

AWS SECURITY, COMPLIANCE & GOVERNANCE · SAMPLE DELIVERABLE

Findings Register, Governance Review, Target Organization, and the SOC 2 Technical Map

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

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

January 15, 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

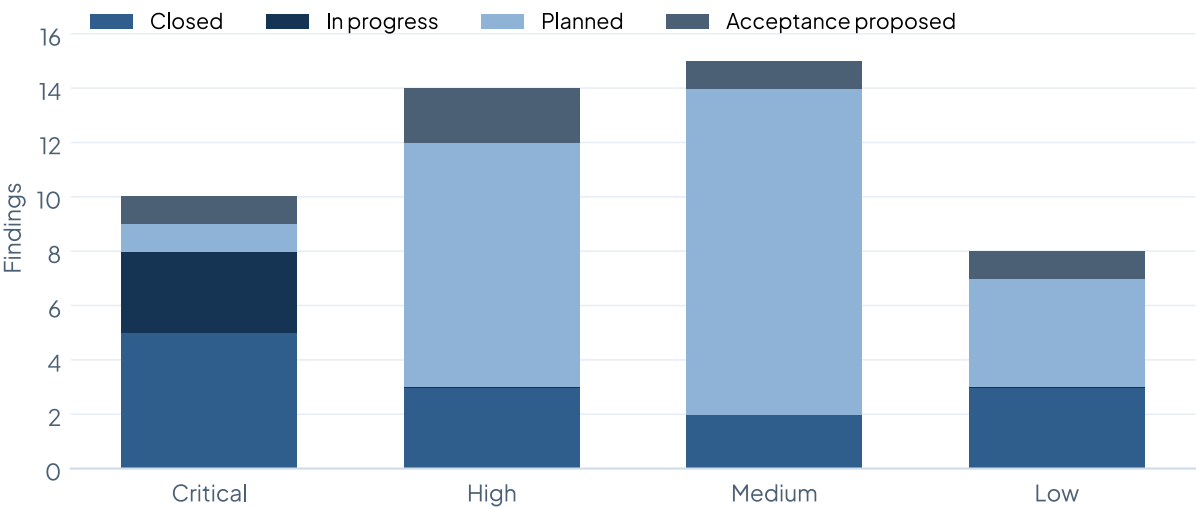
Executive summary	2
Method	5
Deliverable 1: the findings register	6
Critical findings	10
High findings	14
Medium and Low findings	18
Deliverable 2: the governance review	20
Deliverable 3: the target organization	24
Deliverable 4: the SOC 2 technical map	28
What happens next	34

Executive summary

The Audit verified 47 findings in Tidepost’s AWS account: 10 Critical, 14 High, 15 Medium, and 8 Low. Each was read by hand from the account’s own configuration on or after January 5, 2026. On January 15, 2026, 13 are closed, 3 have a first step done, 26 are planned, and 5 are proposed for a written acceptance or a dated deferral that the readout decides on January 16, 2026.

This report holds four deliverables: the findings register, the governance review (which is also the Foundation add-on’s discovery), the target organization, and the first SOC 2 technical map. The Foundation’s separate inventory and design are chapters here and in the week-one scan.

Where each finding stood on January 15



Where each finding stood on January 15, 2026, by severity.

The Critical findings at a glance

The 10 Critical findings. The readout asks the sponsor to agree these as the set the gate is measured on.

ID	What is wrong	Who can reach it	Status on January 15
C-1	Root user with two active access keys and no MFA	One stolen credential or one application bug	In progress; next January 29
C-2	tp-media-originals public-read, and location metadata on 61% of images	Anyone on the internet	Closed January 14
C-3	tp-exports public with listing on: 104,318 user records	Anyone on the internet	Closed January 6
C-4	RDS PostgreSQL publicly accessible from 0.0.0.0/0	One stolen credential or one application bug	Acceptance proposed, to March 22
C-5	OpenSearch domain with a public endpoint and an open access policy	Anyone on the internet	Planned January 21
C-6	Link-preview SSRF reaches IMDSv1 and an instance role with AdministratorAccess	One stolen credential or one application bug	Closed January 8
C-7	Seven IAM users with administrator access and long-lived keys, two of them departed	One stolen credential or one application bug	In progress; next January 26
C-8	Database password and a third-party API key in the repository and in launch template user data	A foothold inside the account	Closed January 9
C-9	No CloudTrail trail	Not an entry point: it removes the evidence	In progress; next January 28
C-10	A forgotten g5.12xlarge with SSH open and a Jupyter server without a token	Anyone on the internet	Closed January 6

What an attacker could reach

4 of the 10 Critical findings need no credential at all. They are C-2, C-3, C-5, C-10: public buckets, an open search endpoint, and a GPU server with a notebook that runs code for anyone. Another 4 need one stolen credential or one application bug (C-1, C-4, C-6, C-7), and they reach the most: C-6 turns a link-preview request into administrator access to the whole account, and C-4 is a database anyone can connect to, whose password C-8 left in the repository. 1 needs a foothold (C-8), and 1 (C-9) is not a way in at all: the account keeps no trail, so a compromise through any of the others would leave no record past the 90 days AWS keeps.

