Best Practices
Community

GovCloud

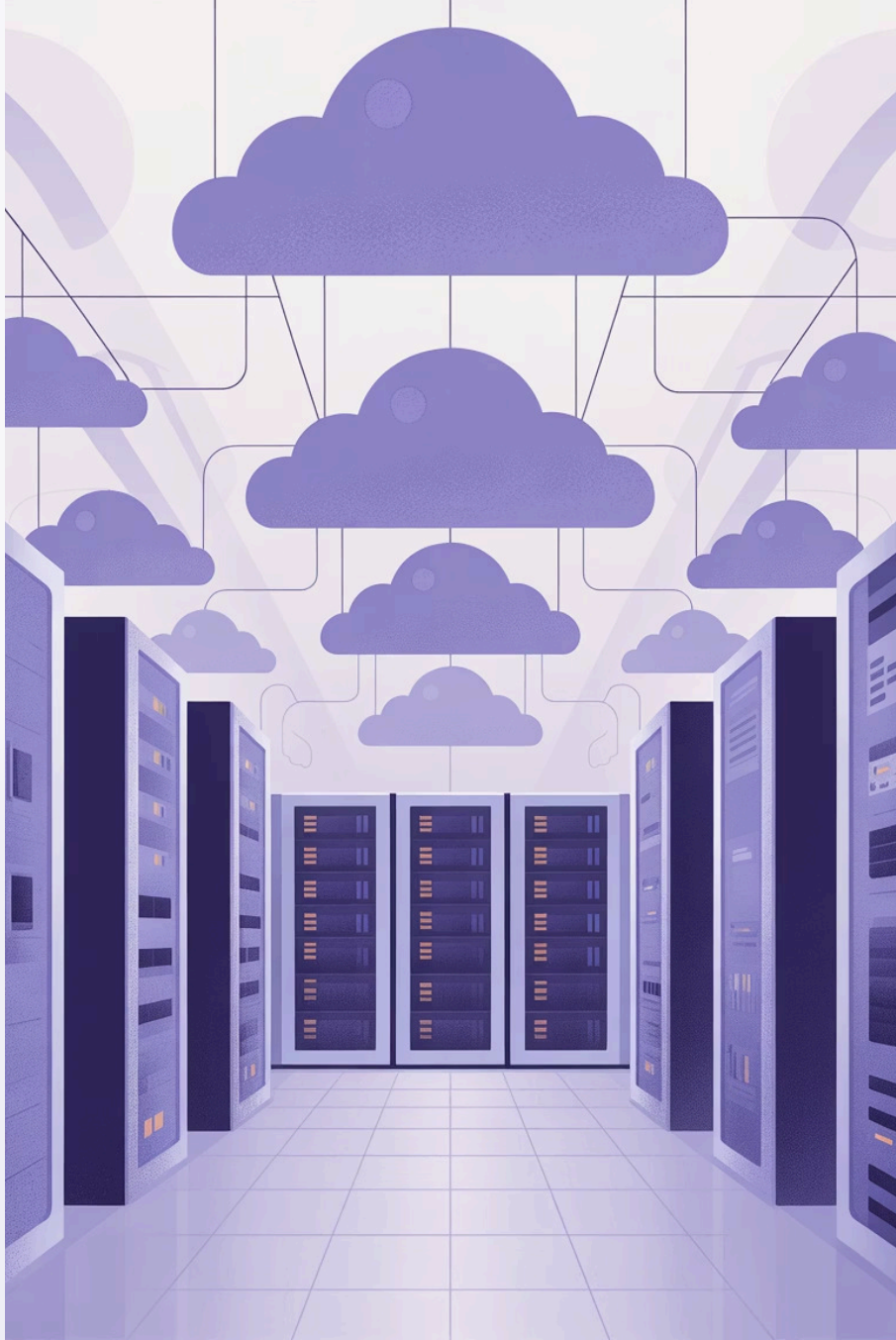
Secure Hosting and Application Solutions

Empowering and Accelerating Public Sector Digital Innovation

DigitalGov.network

GovCloud Best Practices and Vendor Solutions

Securing Government Cloud Adoption



Understanding GovCloud Environments

Chapter 1

What is GovCloud?

GovCloud represents dedicated cloud regions specifically tailored for government workloads with strict compliance needs. These isolated environments ensure data sovereignty whilst meeting the most demanding security standards.

Leading examples include AWS GovCloud (US), Azure Government, and Google Cloud Assured Workloads—each designed to address unique regulatory requirements.

