Vantalect

AWS SECURITY, COMPLIANCE & GOVERNANCE · FIXED PRICE

AWS Security, Compliance & Governance Audit

Your AWS organization, audited from the inside. Hardened in six weeks.

Prepared by Charles Sieg · charles.sieg@vantalect.com · vantalect.com

October 13, 2026

The problem

An audit is coming, a customer sent a security questionnaire, or nobody can say for certain who can reach production. Most AWS organizations got here by growing faster than their guardrails.

This engagement reads your organization from the inside (identity, network exposure, data protection, logging, detection, and governance, across every account and region) and maps what it finds to the framework your auditors use. We find it in two weeks. We close it in six.

The Audit

Two weeks

$25,000

Up to 40 consultant hours

One AWS organization, read from the inside. We scan every account and every enabled region, verify every finding by hand, trace who can reach what, and map it all to the framework your auditors use.

GUARANTEED

The Hardening

Six weeks

$35,000

Up to 110 consultant hours

The Audit in the first two weeks. Then weeks three through five close the findings as code in your repositories, with the engineers who own each account. Week six runs the same scan again and hands it over.

The second half of the fee is invoiced only when every critical finding in the audit is closed, verified by the week-six re-scan.

Who it is for

- A CTO, CISO, VP of Engineering, or head of platform whose production runs on AWS
- A SOC 2, HIPAA, PCI DSS, or ISO 27001 audit coming, a customer questionnaire to answer, or a board asking how exposed you are
- Budget authority for a fixed-price engagement without a procurement cycle

It is not the right engagement if you need a penetration test of your application, an attestation or certificate (we prepare you for your auditor; we are not the auditor), or if you cannot grant a read-only role in your own accounts. It covers AWS only, not Azure or Google Cloud. To review one production workload across all six pillars instead, see the AWS Well-Architected Framework Review at vantalect.com/well-architected.

Week by week

The same weeks, every time, which is why the price is fixed.

The Audit, two weeks.

Week	What happens
1. Access and scan	The read-only role goes into every account on day one. Every account and enabled region is scanned against the CIS and AWS benchmarks, the organization's structure and policies are mapped, and walkthroughs happen with your platform and identity leads.
2. Verify and plan	Every critical and high finding is verified by hand, false positives are removed, and each real finding's blast radius is traced. Then the compliance map, the roadmap, and a sponsor readout.

The Hardening, six weeks.

Week	What happens
1 and 2. Access, scan, verify, plan	The Audit's two weeks, with no changes yet. The week-one scan is the baseline, and the verified findings register is agreed with your sponsor.
3. Criticals and guardrails	Every critical finding fixed as code, highest risk first, proven in non-production before production. Service control policies and account defaults go in at the top of the organization, so what closed stays closed.
4. Identity	People move to single sign-on, long-lived access keys are retired, over-broad roles are cut to what each workload uses, and the root and break-glass accounts are locked down and alarmed.
5. Detection and response	GuardDuty, Security Hub, IAM Access Analyzer, and AWS Config on in every account and region, routed to your on-call. One organization trail into a log archive no application account can alter, and runbooks for what will page you.
6. Re-scan and hand over	The same scan as week one, run the same way. You get the before and after, the runbooks, and a team that knows how to keep the score where it is.

The meetings, and the hours behind them

Every session is held on Zoom and scheduled before week one: a kickoff, an architecture walkthrough, an identity interview, office hours twice a week, a findings review, and a sponsor readout. The Hardening adds a weekly sponsor check-in, a twice-weekly change review in weeks three through five where every fix is read as code before it merges, and a 2-hour handover workshop in week six.

In the Audit, about 8 of the 40 hours are live with your team; in the Hardening, about 38 of the 110. The rest is verification, reviews, and agents doing the scanning under Charles's supervision.

What you receive

The Audit

1. **The scan.** Every account and enabled region scored against the CIS AWS Foundations Benchmark and AWS Foundational Security Best Practices.
2. **The findings register.** Every finding verified by hand and ranked by exploitability and blast radius, with its evidence, resources, and fix.
3. **The identity and access review.** Who and what can reach production: human access, workload roles, cross-account trust, long-lived keys, privilege-escalation paths, and the root and break-glass accounts.
4. **The compliance map.** The findings mapped to the controls of one framework (SOC 2, HIPAA, PCI DSS, NIST 800–53, ISO 27001, or GxP), with the AWS-side evidence each control will be asked for.
5. **The governance review.** Account structure, service control policies, Control Tower, account provisioning, tagging, and logging and detection coverage.
6. **The remediation roadmap.** Every fix sequenced by risk and effort, each with an owner and an estimate.
7. **The sponsor readout.** A short written document, presented in the closing meeting.

The Hardening

Everything in the Audit, then eight more:

8. **Every critical finding closed** as code in your repositories, each through a pull request reviewed by the engineer who owns the account.
9. **Guardrails at the top** of the organization: policies and account defaults for public access and encryption, inherited by every new account.
10. **Identity rebuilt** on single sign-on for people and least-privilege roles for workloads, with long-lived keys retired.
11. **Detection everywhere,** in every account and region, routed to your on-call.
12. **An organization trail** into a log archive that no application account can alter or delete.
13. **Incident runbooks** for the findings most likely to page you.
14. **The week-six re-scan** against week one: same method, same scope. It decides the second invoice.
15. **The handover workshop,** and its recording.