Two of the exposures cannot be undone by closing them. With no access logs on the exports bucket (C-3) and no flow logs or trail around the GPU server (C-10), we cannot say whether anyone used what was open. Counsel has been told. Whether to notify anyone is Tidepost's decision, and Vantalect records only that counsel was told.

What we recommend, in order

1. **Close what needs no design first, and most of it is done.** 13 findings are closed and 3 more have a first step done, because Tidepost's engineers acted on the January 6 call (see the week-one scan).
2. **Agree the 10 Critical findings at the readout** as the set the gate is measured on, and sign the 5 acceptances and deferrals below or decide against them.
3. **Take the greenfield path for the organization:** a new management account, with the founders' account joining it as the production member, so no workload moves ([The path: a new organization, with the founders' account joining it](#)).
4. **Put the guardrails in once, in the organization.** Building them in the single account first would mean building them twice.
5. **Turn detection on from the audit account,** so the trail, Config, GuardDuty, Security Hub CSPM, and Inspector are in place before the SOC 2 observation window opens on April 1, 2026.

Method

Where a severity starts

A finding that a benchmark control covers starts at that control's own severity. A finding no control covers, such as the link-preview request path or secrets in a repository, starts where we would rate the same weakness if a control did cover it. The 50 checks of the two standards cover 28 of the 47 findings; the rest were found by reading configuration and code.

How it is adjusted

We raise a finding when it is reachable by more people than the benchmark assumes, or reaches more than the check names. We lower one when something else already limits it. The ten Critical findings below show it: the benchmark rates some of them lower than we do.

The benchmark's highest rating among a finding's failing checks, against ours.

Finding	Highest benchmark check	Our rating	Why
C-1	Critical	Critical	Everything in the account, with no policy able to limit it, including billing and closing the account
C-2	Critical	Critical	Every original upload, and on 61% of images the GPS coordinates of where the contributor stood (9.8 million originals)
C-3	Critical	Critical	The 104,318 user records in the marketing export
C-4	Critical	Critical	The production database: every user, post, and moderation record
C-5	Critical	Critical	Read, change, or delete of every search index
C-6	High	Critical	Administrator access to the whole account, with the keys of an instance role
C-7	High	Critical	Administrator access, and the keys never expire
C-8	None	Critical	The production database password and a third-party API key
C-9	High	Critical	A compromise through any other finding would leave no trail past the 90 days of management events AWS keeps
C-10	Critical	Critical	Four GPUs to mine on, and whatever the instance's role and network can reach

What "verified by hand" means

Every finding in the register has evidence a reader can repeat: a read-only call that shows the setting, a sample, or a request from outside the account. The appendix lists the evidence for each. A finding is verified when we have both read the configuration and shown that the weakness is real: an exposure that anyone could reach was reached once, with one request and nothing kept; a weakness in code was read in the code. We did not run an exploit, and we did not read data.

Deliverable 1: the findings register

How to read a finding

- **Who can reach it** has four tiers: anyone on the internet; one stolen credential or one application bug; a foothold inside the account; and not an entry point.

- **Status on January 15** is one of four things: closed (every step done), in progress (a first step done), planned (dated, not started), or proposed for a written acceptance or a dated deferral. Nothing is called closed until the re-scan in week six confirms it.
- **Closed through** names who finished it: **Tidepost on notice** is Tidepost's engineers within about a day of our call, with no Vantalect plan; **Hardening** is a change Vantalect specified, reviewed, and verified and Tidepost's engineers made; the **Foundation** is the add-on, for the three findings only an organization can finish.
- **Planned dates** are the dates in the plan we agree at the readout. They are plans, and the week-six re-scan reports what happened.

The register at a glance

All 47 findings. Every one is in the founders' account, which the register calls tp-prod.

