

**Methodology · No cost**

Free AWS Cloud Security Posture Assessment

A two-hour, read-only review of your AWS environment, delivered by a CISSP, producing prioritized findings mapped to the AWS Well-Architected Framework security pillar.

DURATION
2-hour session**DELIVERABLE**
10 business days**ACCESS**
Read-only IAM role**PRICE**
No cost

Engagement phases

PHASE	TIMING	WHAT HAPPENS
Request and scope	1 day	Confirm accounts, Regions, and workloads in scope. Identify compliance drivers and any areas of particular concern.
Access provisioning	1–2 days	You create a scoped IAM role granting read-only permissions (SecurityAudit and ViewOnlyAccess equivalents). No agents are deployed and no write permissions are requested.
Automated collection	1 day	Configuration and posture data pulled from AWS Config, Security Hub, IAM, CloudTrail, GuardDuty, KMS, and Macie, then normalized for review.
Working session	2 hours	Findings reviewed live with your team so context, compensating controls, and planned work are captured before conclusions are drawn.
Reporting	Within 10 business days	Prioritized findings summary, Well-Architected mapping, and remediation roadmap delivered as a written package.

Scope of review

AWS SERVICE OR AREA	WHAT IS EXAMINED
Identity and access	AWS IAM, IAM Identity Center: role policies, permission boundaries, federation, root account posture, MFA coverage, access key age
Logging and monitoring	AWS CloudTrail, Amazon CloudWatch, Amazon GuardDuty: trail coverage, log retention, detector status, alert routing
Configuration and compliance	AWS Config, AWS Security Hub: recorder coverage, enabled standards, control pass rates, drift
Data protection	AWS KMS, Amazon Macie, Amazon S3: encryption defaults, key rotation, public access blocks, sensitive data discovery
Multi-account guardrails	AWS Organizations, AWS Control Tower: SCP coverage, account baselines, guardrail drift

What we need from you

- A scoped read-only IAM role ARN and the external ID for assumption
- A list of AWS account IDs and Regions in scope
- Names of compliance frameworks you report against, if any
- One hour of availability from someone who knows the environment, plus two hours for the working session

Deliverables

- Prioritized findings summary, each finding rated by risk severity
- Mapping to the AWS Well-Architected Framework security pillar
- Remediation roadmap grouped into immediate, 30-day, and 90-day actions

Assumptions and exclusions

- No changes are made to your environment; this is a read-only assessment
- No penetration testing, exploitation, or social engineering is performed
- Application-layer code review is out of scope
- This assessment is not a certification or an audit opinion

Support and service levels

Pre-purchase. Scoping conversations, AWS prerequisite confirmation, and a written statement of work before any private offer is issued. Inquiries answered within two business days.

During the engagement. A named engagement lead, Brian Govanlu, CISSP, as single point of contact. Support Monday to Friday, 9:00 AM to 6:00 PM US Eastern, by email and phone, with a response within one business day. Kickoff within five business days of offer acceptance, weekly written status updates, and a walkthrough of every deliverable.

After delivery. Thirty days of email support for questions about findings and recommendations. Refunds and disputes are handled directly with the engagement lead in accordance with the accepted private offer.

Available directly or through AWS Marketplace as a private offer. If you hold committed AWS spend, the engagement draws down against it and appears on your existing AWS bill. Any AWS infrastructure costs you incur remain your responsibility and are separate from the AWS Marketplace transaction.