



AWS SECURITY, COMPLIANCE & GOVERNANCE · SAMPLE DELIVERABLE

Audit Sponsor Readout

Week 2 of 6: Sponsor readout · prepared for Tidepost, Inc.

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

January 16, 2026 · AWS Security, Compliance & Governance Audit: The Hardening (six weeks)

SAMPLE DELIVERABLE

This is a sample deliverable. Tidepost, Inc. is a fictional company: its people, products, users, accounts, investors, and figures are invented for this sample, and any resemblance to a real company, person, product, or publication is coincidental. AWS prices are list prices from the AWS Price List API retrieved on October 13, 2026, and from the public AWS Price List bulk API on October 18, 2026.

Contents

- The score 2
- What an attacker could reach 3
 - Three paths, in plain terms 5
- Decisions we need from you 6
- The Foundation plan, in brief 7
- The cost of detection 8
- The next four weeks 8
- The gate 10

The score

Tidepost’s AWS account passes 12 of the 50 checks in the scan (24.0%), and the Audit verified 47 findings, 10 of them Critical. By today, 5 of the 10 Critical findings are closed, and the rest have dates. Dev Raman: this is the two-week Audit in one document, for you and for Kofi Brandvold and Sasha Ilyin. The week-one scan and the audit report have the detail; this document has the decisions.

The score is the least interesting number here. It says most of the AWS controls the SOC 2 auditor tests are not yet in place. The findings say why, and the next section says what an attacker could have done with them.

The Audit in nine numbers.

Measure	Value
Checks passing in the week—one scan, January 5	12 of 50 (24.0%)
Resources failing those checks	207
Verified findings	47
Critical findings	10
Critical findings that needed no credential	4
Critical findings closed today	5 of 10
All findings closed today	13 of 47
Findings to accept or defer in writing	5
SOC 2 technical map: controls operating today	4 of 35

For the SOC 2 examination: the technical map lists 35 AWS controls, 4 of them operating today and 31 planned. 33 are planned to operate before the observation window opens on April 1, 2026, and 2 after it (the C1.2 disposal controls, which wait on counsel and the app team). Tidepost’s CPA firm runs its own readiness assessment from February 17, 2026 to March 6, 2026. Vantalect is not the auditor and does not issue, predict, or influence a SOC 2 report: the map is evidence for the auditor, who tests it.

What an attacker could reach

Anyone on the internet, with no credentials, could do 4 of the 10 things below, and 3 of those are already closed. C-5 is still open today, planned to close on January 21, 2026. Another 4 need one stolen credential or one application bug, one needs a foothold inside, and one is not a way in at all: it is the missing record.

The 10 Critical findings, with what it takes to use each, what it reaches, and where it stands.

ID	What is wrong	What an attacker does, as found	What they reach	Status on January 16
C-1	Root user with two active access keys and no MFA	Uses either root access key, from the GitHub Actions secret or the deploy script on a laptop	Everything in the account, with no policy able to limit it, including billing and closing the account	Open; next step January 29
C-2	tp-media-originals public-read, and location metadata on 61% of images	Lists and downloads originals from the public bucket with no credentials	Every original upload, and on 61% of images the GPS coordinates of where the contributor stood (9.8 million originals)	Closed January 14
C-3	tp-exports public with listing on: 104,318 user records	Lists the bucket with no credentials and downloads the export	The 104,318 user records in the marketing export	Closed January 6
C-4	RDS PostgreSQL publicly accessible from 0.0.0.0/0	Connects to the database listener from anywhere and tries the password, which C-8 had left in the repository	The production database: every user, post, and moderation record	Accepted in writing today, to March 22
C-5	OpenSearch domain with a public endpoint and an open access policy	Sends requests to the open search endpoint; the access policy allows every action to every caller	Read, change, or delete of every search index	Open; planned January 21
C-6	Link-preview SSRF reaches IMDSv1 and an instance role with AdministratorAccess	Gives the link-preview service a URL that reaches the instance metadata service and takes the role's temporary credentials	Administrator access to the whole account, with the keys of an instance role	Closed January 8
C-7	Seven IAM users with administrator access and long-lived keys, two of them departed	Uses a long-lived administrator key, including the keys of the two people who had left	Administrator access, and the keys never expire	Open; next step January 26