ID	Severity	Finding	Owner	Status on January 15
C-1	Critical	Root user with two active access keys and no MFA	Kofi Brandvold	In progress; next January 29
C-2	Critical	tp-media-originals public-read, and location metadata on 61% of images	Amara Delacroix	Closed January 14
C-3	Critical	tp-exports public with listing on: 104,318 user records	Lior Haddad	Closed January 6
C-4	Critical	RDS PostgreSQL publicly accessible from 0.0.0.0/0	Kofi Brandvold	Acceptance proposed, to March 22
C-5	Critical	OpenSearch domain with a public endpoint and an open access policy	Marcus Oyelaran	Planned January 21
C-6	Critical	Link-preview SSRF reaches IMDSv1 and an instance role with AdministratorAccess	Marcus Oyelaran	Closed January 8
C-7	Critical	Seven IAM users with administrator access and long-lived keys, two of them departed	Sasha Ilyin	In progress; next January 26
C-8	Critical	Database password and a third-party API key in the repository and in launch template user data	Marcus Oyelaran	Closed January 9
C-9	Critical	No CloudTrail trail	Sasha Ilyin	In progress; next January 28
C-10	Critical	A forgotten g5.12xlarge with SSH open and a Jupyter server without a token	Yuki Sorensen	Closed January 6

ID	Severity	Finding	Owner	Status on January 15
H-1	High	RDS and EBS volumes unencrypted at rest	Kofi Brandvold	Deferral proposed, to March 22
H-2	High	IMDSv1 on every instance	Kofi Brandvold	Planned January 22
H-3	High	No MFA on any of the 16 IAM users with a console password	Sasha Ilyin	Closed January 13
H-4	High	SSH open to the internet on 18 instances	Kofi Brandvold	Closed January 14
H-5	High	Account-level S3 Block Public Access off	Kofi Brandvold	Closed January 6
H-6	High	GuardDuty, Inspector, and Security Hub off in both Regions	Sasha Ilyin	Planned January 29
H-7	High	Redis without AUTH, TLS, or automatic backups	Marcus Oyelaran	Planned January 27
H-8	High	SageMaker notebooks with direct internet access and root access	Yuki Sorensen	Planned February 4
H-9	High	EKS endpoint public, with every developer mapped to cluster administrator	Kofi Brandvold	Planned January 30
H-10	High	No web application firewall on the two public load balancers	Marcus Oyelaran	Planned February 4
H-11	High	Two customer-managed KMS keys whose policies allow any identity in the account	Sasha Ilyin	Planned January 23
H-12	High	No deletion pipeline for removed posts' media	Marcus Oyelaran	Deferral proposed, to May 20
H-13	High	Moderation Lambda functions share one execution role with s3:* and sagemaker:*	Amara Delacroix	Planned February 9
H-14	High	CI on 400-day-old access keys instead of OIDC federation	Kofi Brandvold	Planned January 20
M-1	Medium	No VPC flow logs	Kofi Brandvold	Closed January 15
M-2	Medium	The default security group allows all traffic between members, and 9 instances use it	Kofi Brandvold	Planned January 22

ID	Severity	Finding	Owner	Status on January 15
M-3	Medium	Secrets in the environment variables of 9 Lambda functions	Marcus Oyelaran	Planned February 2
M-4	Medium	AWS Config not recording in either Region	Sasha Ilyin	Planned January 29
M-5	Medium	11 buckets accept requests over plain HTTP	Kofi Brandvold	Planned January 30
M-6	Medium	14 buckets use SSE-S3 where the data class needs customer-managed keys	Lior Haddad	Planned February 9
M-7	Medium	Server access logging off on 7 buckets	Kofi Brandvold	Acceptance proposed, to June 30
M-8	Medium	11 access keys unused for more than 90 days	Kofi Brandvold	Closed January 13
M-9	Medium	No IAM Access Analyzer	Sasha Ilyin	Planned January 29
M-10	Medium	SageMaker endpoints and training jobs without customer-managed volume keys	Yuki Sorensen	Planned February 6
M-11	Medium	No alarms on root sign-in, unauthorized API calls, or IAM changes, and PostgreSQL logs not exported	Kofi Brandvold	Planned January 20
M-12	Medium	Public IPv4 addresses on 14 private-tier instances	Kofi Brandvold	Planned January 28
M-13	Medium	CloudFront accepts TLS 1.0 from viewers	Bea Okafor	Planned January 27
M-14	Medium	Four vendor cross-account roles without an external ID	Kofi Brandvold	Planned January 22
M-15	Medium	Session Manager sessions not logged	Kofi Brandvold	Planned January 20
L-1	Low	41 unused security groups, 18 with blank descriptions	Kofi Brandvold	Planned February 4
L-2	Low	Three DNS records point at released Elastic IP addresses	Kofi Brandvold	Closed January 15
L-3	Low	Billing and operations alternate contacts are the founders' personal addresses	Gwen Tallis	Closed January 9