FedRAMP Compliance

Rigorous authorisation processes

DoD Impact Levels

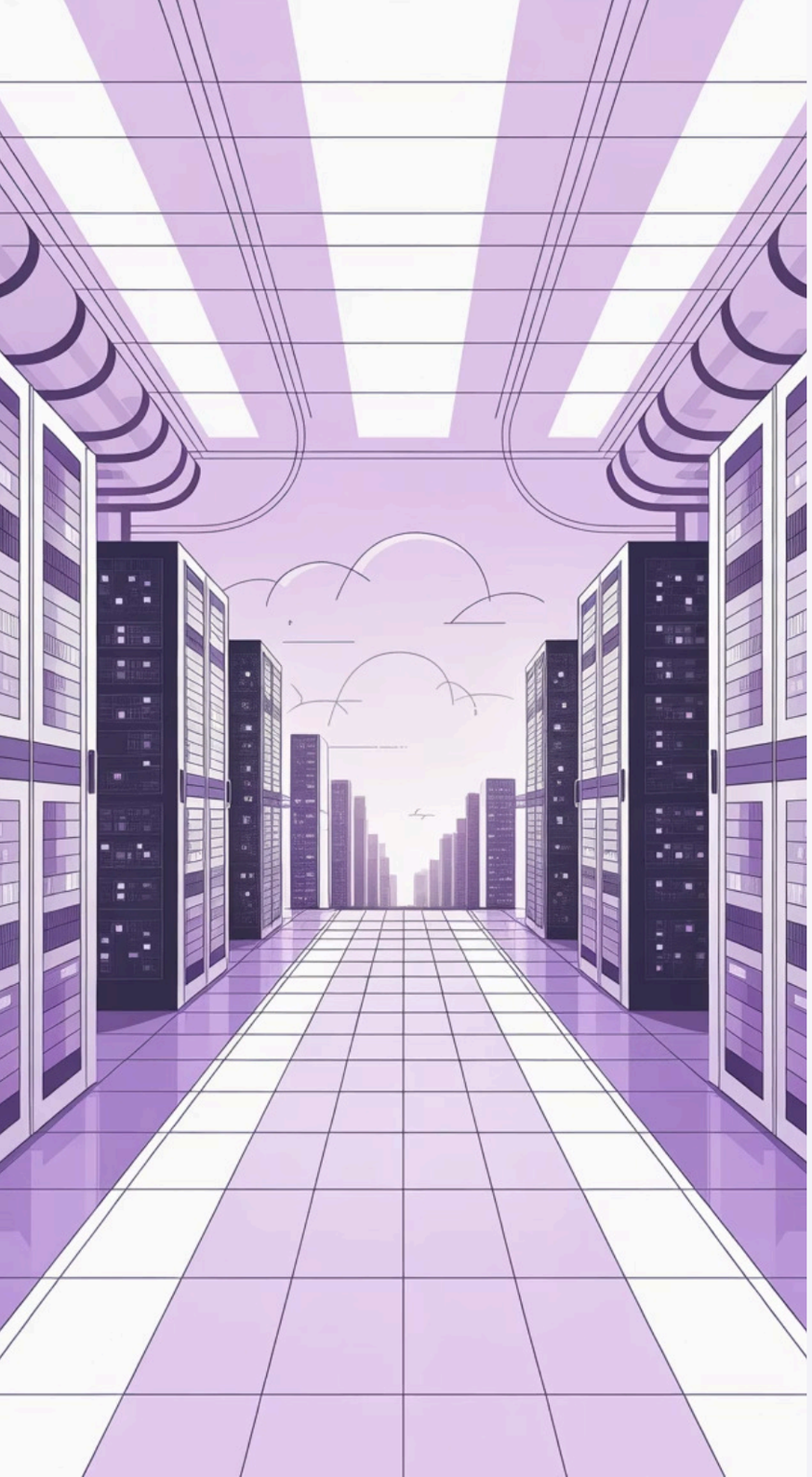
Military-grade security standards

ITAR & CJIS

Regulatory compliance built-in

Data Sovereignty

Complete territorial control



AWS GovCloud (US) Overview

1

Isolated US Regions

Two dedicated regions—GovCloud US-West and US-East—provide data sovereignty and redundancy. Physical and logical isolation ensures compliance with federal regulations whilst enabling disaster recovery capabilities.

2

FedRAMP High Authorisation

AWS GovCloud maintains FedRAMP High JAB P-ATO authorisation, demonstrating rigorous security compliance. This certification enables agencies to host highly sensitive data and mission-critical applications with confidence.