ID	What is wrong	What an attacker does, as found	What they reach	Status on January 16
C-8	Database password and a third-party API key in the repository and in launch template user data	Reads the repository or a launch template's user data, as any engineer or contractor with access can	The production database password and a third-party API key	Closed January 9
C-9	No CloudTrail trail	Nothing: it is the missing record	A compromise through any other finding would leave no trail past the 90 days of management events AWS keeps	Open; next step January 28
C-10	A forgotten g5.12xlarge with SSH open and a Jupyter server without a token	Runs code on a GPU server through the Jupyter server, which asks for no token, with SSH also open	Four GPUs to mine on, and whatever the instance's role and network can reach	Closed January 6

Three paths, in plain terms

Through the public data. Two buckets were open to the internet, and so was the search endpoint. C-3 listed the exports bucket and held 104,318 user records; C-2 exposed every original upload, and on 61% of images the coordinates of where the contributor stood. Tidepost closed the first on January 6, 2026, within the hour, and the second by January 14, 2026, after an S3 Batch Operations job removed the location data from 9,800,000 originals. C-5, the open search domain, is the one of the three still open.

Through the application. The link-preview service fetches any URL a user gives it, follows redirects, and runs on an instance whose role is AdministratorAccess (C-6). Pointing it at the instance metadata service takes the role's temporary credentials, and with them the whole account. The database is reachable from anywhere (C-4) and its password was in the repository (C-8). Both are now closed or restricted: C-6 and C-8 are closed, and C-4 is restricted to one vendor's four address ranges, which is the acceptance you decide below.

Through keys. The root user had two access keys and no MFA (C-1), and 7 IAM users have administrator access with keys that never expire (C-7). Two of those people have left the company. Tidepost deleted both root keys, registered two hardware keys on the root user, and deleted the departed users on January 6, 2026; the 5 current administrators move to IAM Identity Center once the organization exists.

What we have not looked for

This is a configuration review. We did not look for evidence that any of these was used, and there is little to find: the account has no trail past the 90 days AWS keeps of management events, no flow logs, and no access logs on the exports bucket. Whether anyone read the exports file or used the GPU server cannot be established, and counsel has been told. Whether to notify anyone is Tidepost's decision, and Vantalect records only that counsel was told.

Decisions we need from you

Eight decisions come out of the Audit. All but decision 7 are today's; decision 7 is signed by January 21, 2026.

The decisions, in the order we would take them.

No. Decision	Who decides, and when
1 Agree the register , and agree that its 10 Critical findings (C-1 to C-10) are the ones the gate is measured on	Dev Raman, at this readout
2 Sign the written acceptance of C-4 , the public database. PubliclyAccessible stays true until the new encrypted private instance replaces this one at the March 22, 2026 cutover; until then the security group admits only the BI vendor's four published ranges and TLS is required. It meets the gate as accepted in writing, stays on the register and on the SOC 2 map as open, and ends when the Well-Architected Review performs the cutover	Dev Raman, at this readout
3 Defer H-1 in writing , unencrypted RDS storage, to the same cutover. The database cannot be encrypted in place. The EBS half proceeds: default encryption on in week 3 and the last unencrypted volumes replaced by February 10	Dev Raman, at this readout
4 Defer H-12 in writing to May 20, 2026 : removed posts' media is not deleted, and the app team cannot ship the deletion pipeline before the retention schedule exists, which waits on counsel	Sasha Ilyin, at this readout
5 Take the greenfield path for the organization : a new management account, with the founders' account joining it as the production member. No workload moves, and no commitment or credit is lost, because there are none	Dev Raman, at this readout