ID	Severity	Finding	Owner	Status on January 15
L-4	Low	Bucket names disclose internal project names	Kofi Brandvold	Acceptance proposed, to June 30
L-5	Low	Two public ECR repositories	Kofi Brandvold	Closed January 8
L-6	Low	Two unused IAM roles trust an account no one at Tidepost can identify	Kofi Brandvold	Planned January 20
L-7	Low	No DMARC policy on the company domain	Sasha Ilyin	Planned January 22
L-8	Low	Deletion protection off on 6 DynamoDB tables	Lior Haddad	Planned February 6

Critical findings

C-1: Root user with two active access keys and no MFA

Critical. Root user of tp-prod. **Who can reach it:** One stolen credential or one application bug.

What they do: Uses either root access key, from the GitHub Actions secret or the deploy script on a laptop. **What they reach:** Everything in the account, with no policy able to limit it, including billing and closing the account.

Failed checks: IAM.4 (2 failed resources), IAM.6 (1 failed resource), IAM.9 (1 failed resource). **SOC 2:** CC6.1. **Owner:** Kofi Brandvold. **Status on January 15:** In progress; next January 29.

Plan

- Done January 6, Tidepost on notice: Both root access keys deleted after the pipeline and the script moved to roles; two FIDO2 keys registered
- Planned January 29, Foundation: Root credentials removed from the member account under centralized root access after the January 28 join; root tasks run through sts:AssumeRoot

C-2: tp-media-originals public-read, and location metadata on 61% of images

Critical. S3 bucket tp-media-originals. **Who can reach it:** Anyone on the internet. **What they do:** Lists and downloads originals from the public bucket with no credentials. **What they reach:** Every original upload, and on 61% of images the GPS coordinates of where the contributor stood (9.8 million originals).

Failed checks: S3.2 (2 failed resources), S3.8 (17 failed resources). **SOC 2:** CC6.6. **Owner:** Amara Delacroix. **Status on January 15:** Closed January 14.

Plan

- Done January 6, Tidepost on notice: Block Public Access turned on and CloudFront origin access control put in front of the bucket; originals answer only a short-lived signed URL from the API, and every other reader gets renditions
- Done January 14, Hardening: Location metadata stripped from 9,800,000 image originals by an S3 Batch Operations job that ran January 7 to 14

C-3: tp-exports public with listing on: 104,318 user records

Critical. S3 bucket tp-exports. **Who can reach it:** Anyone on the internet. **What they do:** Lists the bucket with no credentials and downloads the export. **What they reach:** The 104,318 user records in the marketing export.

Failed checks: S3.2 (2 failed resources). **Owner:** Lior Haddad. **Status on January 15:** Closed January 6.

Plan

- Done January 6, Tidepost on notice: Closed within the hour; the CSV deleted after counsel copied it. With no access logs, exposure could not be ruled out; counsel was told, and the decision on notification is Tidepost's (Vantalect records only that counsel was told)

C-4: RDS PostgreSQL publicly accessible from 0.0.0.0/0

Critical. RDS for PostgreSQL 13 production writer. **Who can reach it:** One stolen credential or one application bug. **What they do:** Connects to the database listener from anywhere and tries the password, which C-8 had left in the repository. **What they reach:** The production database: every user, post, and moderation record.

Failed checks: RDS.2 (2 failed resources). **SOC 2:** CC6.6. **Owner:** Kofi Brandvold. **Status on January 15:** Acceptance proposed, to March 22.

Proposed written acceptance, to be signed by Dev Raman: PubliclyAccessible stays true until the new encrypted private instance replaces this one at the March 22 cutover; until then the security group admits only the BI vendor's four published ranges and TLS is required. It would run to March 22, 2026, the cutover that the Well-Architected Review performs. It would meet the gate as accepted in writing, not as closed, and stays on the register as open.

Plan

- Done January 7, Hardening: Security group restricted to the BI vendor's four published ranges and TLS required; the staging copy's security group restricted the same day

C-5: OpenSearch domain with a public endpoint and an open access policy

Critical. OpenSearch domain tp-search (2.13). **Who can reach it:** Anyone on the internet. **What they do:** Sends requests to the open search endpoint; the access policy allows every action to every caller. **What they reach:** Read, change, or delete of every search index.

Failed checks: 0pensearch.2 (1 failed resource). **SOC 2:** CC6.6. **Owner:** Marcus Oyelaran. **Status on January 15:** Planned January 21.

