine enterprise content management, process automation, IT asset management, and cybersecurity, all running on AWS. Together, these capabilities give agencies a single, governed environment to manage and protect information across their full lifecycle. Agencies maintain control and visibility while enhancing the value of SAP, Microsoft, Salesforce, and other systems driving their operations.

The impact is measurable: [43% of employees struggle to access the information](#) they need because it's scattered across multiple systems. Digitizing operations improves collaboration, reduces complexity, and ensures agency-wide compliance.

With IL5 authorization for DoD workloads, deeper SAP integration, data discovery and protection solutions, and Aviator AI capabilities on the roadmap for FedRAMP authorization in 2026, OpenText is expanding to support the most sensitive and complex federal use cases.

This paper outlines how OpenText and AWS help agencies move from infrastructure modernization to operational transformation.





## Modernizing FedRAMP workloads for federal agencies

Federal agencies have made significant progress moving workloads to the cloud. FedRAMP-authorized environments now support a growing share of mission-critical systems, from benefits administration and grants management to national security operations. The shift is accelerating, driven by executive mandates, zero trust adoption requirements, and the practical need to scale capacity without proportional increases in infrastructure cost.

Yet modernization is not just an infrastructure problem. As agencies move to the cloud, they carry with them the full complexity of their operations: large volumes of regulated content, deeply integrated legacy systems, distributed workforces, and compliance obligations that span multiple frameworks. The cloud provides the foundation, but agencies still need to govern what they run on it.

Three operational pressures dominate the agenda for most federal IT and security leaders today:

- Security and compliance requirements that span FedRAMP, FISMA, NIST 800-53, and, in Canada and Australia, Protected B and IRAP frameworks
- Large volumes of content and records that must be managed, retained, and made accessible in accordance with federal records law and mission need
- Multiple systems and distributed teams that operate across organizational boundaries, requiring integration rather than consolidation

The central challenge is that content, processes, and security are typically handled by separate tools, managed by separate teams, and governed by separate policies. The result is fragmented visibility, duplicated effort, and compliance gaps that grow harder to address as workloads scale.

Agencies need a unified approach: one that manages regulated workloads, automates processes, and applies consistent security controls without requiring a complete overhaul of existing systems. That approach must also be AI-ready, as agencies begin to operationalize machine learning and generative AI capabilities within their compliance boundaries.

## The infrastructure gap

FedRAMP authorization covers the platform. Content governance, process automation, records management, and application security require purpose-built capabilities running on top of that platform. OpenText fills this gap within the AWS environment federal agencies already use.

## Supporting mission outcomes in FedRAMP environments

Agencies are under pressure to do more with existing resources. Constituents and oversight bodies expect faster services, cleaner audits, and better information access. Meanwhile, IT and security teams face workforce constraints, technology debt, and the ongoing challenge of keeping pace with evolving threat landscapes.

These pressures converge on several common challenges:

- Disconnected systems that require manual reconciliation and create information silos
- Manual processes that slow service delivery and introduce error and compliance risk
- Limited visibility into workflows and data, making it difficult to answer audit inquiries, optimize operations, or respond to incidents

AWS addresses the infrastructure layer of this problem. As a leading FedRAMP-authorized cloud provider, AWS delivers the secure, scalable compute, storage, and networking that agencies need to run regulated workloads. AWS GovCloud regions provide the physical and logical separation required for sensitive data, and AWS's investment in compliance automation accelerates authorization timelines for agencies and their technology partners.

But infrastructure alone does not address content, process, and governance needs. Storing data securely in the cloud does not make it easier to find, act on, or retain appropriately. Secure networks do not automate the workflows that move information between systems. Compliance certifications for the platform do not substitute for governance controls applied to the workloads running on it.





## OpenText on AWS: Content management, IT asset management, and cybersecurity together

OpenText brings together capabilities that agencies typically source from multiple vendors: enterprise content management, process automation, IT asset management, and cybersecurity. Running these capabilities on a shared AWS infrastructure, under a unified governance model, reduces the operational complexity and added expense that comes with managing disparate tools.

### Enterprise content management

OpenText's content management platform provides a secure, FedRAMP-authorized repository for agency documents, records, and unstructured data. Agencies can manage content across its full lifecycle: from creation and collaboration through retention, disposition, and legal hold. Role-based access controls, audit trails, and metadata-driven classification apply consistent governance regardless of where content originates.

### Process automation

OpenText automates the workflows that route content and drive decisions through agency operations. Case intake, approvals, notifications, and routing can be configured using a low-code development kit, reducing the time and cost of implementing new processes. Automation reduces manual touchpoints, lowers error rates, and creates audit-ready records of every action taken.