No. Decision	Who decides, and when
6 Approve the first change window in writing: W1, landing zone, on January 21, 2026	Dev Raman and Kofi Brandvold, at this readout
7 Accept M-7 and L-4 in writing: access logging stays off on the media buckets, because object-level data events cover the two buckets that hold user data, and three bucket names stay as they are. Both are reviewed on June 30, 2026	Sasha Ilyin, by January 21, 2026
8 Decline Amazon Macie across the media buckets: nearly all of the media is public news by design, and the two buckets that hold user data are small	Sasha Ilyin, at this readout

One more is already made: Sasha Ilyin declined a history rewrite of the repository that held the C-8 secrets on January 9, 2026, because both secrets were rotated, so the exposed values no longer work; rewriting history would break every clone and open pull request for no added protection. Two of the eight deserve a sentence. **Decision 2 is the one that makes the gate real.** An acceptance meets the gate only if it has a named signer, a reason, and a closing date, and this one has all three; if the cutover slips, the acceptance does not extend itself, and the gate does not pass on it. **Decision 5 sets the order of everything after it.** The guardrails, the organization trail, and the delegated detection all belong to an organization, and building them in the single account first would mean building them twice.

The Foundation plan, in brief

The Foundation add-on is the Build's weeks three to six: January 20 to February 13, 2026. The Foundation plan readout carries the full plan, and the Audit's governance review is its discovery. This is the part you decide today.

- **The path.** Greenfield, not retrofit. No organization existed: the founders' account was its own payer, so there was nothing to retrofit. The account that would have been the payer runs production, and the management account holds no workloads.
- **The accounts.** 9 accounts in 9 organizational units. tp-management exists already; Kofi Brandvold created it on January 12, 2026.
- **The windows.** Six change windows, each approved in writing two business days ahead:

The six change windows.

Window	Date	What happens
W1	January 21, 2026	Landing zone
W2	January 23, 2026	IAM Identity Center and the identity provider
W3	January 28, 2026	The join and enrollment
W4	February 3, 2026	Policies to Sandbox and NonProd
W5	February 5, 2026	Policies to Prod, and the vended account
W6	February 10, 2026	Backup and tag policies; the backup account

- **The checks.** 12 Foundation checks are in scope, and the add-on passes when every one passes at its end, with a waiver in writing counting as passed.
- **The risks.** 10 risks are sized and owned. The one sized high is FR-8, the blast radius of a wrong policy in a single production account, which is why every policy runs in Policy Staging first.
- **The price.** The add-on is its own statement of work: \$25,000, half at signature and \$12,500 on its gate, February 13, 2026.

The cost of detection

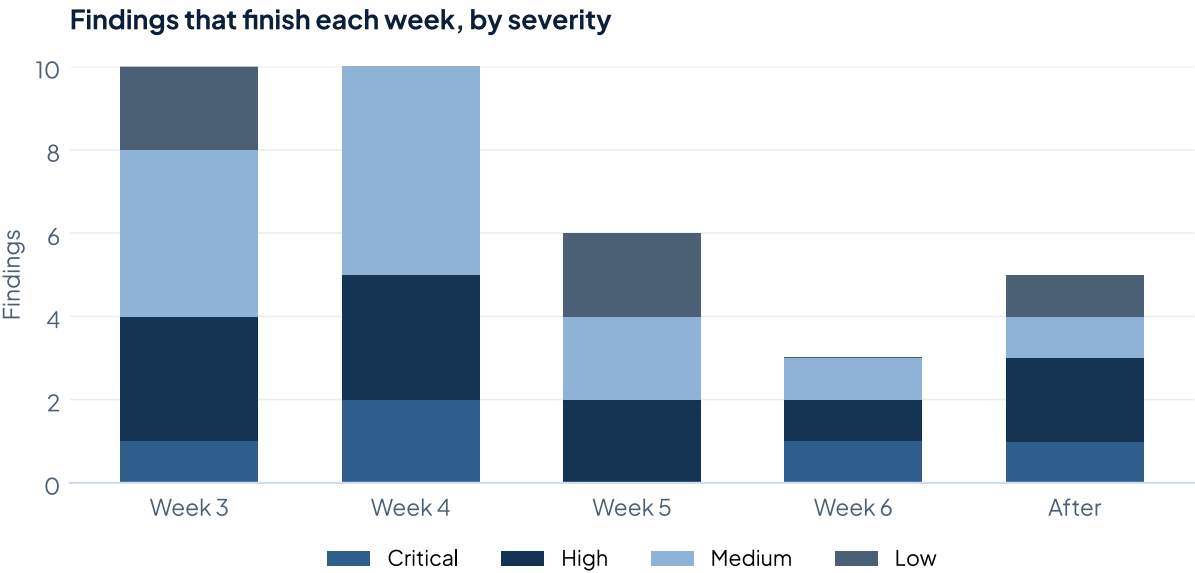
Turning detection on adds roughly **\$2,584 a month at list prices, about 1.6% of the \$157,565 monthly run rate on January 5, 2026.** That is GuardDuty and its protection plans, Security Hub CSPM, AWS Config, and Amazon Inspector, in the accounts and Regions that need them. It is an estimate at list prices, not a measurement; the cost engagement later reports what the bill carries. The cost of not having it is the missing record under C-9.