Plan

- Planned January 21, Hardening: Domain moved into the VPC with fine-grained access control and a restrictive access policy

C-6: Link-preview SSRF reaches IMDSv1 and an instance role with AdministratorAccess

Critical. Link-preview service on the web tier. **Who can reach it:** One stolen credential or one application bug. **What they do:** Gives the link-preview service a URL that reaches the instance metadata service and takes the role's temporary credentials. **What they reach:** Administrator access to the whole account, with the keys of an instance role.

Failed checks: IAM.1 (4 failed resources). **SOC 2:** CC6.3. **Owner:** Marcus Oyelaran. **Status on January 15:** Closed January 8.

Plan

- Done January 8, Hardening: Allowlisted egress proxy and URL validation added; IMDSv2 required on the tier; the role cut to 14 actions

C-7: Seven IAM users with administrator access and long-lived keys, two of them departed

Critical. Seven IAM users in tp-prod. **Who can reach it:** One stolen credential or one application bug. **What they do:** Uses a long-lived administrator key, including the keys of the two people who had left. **What they reach:** Administrator access, and the keys never expire.

Failed checks: IAM.1 (4 failed resources), IAM.2 (16 failed resources). **SOC 2:** CC6.2. **Owner:** Sasha Ilyin. **Status on January 15:** In progress; next January 26.

Plan

- Done January 6, Tidepost on notice: The two departed users' passwords and keys deleted, and the users with them
- Planned January 26, Hardening: The 14 current staff provisioned into IAM Identity Center over SCIM, by group (Identity Center connected January 23)
- Planned January 28, Hardening: Permission sets assigned to tp-prod the day it joined the organization: the 5 remaining administrators and the 9 other people with console access sign in through Identity Center
- Planned February 10, Foundation: The five IAM users deleted after the policy set that denies new IAM users and keys reached Prod on February 5

C-8: Database password and a third-party API key in the repository and in launch template user data

Critical. The backend repository and launch template versions. **Who can reach it:** A foothold inside the account. **What they do:** Reads the repository or a launch template's user data, as any engineer or contractor with access can. **What they reach:** The production database password and a third-party API key.

Failed checks: None; no benchmark control covers it. **SOC 2:** CC6.1. **Owner:** Marcus Oyelaran. **Status on January 15:** Closed January 9.

Plan

- Done January 9, Hardening: Both secrets rotated into Secrets Manager and read at runtime, and user data cleaned; the history rewrite was declined because rotation closes the exposure

C-9: No CloudTrail trail

Critical, and not an entry point. CloudTrail in tp-prod. **Who can reach it:** Not an entry point: it removes the evidence. **What they do:** Nothing: it is the missing record. **What they reach:** A compromise through any other finding would leave no trail past the 90 days of management events AWS keeps.

Failed checks: CloudTrail.1 (1 failed resource), CloudTrail.2 (1 failed resource), CloudTrail.4 (1 failed resource). **SOC 2:** CC7.1. **Owner:** Sasha Ilyin. **Status on January 15:** In progress; next January 28.

Plan

- Done January 6, Hardening: An account trail created, multi-Region, writing to a locked bucket

- Planned January 28, Foundation: Replaced by the organization trail into tp-log-archive when the account joined

C-10: A forgotten g5.12xlarge with SSH open and a Jupyter server without a token

Critical. EC2 instance (g5.12xlarge) in tp-prod. **Who can reach it:** Anyone on the internet. **What they do:** Runs code on a GPU server through the Jupyter server, which asks for no token, with SSH also open. **What they reach:** Four GPUs to mine on, and whatever the instance's role and network can reach.

Failed checks: EC2 . 13 (6 failed resources), EC2 . 19 (3 failed resources). **Owner:** Yuki Sorensen. **Status on January 15:** Closed January 6.

Plan

- Done January 6, Tidepost on notice: Snapshotted for the record and terminated. No indicators in its shell history, processes, or packages; with no flow logs, compromise could not be ruled out, and counsel was told. The cost engagement does not count this instance

High findings

14 High findings. The evidence for each is in the appendix under the same ID.

H-1: RDS and EBS volumes unencrypted at rest

High. RDS production writer and 58 of 61 EBS volumes. **Failed checks:** RDS . 3 (2), EC2 . 7 (2). **Owner:** Kofi Brandvold. **Status on January 15:** Deferral proposed, to March 22.

Proposed dated deferral, to be signed by Dev Raman: the production database cannot be encrypted in place; the new encrypted PostgreSQL 16 instance replaces it at the March 22 cutover. It would run to March 22, 2026, when the Well-Architected Review finishes it.