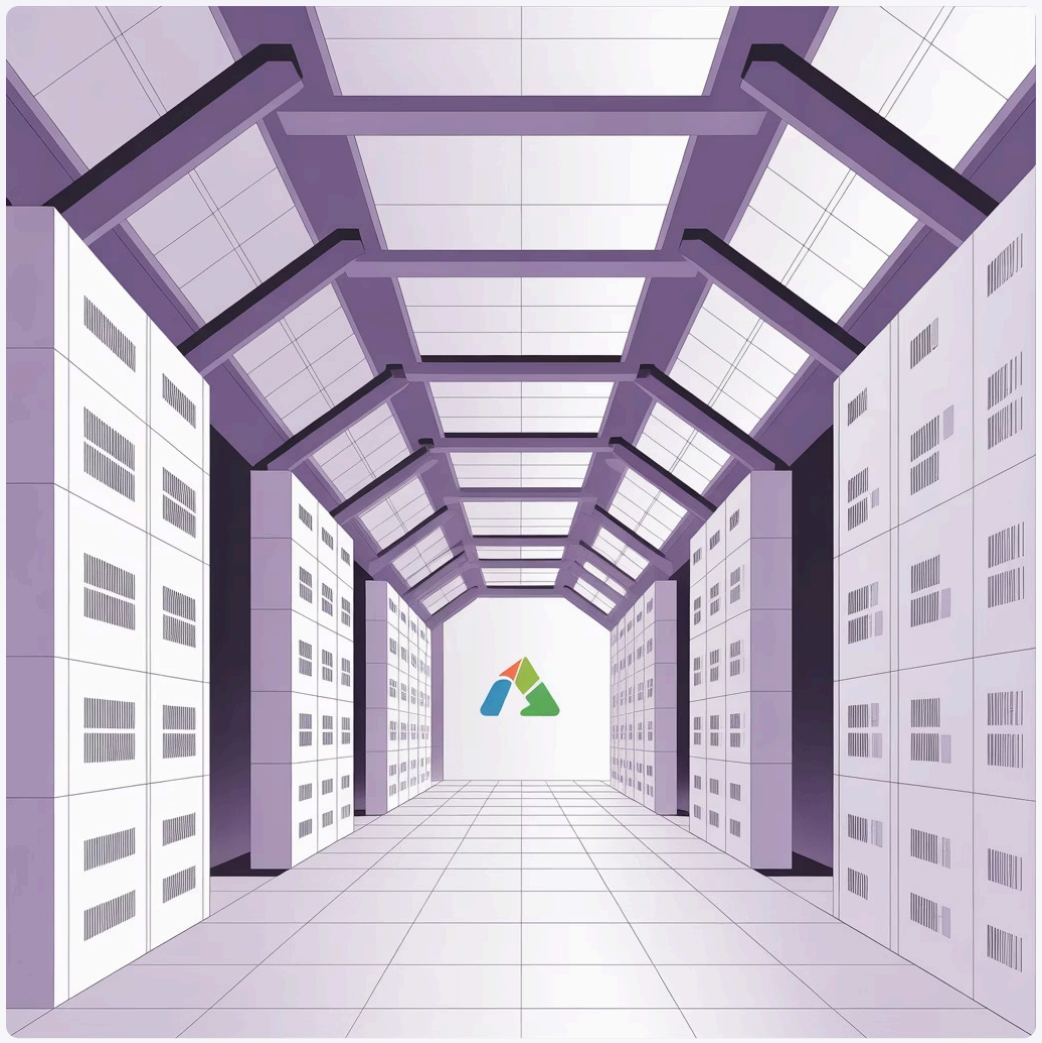
3

Restricted Access Controls

Access is strictly limited to vetted U.S. persons and entities, supporting sensitive and regulated workloads. This ensures that only authorised personnel can manage and access government data and systems.

Azure Government and Google Assured Workloads

Azure Government



Microsoft's Azure Government operates through physically isolated data centres dedicated exclusively to U.S. government entities. These facilities maintain separate network infrastructure and dedicated compliance certifications, including FedRAMP High and DoD Impact Level 5.

- Complete physical separation from commercial cloud
- Screened U.S. personnel only
- Enhanced compliance reporting

Google Cloud Assured Workloads

Google Cloud provides automated compliance controls through Assured Workloads, enabling government agencies to configure guardrails that enforce regulatory requirements. This approach supports both FedRAMP and other government standards.