The next four weeks

If you agree the register, the Hardening carries out the plan through Tidepost's own change process, with the engineers who own each item. Every change is a pull request and a change review before it merges, and nothing is applied without its owner's yes.

The Hardening, week by week, from the dates in the register.

Week	Starts	What goes in	Findings that finish
3	Jan 19	Every remaining Critical in the account closed or scheduled, and the workload guardrails that keep them closed	10C-5
4	Jan 26	Identity: people on IAM Identity Center, CI on OIDC federation, workloads on roles	10C-1, C-9
5	Feb 2	Detection and response from the audit account, and the first runbooks	6None
6	Feb 9	The same scan as week one, run the same way, the evidence index, and the handover	3C-7
After	Feb 13	Findings that wait on a date outside the engagement, or on a review: C-4, H-1, H-12, M-7, L-4	5C-4



The findings that finish each week, by severity. The Critical findings that finish are in the table above.

You will see Kofi Brandvold and us in a weekly 30-minute sponsor check-in and in the change reviews. 5 findings finish or are reviewed after week 6, on March 22, 2026, May 20, 2026, and June 30, 2026; the audit report gives each an owner and a date.

The gate

The gate

The second half of the Hardening's \$29,750 fee, \$14,875, is invoiced only when this holds: Every critical finding agreed at the January 16 readout is closed, verified by the week-six re-scan, or accepted in writing by a named Tidepost signer with a closing date. If the gate is not met, the second invoice is not issued and you keep everything delivered.

The gate is measured on the 10 Critical findings in this register, C-1 to C-10, as agreed with Dev Raman today, and decided by the re-scan on February 12, 2026. New findings the re-scan turns up are reported with a proposed fix and are not part of the gate. Beyond the gate, we cannot promise that an environment will not be breached: the Hardening reduces risk. It is not a SOC 2 report, a certification, or a penetration test.

What we ask of you at this readout: agree the register, sign the three acceptances and deferrals in decisions 2 to 4, and take the greenfield path. Everything else is already in motion, and the first change review is the week of January 19, 2026.

© 2026 Vantalect, LLC. Sample deliverable; Tidepost, Inc. is fictional.

AWS, Amazon Web Services, AWS Graviton, AWS Inferentia, and the AWS service names are trademarks of Amazon.com, Inc. or its affiliates. PostgreSQL is a registered trademark of the PostgreSQL Community Association of Canada. Kubernetes is a registered trademark of The Linux Foundation. Redis is a registered trademark of Redis Ltd. Valkey is a trademark of the Linux Foundation. OpenSearch is a registered trademark of Amazon.com, Inc. SOC 2 is a registered trademark of the American Institute of Certified Public Accountants. CIS Benchmarks is a trademark of the Center for Internet Security, Inc. GitHub is a trademark of GitHub, Inc. Jupyter is a trademark of LF Charities. Vantalect is not affiliated with or endorsed by any of them. Tidepost, Inc. is fictional.