Plan

- Planned January 21, Hardening: EBS default encryption turned on in both Regions
- Planned January 27, Hardening: The staging copy of the database re-created from an encrypted snapshot copy
- Planned February 10, Hardening: The last unencrypted volumes replaced as node groups and instances rotated

H-2: IMDSv1 on every instance

High. 52 EC2 instances and their launch templates. **Failed checks:** EC2.8 (52). **Owner:** Kofi Brandvold. **Status on January 15:** Planned January 22.

Plan

- Planned January 22, Hardening: HttpTokens required on every instance and launch template; a declarative policy in the Foundation's policy set keeps it that way

H-3: No MFA on any of the 16 IAM users with a console password

High. 16 IAM users. **Failed checks:** IAM.5 (16). **Owner:** Sasha Ilyin. **Status on January 15:** Closed January 13.

Plan

- Done January 13, Hardening: A policy condition requiring MFA applied to every console user; the remaining users' IAM identities were replaced by Identity Center sign-in on January 28, when the permission sets reached tp-prod

H-4: SSH open to the internet on 18 instances

High. 6 security groups covering 18 instances. **Failed checks:** EC2.13 (6). **Owner:** Kofi Brandvold. **Status on January 15:** Closed January 14.

Plan

- Done January 14, Hardening: Port 22 rules removed from all six groups; shell access through SSM Session Manager

H-5: Account-level S3 Block Public Access off

High. S3 account settings in tp-prod. **Failed checks:** S3.1 (1). **Owner:** Kofi Brandvold. **Status on January 15:** Closed January 6.

Plan

- Done January 6, Tidepost on notice: Account-level Block Public Access turned on in the same sitting as C-2; app versions older than 4.2, which read the originals bucket on its S3 address, were sent to the update prompt that afternoon (C-2)

H-6: GuardDuty, Inspector, and Security Hub off in both Regions

High. Detection services in tp-prod. **Failed checks:** GuardDuty.1 (2), SecurityHub.1 (2), Inspector.1 (2). **SOC 2:** CC6.8, CC7.2. **Owner:** Sasha Ilyin. **Status on January 15:** Planned January 29.

Plan

- Planned January 29, Hardening: GuardDuty (with runtime monitoring on EKS), Inspector, and Security Hub enabled, delegated to tp-audit

H-7: Redis without AUTH, TLS, or automatic backups

High. ElastiCache Redis OSS 7.1 replication group. **Failed checks:** ElastiCache.1 (1), ElastiCache.5 (1). **SOC 2:** CC6.6. **Owner:** Marcus Oyelaran. **Status on January 15:** Planned January 27.

Plan

- Planned January 27, Hardening: Replication group rebuilt with in-transit encryption, an AUTH token read from Secrets Manager, and a daily automatic backup

H-8: SageMaker notebooks with direct internet access and root access

High. 6 SageMaker notebook instances. **Failed checks:** SageMaker.1 (6). **Owner:** Yuki Sorensen. **Status on January 15:** Planned February 4.

Plan

- Planned February 4, Hardening: Notebooks moved to VPC-only access with root disabled by a lifecycle configuration

H-9: EKS endpoint public, with every developer mapped to cluster administrator

High. 3 EKS clusters (production, staging, development). **Failed checks:** EKS.1 (3). **SOC 2:** CC6.3. **Owner:** Kofi Brandvold. **Status on January 15:** Planned January 30.

Plan

- Planned January 30, Hardening: Endpoints made private on all three clusters; developers moved to EKS access entries with namespace-scoped roles

H-10: No web application firewall on the two public load balancers

High. 2 Application Load Balancers. **Failed checks:** ELB. 16 (2). **SOC 2:** CC6.6. **Owner:** Marcus Oyelaran. **Status on January 15:** Planned February 4.

Plan

- Planned February 4, Hardening: AWS WAF web ACL with the managed rule groups and a rate limit associated with both

H-11: Two customer-managed KMS keys whose policies allow any identity in the account

High. 2 KMS keys. **Failed checks:** none; no benchmark control covers it. **Owner:** Sasha Ilyin. **Status on January 15:** Planned January 23.

Plan

- Planned January 23, Hardening: Both key policies rewritten with named key administrators and per-service grants

H-12: No deletion pipeline for removed posts' media

High. Originals, renditions, and backups of removed posts. **Failed checks:** none; no benchmark control covers it. **SOC 2:** C1.2. **Owner:** Marcus Oyelaran. **Status on January 15:** Deferral proposed, to May 20.

