AWS GovCloud and Azure Government Cloud Operations

Architecture optimization and operational maturity engagement for organizations running workloads in AWS GovCloud or Azure Government, improving cost efficiency, security posture, and operational reliability.

PRACTICE

Cloud and Edge

CLIENT PROFILE

Federal organization operating in AWS GovCloud or Azure Government needing architecture optimization, security hardening, and operational excellence in their authorized cloud environment

Challenge

- Cloud infrastructure deployed without well-architected best practices resulting in cost overruns
- Security configurations not aligned with agency security requirements and STIG baselines
- Lack of operational automation for scaling, patching, and incident response in cloud

Approach

- Conduct Well-Architected Review assessing security, reliability, performance, cost, and operational excellence
- Implement cloud security baseline with guardrails, logging, and compliance monitoring
- Optimize resource sizing, reserved capacity, and storage tiering for cost reduction
- Establish cloud operations runbooks and automation for day-2 management

Typical Outcomes

- Reduced cloud spend through right-sizing and optimization recommendations
- Hardened security posture with automated compliance monitoring
- Improved operational reliability with documented runbooks and automation

Procurement Paths

- NASA SEWP V and SEWP VI for cloud services and tooling
- GSA MAS for cloud architecture and operations services
- CIO-CS (NITAAC) for cloud management solutions

Compare vehicles and ordering steps on **How to buy**.

Partner Technology Examples

- AWS GovCloud
- Microsoft Azure Gov
- Palo Alto Networks (Prisma Cloud)
- Elastic

This is a representative use case. To request a briefing or a quote, contact Norseman Defense Technologies at 410.579.8600 or sales@norseman.com.