- Automated policy enforcement
- Real-time compliance monitoring
- Multi-cloud strategy support

All three major providers support multi-cloud and hybrid strategies, which are increasingly common in modern government IT architectures.

GovCloud Geographic Footprint

AWS GovCloud Regions

US-West (Oregon) and US-East (Ohio) providing coast-to-coast coverage

Azure Government

Multiple US regions including Virginia, Texas, and Arizona with DoD-specific zones

Google Assured Workloads

Compliance controls available across US regions with automated governance

Best Practices for Adopting GovCloud

Chapter 2

Compliance and Eligibility Essentials

01

Confirm Organisational Eligibility

Federal, state, and local agencies, government contractors, educational institutions, and other qualified entities

02

Understand Shared Responsibility

CSPs secure infrastructure and physical facilities whilst customers secure data, applications, and access management

03

Review Responsibility Matrix

Obtain and thoroughly examine the CSP's customer responsibility matrix for clear compliance boundaries

> "Understanding where provider responsibility ends and customer responsibility begins is fundamental to maintaining compliance in GovCloud environments."

Identity and Access Management (IAM)

Zero Trust Architecture

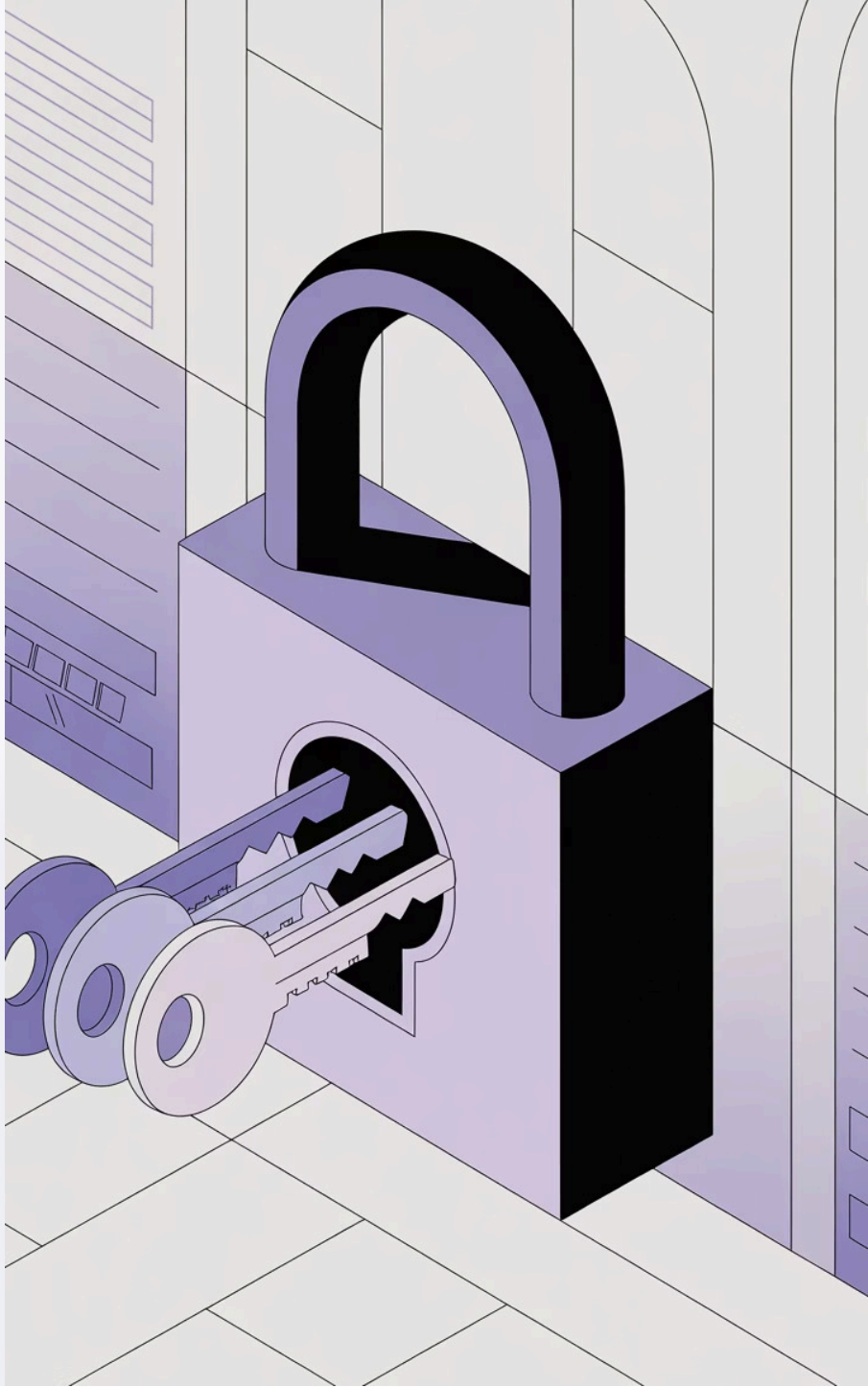
Enforce the Principle of Least Privilege and implement Zero Trust security models across all GovCloud environments. Never trust, always verify—even for internal network access.