Proposed dated deferral, to be signed by Sasha Ilyin: the app team cannot ship the deletion pipeline before the retention schedule exists, and the schedule waits on counsel. The risk that remains until then: a removed post's renditions still load through the distribution for anyone who kept their address, and its original for anyone holding a signed URL issued before the removal, until that URL expires. It would run to May 20, 2026, when Tidepost finishes it.

Plan

H-13: Moderation Lambda functions share one execution role with s3:* and sagemaker:*

High. 11 Lambda functions, one execution role. **Failed checks:** none; no benchmark control covers it. **SOC 2:** CC6.3. **Owner:** Amara Delacroix. **Status on January 15:** Planned February 9.

Plan

- Planned February 9, Hardening: One role per function, each limited to its own buckets and endpoints

H-14: CI on 400-day-old access keys instead of OIDC federation

High. The CI IAM user and its 2 access keys. **Failed checks:** IAM.3 (16). **Owner:** Kofi Brandvold.

Status on January 15: Planned January 20.

Plan

- Planned January 20, Hardening: GitHub Actions moved to OIDC federation with a deploy role per repository; the CI user and both its keys deleted

Medium and Low findings

The 15 Medium and 8 Low findings.

ID	Severity	Finding	Failed checks	Owner	Status on January 15
M-1	Medium	No VPC flow logs	EC2.6	Kofi Brandvold	Closed January 15
M-2	Medium	The default security group allows all traffic between members, and 9 instances use it	EC2.2	Kofi Brandvold	Planned January 22
M-3	Medium	Secrets in the environment variables of 9 Lambda functions	None	Marcus Oyelaran	Planned February 2
M-4	Medium	AWS Config not recording in either Region	Config.1	Sasha Ilyin	Planned January 29
M-5	Medium	11 buckets accept requests over plain HTTP	S3.5	Kofi Brandvold	Planned January 30
M-6	Medium	14 buckets use SSE-S3 where the data class needs customer-managed keys	None	Lior Haddad	Planned February 9
M-7	Medium	Server access logging off on 7 buckets	S3.9	Kofi Brandvold	Acceptance proposed, to June 30
M-8	Medium	11 access keys unused for more than 90 days	IAM.8	Kofi Brandvold	Closed January 13

ID	Severity	Finding	Failed checks	Owner	Status on January 15
M-9	Medium	No IAM Access Analyzer	IAM.28	Sasha Ilyin	Planned January 29
M-10	Medium	SageMaker endpoints and training jobs without customer-managed volume keys	None	Yuki Sorensen	Planned February 6
M-11	Medium	No alarms on root sign-in, unauthorized API calls, or IAM changes, and PostgreSQL logs not exported	RDS.9	Kofi Brandvold	Planned January 20
M-12	Medium	Public IPv4 addresses on 14 private-tier instances	None	Kofi Brandvold	Planned January 28
M-13	Medium	CloudFront accepts TLS 1.0 from viewers	None	Bea Okafor	Planned January 27
M-14	Medium	Four vendor cross-account roles without an external ID	None	Kofi Brandvold	Planned January 22
M-15	Medium	Session Manager sessions not logged	None	Kofi Brandvold	Planned January 20
L-1	Low	41 unused security groups, 18 with blank descriptions	None	Kofi Brandvold	Planned February 4
L-2	Low	Three DNS records point at released Elastic IP addresses	None	Kofi Brandvold	Closed January 15
L-3	Low	Billing and operations alternate contacts are the founders' personal addresses	None	Gwen Tallis	Closed January 9
L-4	Low	Bucket names disclose internal project names	None	Kofi Brandvold	Acceptance proposed, to June 30
L-5	Low	Two public ECR repositories	None	Kofi Brandvold	Closed January 8
L-6	Low	Two unused IAM roles trust an account no one at Tidepost can identify	None	Kofi Brandvold	Planned January 20
L-7	Low	No DMARC policy on the company domain	None	Sasha Ilyin	Planned January 22
L-8	Low	Deletion protection off on 6 DynamoDB tables	None	Lior Haddad	Planned February 6

Acceptances and deferrals proposed

5 findings are proposed for a written acceptance or a dated deferral instead of a fix. A Critical accepted in writing meets the gate as accepted, not as closed: it stays on the register as open and carries a date. The readout on January 16, 2026 decides C-4, H-1, and H-12; Sasha Ilyin signs M-7 and L-4 by January 21, 2026.

The proposed acceptances and deferrals. Each has a named signer and a date.