How the result is measured

Each finding is rated by how exploitable it is and how far the damage would reach, starting from the benchmark's own severity. That register is agreed with your sponsor at the week-two readout, and its critical findings are the ones the guarantee is measured on. In week six the same scan is run the same way and compared with week one.

The guarantee

The second half of the Hardening fee is invoiced only when every critical finding in the audit is closed, verified by the week-six re-scan. If the gate is not met, the second invoice is not issued and you keep everything delivered.

A critical finding you accept in writing as a risk counts as closed, as does a fix you approved and then chose not to apply.

Beyond that gate, no particular result is guaranteed: a security engagement reduces risk but cannot promise an environment will never be breached. It is not an audit opinion, an attestation, a certification of compliance, or a penetration test.

Terms at a glance

Fees, hours, and scope. Invoices are due within fifteen days.

Term	The Audit	The Hardening
Fee	$25,000, fixed	$35,000, fixed
Length	Two weeks	Six weeks
Consultant hours included	Up to 40	Up to 110
Time live with your team (estimate)	About 8 hours	About 38 hours
Invoicing	As the statement of work sets out	Half at signature, half only if the guarantee is met
Beyond the cap	$450 per hour, by written change order agreed before the hour is spent, invoiced monthly	Same
Scope	One AWS organization of up to 50 accounts, every enabled region; one compliance framework mapped	Same, plus fixes in up to four infrastructure-as-code repositories (Terraform, CloudFormation, or CDK)

Additional accounts, organizations, or frameworks, an on-site day, infrastructure migration, and support after the closing readout are outside scope, available only by written change order. Either party may end an engagement with five business days' written notice; you then pay for hours spent to date at $450 per hour, capped at the fee, and keep everything delivered.

> **Your data and your ownership**
>
> The audit role reads how your accounts are configured, not what they store. Scan results are kept in your engagement's Pavilion workspace, exported to you at the close, and deleted from Vantalect's systems within thirty days after it. Security findings are never cited, with or without your name. You own outright what is delivered: infrastructure code, policies, runbooks, plans, recordings, and reports.

What we need from you

The read-only audit role, from a CloudFormation StackSet we hand you, carries AWS's SecurityAudit and ViewOnlyAccess policies and nothing else. In the Hardening, every fix lands in your repositories and is applied by your pipeline. Sessions run on Zoom, the record lives in Pavilion, and scheduling, approvals, and invoices go by email.

- The audit role deployed in every in-scope account within three business days of signature. The schedule starts when it exists, and slides by the same number of business days if an obligation is not met.
- A platform or security lead available at least four hours a week.
- Your sponsor available for thirty minutes a week and for the readouts.
- In the Hardening, approval or decline of each change within two business days through your normal change process.
- Your permission to record the sessions.

What comes with every engagement

- **Charles, personally.** Charles Sieg delivers every engagement inside your accounts, with your engineers and no hand-off to a junior team. He holds AWS Certified Solutions Architect and DevOps Engineer at the professional level and Security at the specialty level.
- **Pavilion, your private workspace.** Set up in week one: the calendar, every recording with its transcript and summary, the findings register, the decisions, and the action items, in one place you keep afterward.
- **Every session recorded,** with your permission, with transcripts and recaps.

- **A start within two weeks** of signature, once the access it needs exists.

Questions clients ask

Will this make us SOC 2 compliant?

Nothing makes you compliant by itself, and we are not your auditor: SOC 2 reports are issued by licensed CPA firms. What you get is the AWS side of the evidence, mapped to the controls your auditor will test, and in the Hardening, the gaps closed before they look.

What access do you need?

A read-only role in each account: AWS's SecurityAudit and ViewOnlyAccess policies, nothing else. It cannot open an object in a bucket, query a database, or read a secret's value. You can read every line before you deploy it, and delete it the day we finish.

Do you ever change production?

Not directly. In the Hardening, every fix is written as code and goes through your pull requests and your pipeline, reviewed by the engineer who owns the account.

What if we decide not to fix something?

Then it is your call, recorded in writing as an accepted risk, and it counts as closed for the guarantee.

Start with an email

Write to **charles.sieg@vantalect.com** and tell us how many accounts you have, which framework your auditors use, and what prompted the question. Charles replies within one business day, and the first call is thirty minutes.

The full description is at **vantalect.com/security-audit**, and the standard terms are at **vantalect.com/terms**.

© 2026 Vantalect, LLC. Prices and terms as of October 13, 2026; the terms at vantalect.com/terms govern.

AWS, Amazon Web Services, and the AWS service names are trademarks of Amazon.com, Inc. or its affiliates. SOC 2 is a registered trademark of the American Institute of Certified Public Accountants. PCI DSS is a trademark of the PCI Security Standards Council, LLC. ISO is a registered trademark of the International Organization for Standardization. CIS Benchmarks is a trademark of the Center for Internet Security, Inc. Zoom is a trademark of Zoom Video Communications, Inc. Vantalect is not affiliated with or endorsed by any of them.