Platform-Specific IAM

Leverage AWS IAM, Azure Active Directory with Role-Based Access Control (RBAC), and Google Cloud IAM—each tailored specifically for government use cases and compliance requirements.

Continuous Auditing

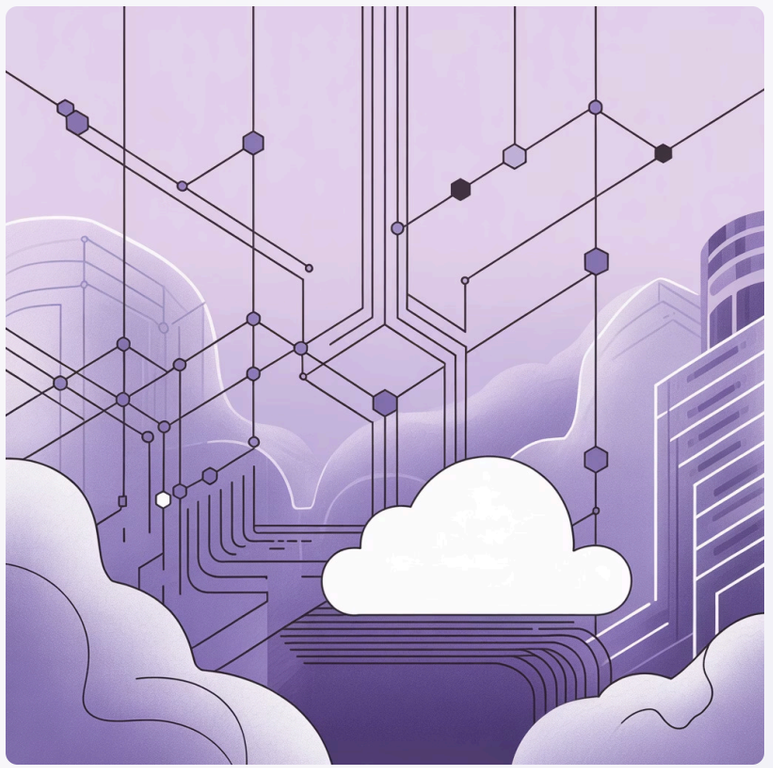
Regularly audit access permissions, rotate credentials on a defined schedule, and mandate multi-factor authentication (MFA) for all users without exception.



Infrastructure as Code (IaC) in GovCloud

Automation & Compliance

Infrastructure as Code is essential for maintaining consistent, auditable, and compliant GovCloud deployments. Automated provisioning reduces human error whilst ensuring security standards are met.



Region-Aware Templates

Utilise region- and partition-aware IaC templates using tools like Terraform and AWS CloudFormation. These templates must account for GovCloud-specific configurations and limitations.

Adapt Resource Identifiers

Modify Amazon Resource Names (ARNs) and resource identifiers for GovCloud partitions, such as `arn:aws-us-gov` instead of standard commercial partition identifiers.

CI/CD Integration

Integrate automated compliance checks and continuous monitoring directly into CI/CD pipelines, enabling rapid deployment whilst maintaining security posture.

Networking and Data Protection

Virtual Private Clouds

Configure VPCs with strict segmentation, firewall rules, and network access control lists to isolate workloads and limit lateral movement.