### IT asset management

IT asset management is a core component of OpenText's FedRAMP offering. Agencies maintain visibility into hardware and software assets across their environments, supporting both compliance reporting and operational decision-making. Asset data integrates with content and process workflows, connecting the information an agency has about its technology to the work being done with it.

### Cybersecurity

OpenText's cybersecurity capabilities address application security testing, vulnerability management, and sensitive data discovery. Data discovery and protection tools locate regulated data across systems and automatically apply masking or protection controls. AI-powered application security testing identifies vulnerabilities earlier in the development lifecycle, reducing remediation cost and risk exposure. These capabilities are available within the FedRAMP boundary, allowing agencies to run security workflows without moving sensitive data outside their authorized environment.

The combined effect is a reduction in reliance on multiple point tools, improved control across workloads, and a consistent governance posture that can be demonstrated to auditors and oversight bodies.

## AWS global infrastructure

26

Regions

85

Zones

245

Countries and territories

200

Global cloud-based services

## How OpenText and AWS work together

OpenText applications run natively on AWS infrastructure within FedRAMP-authorized boundaries. The architecture is designed for agencies that need cloud-scale performance, compliance assurance, and integration with the systems already embedded in their operations.

### OpenText brings

- 30 years of experience helping the world's largest organizations extract value from information
- Expertise as the provider of information management solutions to the U.S. government
- More than 3,700 public sector customers, including 20 of the 20 largest national governments based on GDP
- 68,000 cloud customers worldwide
- 3,000 Cloud Managed Services customers
- FedRAMP High, DOD IL5, IRAP, and Protected B authorized solutions
- Integrated enterprise content management, process automation, IT asset management, and cybersecurity on AWS
- The most comprehensive portfolio of integrated content and information management solutions available, including content services, Government-to-Government (G2G) integration, AI and analytics, and information security

### AWS brings

- More than 1,000 FedRAMP authorized cloud solutions, more than the next two public clouds combined, with 7,500 U.S. government agency customers
- An extensive global cloud footprint spanning 84 availability zones within 26 geographic regions, serving 245 countries and territories
- A deep set of cloud security tools, with 230 security, compliance, and governance features and 98 security and compliance certifications
- More than 200 global cloud-based services, from infrastructure technologies like compute and storage to emerging technologies like data lakes and Internet of Things
- A reputation for driving down the cost of IaaS
- Excellence as the named world leader in cloud infrastructure as a service



## Core capabilities

- Secure content management, with encryption at rest and in transit, role-based permissions, and immutable audit logs
- Role-based access and policy enforcement across content, processes, and data assets
- Workflow and process automation that spans content intake, routing, approvals, and records management
- Sensitive data discovery and automated classification to support privacy compliance and risk reduction

## System integrations

Agencies do not need to replace existing systems to benefit from OpenText on AWS. OpenText integrates directly with the platforms already installed in government:

- **SAP:** Connect content and process workflows to financial, procurement, and HR transactions
- **Microsoft 365:** Extend governance and records management to Teams, SharePoint, and Exchange content
- **Salesforce:** Apply content management and process automation to constituent service and case workflows

These integrations allow agencies to apply consistent governance across systems without requiring users to change how they work. Content and process controls operate in the background, capturing records and enforcing policy without disrupting existing workflows.

## Deployment options

OpenText on AWS supports multiple deployment models to accommodate agency procurement preferences and technical requirements:

- Cloud-native SaaS applications, managed by OpenText within the FedRAMP boundary
- Managed services with OpenText operating the environment on behalf of the agency

Both models reduce the operational burden on agency IT teams, accelerate time to deployment, and maintain the compliance posture required for FedRAMP authorization.



## Key federal use cases

OpenText and AWS support a range of mission-critical use cases across federal agencies. The following represent the highest-impact deployment patterns based on agency operational needs and FedRAMP compliance requirements.

### Case management

Agencies managing benefits, investigations, permits, or constituent services require connected, auditable case records. OpenText connects information across systems into a unified case file, applies workflow automation to move cases through processing stages, and provides supervisors and auditors with complete visibility into case history. The result is faster response times, lower manual processing costs, and defensible documentation for oversight purposes.

### Records management and information governance

Federal records law requires agencies to manage records from creation through disposition. OpenText applies retention schedules, legal hold capabilities, and automated classification to content wherever it lives, including within M365 environments. Agencies can respond to FOIA requests, support audits, and demonstrate compliance with NARA requirements without manual file review.

### Low-code process automation

Across agency operations, manual processes create bottlenecks, introduce errors, and consume staff time that could be directed toward higher-value work. OpenText automates document intake, routing, approval workflows, and notifications, reducing cycle times and creating complete records of every process step. Agencies report significant reductions in processing time and improved accuracy after deploying automated workflows.

