

G2 Ops, Inc.

AWS Marketplace

Secure Cloud Computing Architecture Engineering

ATO-Ready AWS Environment Design & Implementation

The Secure Cloud Computing Architecture (SCCA) Engineering service delivers end-to-end design and implementation of secure cloud environments in Amazon Web Services aligned to NIST 800-53, RMF, and DoD security requirements.

This offering ensures systems are architected secure-by-design and ATO-ready from inception, reducing rework, accelerating authorization timelines, and enabling mission owners to operate securely and efficiently in cloud environments.

The engagement covers architecture design, security control integration, network segmentation, identity and access management, and deployment of scalable, compliant cloud infrastructure.

Scope of Work

This engagement includes:

Cloud Architecture Strategy & Design

- Define target cloud architecture aligned to mission requirements
- Develop secure reference architecture (network, compute, storage, identity)
- Align architecture to compliance frameworks (NIST 800-53, RMF)

Secure Environment Engineering

- Design and implement Virtual Private Cloud (VPC) architecture
- Configure network segmentation, routing, and access controls
- Establish boundary protections and secure ingress/egress patterns

Identity & Access Management (IAM)

- Implement role-based access control (RBAC) and least privilege
- Configure IAM roles, policies, and federation
- Integrate with enterprise identity providers where applicable

Security Control Implementation

- Implement technical controls aligned to RMF Step 3
- Configure encryption (at rest and in transit)
- Enable logging, monitoring, and alerting capabilities

Cloud Security Tooling Integration

- Deploy and configure native AWS security services (e.g., GuardDuty, Security Hub, CloudWatch)
- Integrate vulnerability scanning and compliance tooling
- Establish centralized logging and audit capabilities

DevSecOps & Automation Enablement

- Implement Infrastructure as Code (IaC) for repeatable deployments
- Integrate security controls into CI/CD pipelines
- Establish automated compliance and monitoring workflows

ATO Alignment & RMF Integration

- Align architecture to RMF control requirements
- Support control inheritance strategies
- Prepare artifacts to support RMF documentation and ATO efforts

Out of Scope (unless otherwise agreed via Private Offer):

- Application development
- Long-term managed services or operations
- Full RMF package development (covered under RMF Acceleration offering)

Deliverables

At the conclusion of the engagement, the customer will receive:

- **Secure cloud architecture design documentation**
- **Deployed AWS environment (or validated architecture)**
- **Network architecture diagrams (VPC, segmentation, boundaries)**
- **IAM design and access control framework**
- **Security control implementation mapping (aligned to NIST 800-53)**

- **Logging, monitoring, and alerting configuration**
 - **Infrastructure as Code (IaC) templates (as applicable)**
 - **ATO readiness artifacts and architecture alignment documentation**
 - **Executive briefing and technical walkthrough**
-

Engagement Timeline

Typical duration: **6–12 weeks**

Phase 0: Preparation & Architecture Planning (Weeks 1–2)

- Requirements gathering
 - Security and compliance alignment
 - Architecture design and approval
-

Phase 1: Environment Build & Configuration (Weeks 3–8)

- Cloud environment deployment
 - Network and IAM configuration
 - Security control implementation
-

Phase 2: Validation & Optimization (Weeks 9–10)

- Security validation and testing
 - Logging and monitoring verification
 - Architecture tuning and optimization
-

Phase 3: ATO Alignment & Transition (Weeks 11–12)

- Control mapping and documentation support
- ATO readiness validation
- Knowledge transfer and handoff

Customer Responsibilities

To ensure successful delivery, the customer will:

- Provide AWS account access and required permissions
 - Assign a cloud and security point of contact
 - Participate in architecture reviews and approvals
 - Provide compliance requirements and constraints
 - Support integration with existing enterprise systems
-

Pricing

Final pricing may vary based on:

- Environment complexity and scale
- Number of accounts / regions
- Security and compliance requirements
- Integration with existing systems
- Timeline urgency

Custom pricing available via Private Offer.

Delivery Method

- Remote (default)
 - Hybrid or onsite delivery available upon request
-

Geographic Availability

- United States (including federal and regulated environments)
-

Service Categories

- Security & Compliance
- Migration & Modernization
- DevSecOps

Support & Follow-On Services (Optional)

Available via Private Offer:

- Ongoing cloud security engineering and optimization
- RMF integration and ATO support (paired with RMF Acceleration Package)
- Continuous monitoring and compliance automation
- Cost optimization and performance tuning
- Multi-account and enterprise-scale architecture expansion