Compliance Validation

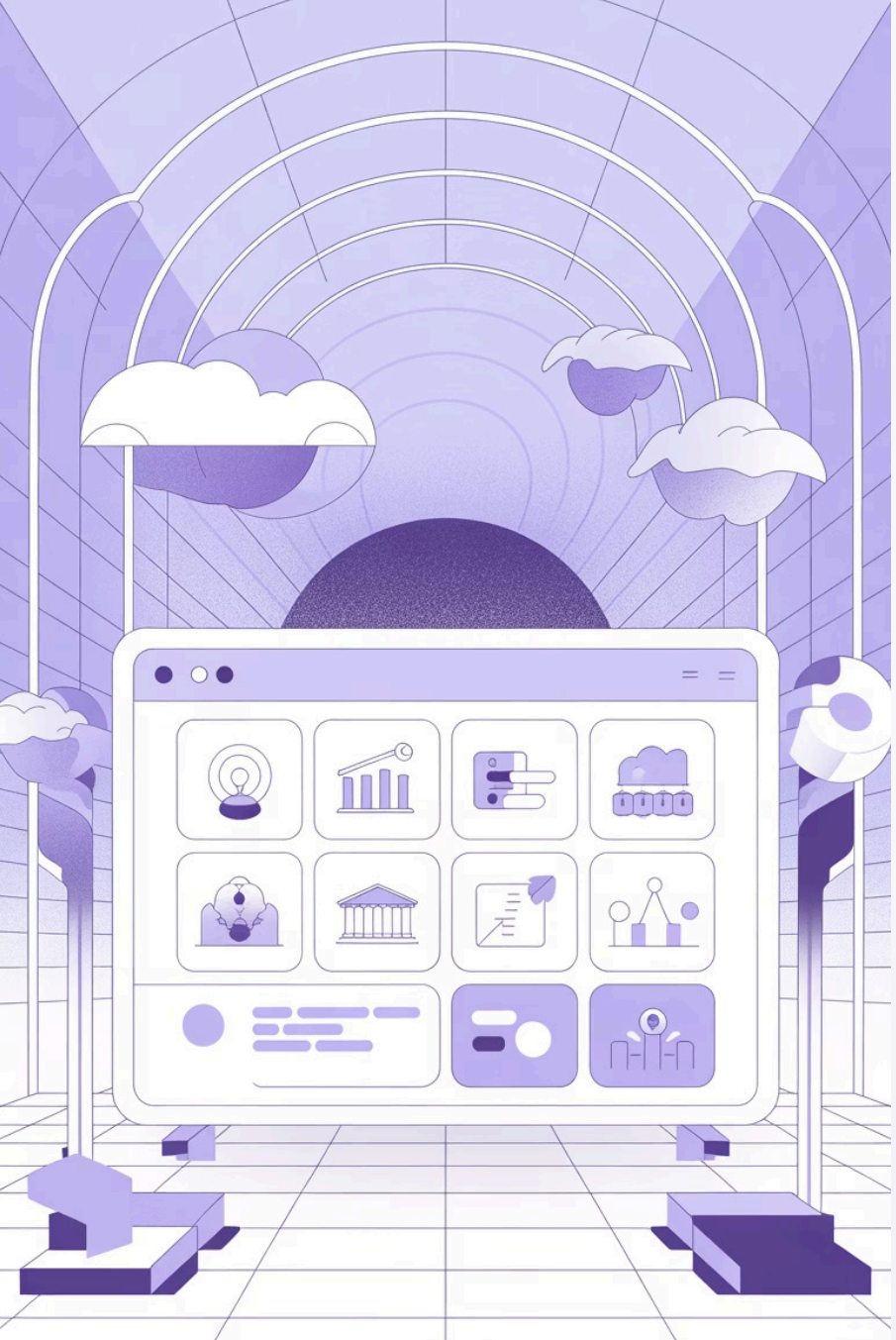
Regularly validate security controls against FedRAMP, NIST, and agency-specific requirements through automated scanning.

End-to-End Encryption

Encrypt data at rest and in transit using CSP-managed keys or bring-your-own-key (BYOK) solutions for enhanced control.

Continuous Auditing

Implement logging and monitoring with GovCloud-native tools like AWS CloudTrail, Azure Monitor, and Google Cloud Logging.