### Digital services

Citizens and agency employees expect digital interactions that are fast, clear, and responsive. OpenText supports digital forms, document submission, and status communication, improving the experience for people interacting with agency services while reducing the administrative burden on agency staff.

### Data discovery and risk mitigation

Regulated data that agencies do not know they have represents both a compliance risk and a security vulnerability. OpenText's data discovery capability locates sensitive information across structured and unstructured data stores, automatically classifies it, and applies masking or protection controls. This capability is available via IRAP authorization for Australian government environments and is expected to achieve FedRAMP authorization in 2026.

---

## What sovereign cloud means in practice

Data residency stays within the authorized jurisdiction. Legal access is governed by local law, not extraterritorial claims. AI and automation capabilities operate on the same infrastructure, subject to the same controls. Agencies get the benefits of cloud-scale AI without accepting data sovereignty trade-offs.

## Sovereign cloud: Local control at global scale

**Sovereign cloud** requirements extend beyond U.S. federal agencies. Allied governments in Canada, Australia, Europe, and elsewhere face their own data residency, jurisdiction, and compliance requirements. The OpenText approach to sovereign cloud is designed to address these needs across frameworks, including Protected B in Canada and IRAP in Australia, while maintaining a consistent architecture built on AWS.

OpenText defines sovereign cloud as a model that gives organizations full control over where their data lives, who can access it, and what legal framework governs its use. This matters for agencies operating sensitive workloads or handling information subject to jurisdictional restrictions. It also matters for multinational agencies and defense partners that need to collaborate across boundaries without compromising the sovereignty of each party's data.

OpenText and AWS are expanding this capability. Building on existing North American federal deployments, OpenText is extending its sovereign cloud architecture to support regulated European Union organizations through AWS European Sovereign Cloud infrastructure. This hybrid approach provides organizations with AI-ready data platforms that meet local requirements without sacrificing the scale and capability advantages of AWS.

## Agency in action: U.S. federal health agency

A United States federal health agency responsible for regulating the manufacturing, distribution, and marketing of over-the-counter, age-restricted drugs needed to modernize a complex, document-intensive approval process.

### Challenge

The approval process for new age-restricted products required thousands of highly technical and proprietary documents to be exchanged between vendors and government scientists. The agency needed to manage submissions, enable scientific review, and support ongoing correspondence with vendors throughout the evaluation process. The challenge was building complex data models and workflows in under a year, a timeline unprecedented for public sector technology projects.





## Solution

The agency deployed [OpenText™ Content Management](#) and [OpenText™ Process Automation](#) through the OpenText™ Cloud for Government solution. Submissions are automatically routed through workflows based on submission and approval type, then sent to government scientists for review. The OpenText Content Management platform routes documentation to multiple reviewers, enables collaborative editing, and streamlines the approval process. A Letter Generator tool allows the agency to correspond directly with vendors to request additional information or documentation. OpenText Process Automation, a low-code development platform, enables rapid prototyping of new functionality as requirements evolve.

## Results

The agency had the full solution up and running within nine months, an unprecedented timeline for a public sector technology project of this complexity.

- Deployed a document-centric workflow for electronic management of the drug approval process
- Enabled collaborative review and editing across government scientists
- Streamlined vendor correspondence through automated letter generation
- Positioned the agency to respond quickly to future functionality requests through low-code development

## Roadmap and future investments

OpenText is investing in capabilities that will expand the range of workloads agencies can run within FedRAMP and sovereign cloud boundaries. These investments address the most sensitive and complex use cases in the federal market, including classified-adjacent environments, tighter SAP integration, and AI capabilities that operate natively within the compliance boundary.

## IL5 authorization for DoD workloads

OpenText is pursuing Impact Level 5 (IL5) authorization to support Department of Defense (DoD) workloads that require higher security controls. IL5 covers Controlled Unclassified Information (CUI) at the highest sensitivity level below classified, including systems supporting national security operations. IL5 authorization is expected to allow DoD components to deploy OpenText content management and cybersecurity capabilities for workloads that cannot run in standard FedRAMP High environments.

## SAP integration

Most agencies run procurement in SAP and content in a separate system, which means approvals, source documents, and compliance records have to be manually linked or reconciled after the fact. Gaps in procurement documentation are one of the most common findings in federal audits and Inspector General (IG) reviews. OpenText integrates with SAP® Procurement for Public Sector to attach approvals, source documents, and compliance records

---

directly to SAP transactions, giving contracting officers a complete, audit-ready record tied to each transaction and eliminating the manual reconciliation that creates exposure in the first place.

This integration supports agencies modernizing procurement operations on SAP S/4HANA® Public Cloud while preserving the records governance requirements of federal contracting.

### **Expanded cybersecurity capabilities**

OpenText continues to invest in application security, vulnerability management, and sensitive data protection within the FedRAMP boundary. As agencies adopt DevSecOps practices and shift security testing earlier in the development lifecycle, OpenText AI-powered application security capabilities provide the tools to identify and remediate vulnerabilities before they reach production.

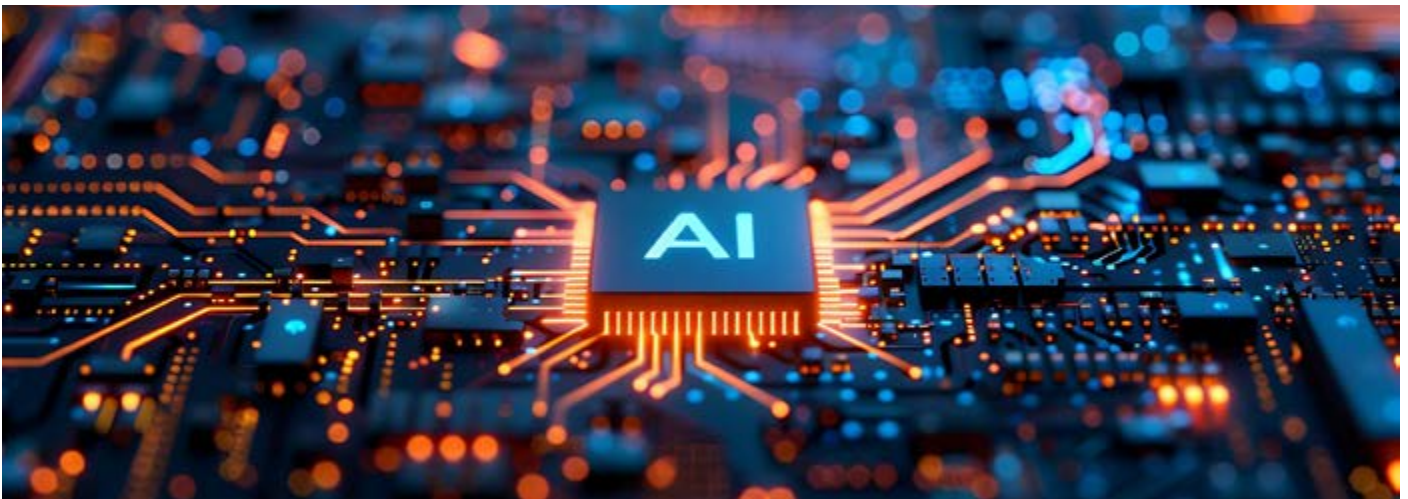
### **GenAI in sovereign cloud environments**

OpenText™ Aviator™ is the company's suite of generative AI capabilities, built to operate within enterprise data environments rather than relying on public AI models. OpenText is bringing Aviator functionality into future FedRAMP instances for all currently authorized products. This means agencies will be able to use AI-powered content analysis, automated summarization, intelligent search, and process assistance within their FedRAMP boundary, without sending sensitive data to external AI services.

Aviator operates on the agency's own data, within their authorized environment, with the same access controls and audit logging that govern the rest of the platform. This approach allows agencies to capture the productivity and mission benefits of generative AI while maintaining the data sovereignty and compliance posture that federal operations require.

### **Agentic workflows**

OpenText is extending Aviator into agentic automation, where AI can initiate and complete multi-step tasks across systems without manual intervention. For federal agencies, this means process automation that goes beyond routing and approvals to include intelligent triage, anomaly detection, and cross-system orchestration, all within the FedRAMP boundary.



---

## Ready to see it in action?

Schedule a demo to see how OpenText and AWS deliver secure, scalable cloud solutions for regulated government workloads.

[Schedule a demo >](#)

## Getting started with OpenText and AWS

OpenText and AWS provide a single approach to the content, process, and security needs of federal agencies. Rather than assembling separate tools for content management, records governance, workflow automation, and cybersecurity, agencies can deploy integrated capabilities on the AWS infrastructure they already use, within the FedRAMP boundary they have already authorized.

### What this means for agencies

- **Faster compliance readiness:** OpenText's FedRAMP-authorized capabilities address up to 80 percent of common compliance requirements, accelerating the path to authorization for new systems
- **Lower total cost of ownership:** Agencies consolidate point tools, reduce integration overhead, and benefit from managed cloud operations, with reported TCO reductions of up to 40 percent
- **Operational continuity:** Integration with SAP, Microsoft 365, and Salesforce means agencies can move data seamlessly into and out of existing systems without manual intervention
- **A clear AI path:** Aviator AI capabilities within the FedRAMP boundary give agencies a governed, compliant path to generative AI without data sovereignty risk
- **Future-ready architecture:** IL5 authorization in progress, sovereign cloud expansion underway, and continued investment in cybersecurity ensure that OpenText on AWS can support increasingly sensitive workloads over time.