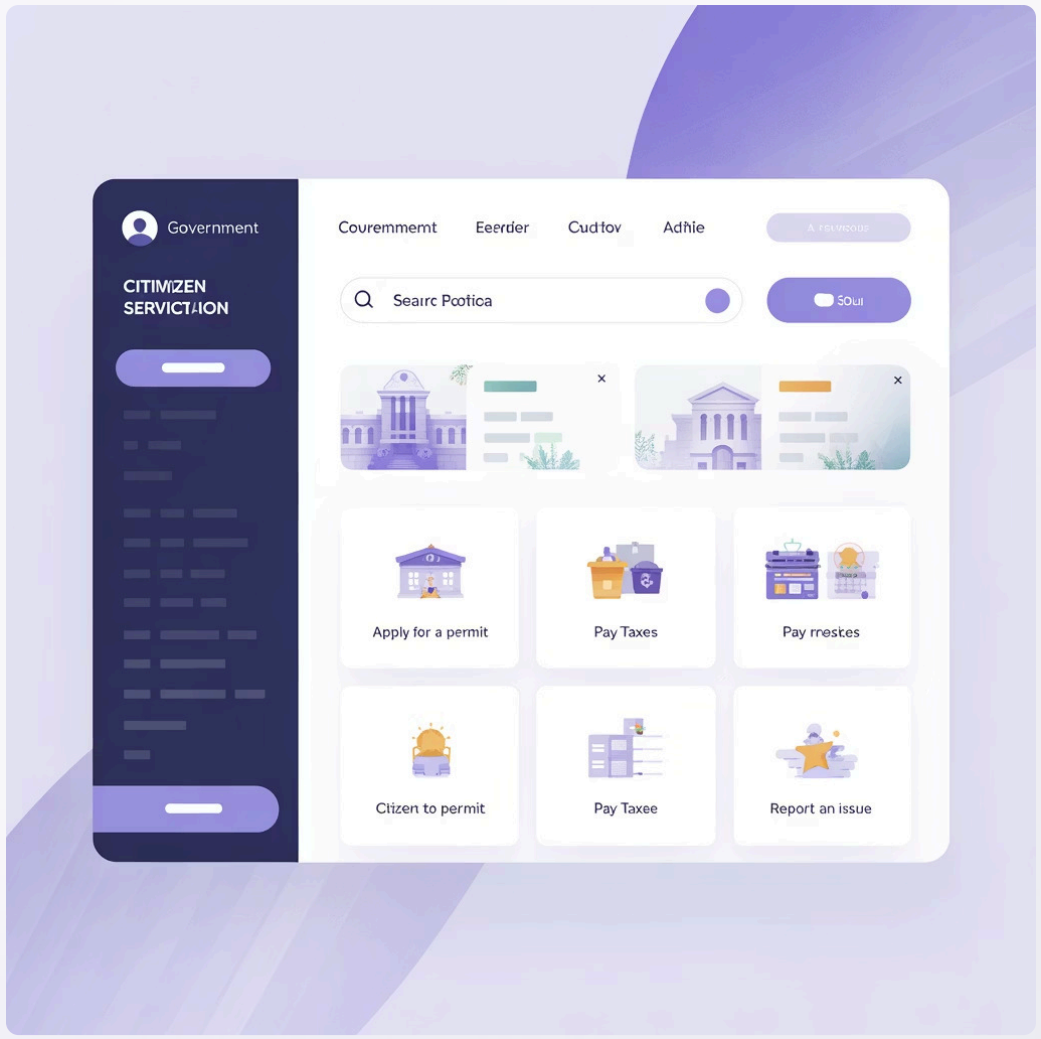
SaaS Providers Building on GovCloud

Chapter 3

SaaS Solutions for Government on GovCloud

SaaS vendors leverage GovCloud infrastructure to deliver specialised public sector applications whilst maintaining the highest security standards. These solutions address unique government needs including case management, citizen engagement, and secure document workflows.

By building atop certified GovCloud platforms, SaaS providers inherit baseline compliance whilst adding application-layer security tailored to government requirements.



Document Management

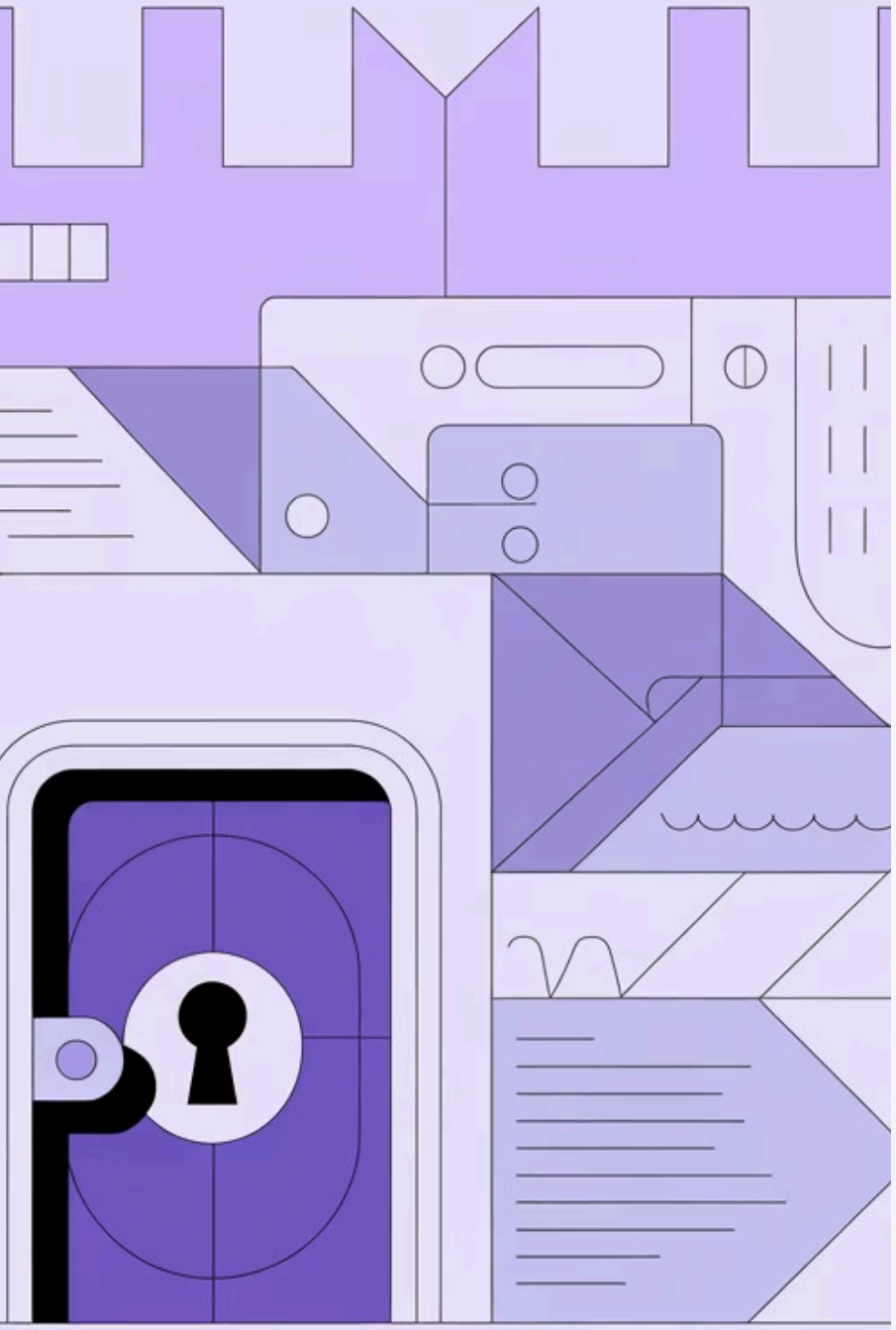
Secure storage, version control, and collaboration for sensitive government documents with full audit trails

Case Management

Streamlined workflows for agencies managing investigations, permits, benefits, and other case-based processes

Citizen Engagement

Public-facing portals enabling secure communication, service requests, and information access for constituents



Securing SaaS Applications for Government

Multi-Layered Security

Application-level encryption, secure key management, and identity federation with government Identity Providers (IdPs) ensure data protection beyond infrastructure security.

Continuous Vulnerability Management

Ongoing vulnerability scanning, penetration testing, and security assessments specifically tailored for government threat models and attack vectors.

Incident Response & Compliance

Dedicated incident response procedures and compliance reporting aligned with government audit requirements, including timely breach notifications and remediation.

256-..

Encryption Standard

Industry-leading encryption for data at rest and in transit

24/7

Security Monitoring

Round-the-clock threat detection and response

99.9%

Uptime SLA

High availability for mission-critical government services

Maximising GovCloud Benefits with Best Practices

Secure Foundation

GovCloud environments provide a compliant, secure foundation purpose-built for government workloads

Best Practices

Adopting IAM, IaC, and compliance management best practices is critical for success

SaaS Partnership

Partner with SaaS providers building on GovCloud for tailored, secure public sector solutions

---

The Future of Government Cloud

Multi-Cloud Strategies

Avoiding vendor lock-in whilst leveraging best-of-breed capabilities from multiple providers

Automation & AI

Intelligent automation driving efficiency, security, and faster service delivery

Zero Trust Evolution

Continuous verification and micro-segmentation becoming the new security standard

> The convergence of multi-cloud architecture, advanced automation, and zero-trust principles will drive the next generation of government cloud innovation and operational resilience.