ID	Severity	Signs	Signed on	Runs to	Why
C-4	Critical	Dev Raman	January 16	March 22 (Well-Architected Review)	PubliclyAccessible stays true until the new encrypted private instance replaces this one at the March 22 cutover; until then the security group admits only the BI vendor's four published ranges and TLS is required
H-1	High	Dev Raman	January 16	March 22 (Well-Architected Review)	The production database cannot be encrypted in place; the new encrypted PostgreSQL 16 instance replaces it at the March 22 cutover
H-12	High	Sasha Ilyin	January 16	May 20 (Tidepost)	The app team cannot ship the deletion pipeline before the retention schedule exists, and the schedule waits on counsel. The risk that remains until then: a removed post's renditions still load through the distribution for anyone who kept their address, and its original for anyone holding a signed URL issued before the removal, until that URL expires
M-7	Medium	Sasha Ilyin	January 21	Reviewed June 30	Object-level CloudTrail data events cover the two buckets that hold user data, and the other five hold public news media; access logs on the media buckets would be among the largest log volumes in the account
L-4	Low	Sasha Ilyin	January 21	Reviewed June 30	S3 bucket names cannot be changed in place, and the names disclose nothing that is not already in public contracts

Deliverable 2: the governance review

This review is also the Foundation add-on's discovery. It reads the account the way an organization would have to take it over: what exists above the account (nothing), what is shared, and what is missing.

How the account is governed today

Tidepost has one account, opened by the founders and still its own payer. There is no organization, so there are no organizational units, no policies above the account, no delegated administrators, and nowhere for a central trail to go. Accounts are opened by hand in the console, and there has only ever been one. 18 IAM users stand in for an identity system: 16 have console passwords, 7 of those are administrators, and 2 of the administrators have left the company.

The Foundation's checks read as a governance review: what is there, and what the end state is.

Area	As found	The target, and the check that tests it
Landing zone	No organization and no landing zone	The landing zone is enrolled, active, and not drifted; all features are on in the organization (MAF-01)
Accounts placed	One standalone account; no organization to place it in	Every in-scope account is in its target OU and enrolled (MAF-02)
Organization trail	No trail of any kind (C-9)	A multi-Region organization trail, logging, with log file validation, delivers to a bucket in the Log Archive account (MAF-03)
Security delegated	No security service enabled	GuardDuty, Security Hub, IAM Access Analyzer, and the Config aggregator (and Inspector) are administered from the Audit account, with new accounts enrolled automatically (MAF-04)
Identity	No Identity Center; 18 IAM users, seven of them administrators with long-lived keys	IAM Identity Center is the organization's instance and is connected to the identity provider; no workload account has an IAM user with a console password or an active access key, except in the Exceptions OU with a written exception (MAF-05)
Root	Two active root access keys and no root MFA (C-1)	The management account's root user has MFA; centralized root access is on; member accounts hold no root password or access keys (MAF-06)
Guardrails	No organization, so no SCP, RCP, or declarative policy	The agreed SCPs, RCPs, and declarative policies are attached at the agreed OUs, inherited by every in-scope account, and match the repository (MAF-07)
Controls	No Control Tower	The agreed Control Tower controls are enabled on every target OU (MAF-08)
Vending	No Account Factory	New accounts are vended through Account Factory, and one account vended in week five passes MAF-02 through MAF-08 untouched by hand (MAF-09)

Area	As found	The target, and the check that tests it
Backup	No central backup; a snapshot cron job in the one account	A backup policy is attached to the agreed OUs, AWS Backup is administered from a delegated account, and copies land in a central vault in a separate account (MAF-10)
Network	One VPC and no Transit Gateway	Shared networking is owned by a Network account and shared through AWS RAM (MAF-11, out of scope)
Tagging	No tags on 94% of resources and no tag policy	The agreed tag policy is attached and effective, with its compliance report readable from the management account (MAF-12)
No lingering access	No role yet	Vantalect's operator role and any temporary assignment are gone from the management account (MAF-13)

The discovery items

These are the items the Foundation's discovery sized before it designed anything. Each has an owner. The Foundation plan readout carries the handling of each.

The discovery items, sized from the account as found.

ID	Area	Size	What we found	Owner
FR-1	Billing transfer	Medium	One account that joins mid-month, with no commitments or credits, no budgets, no cost allocation tags, and no Cost and Usage Report to carry over	Gwen Tallis
FR-2	Reserved Instances and Savings Plans	Low	None exist; the Activate credits ran out in June 2025	Gwen Tallis
FR-3	Marketplace subscriptions	Low	No active subscription in the inventory	Gwen Tallis
FR-4	Support plans	Medium	Support plans are per account: tp-prod has Business Support+ on its own usage, the new accounts start on Basic Support, and an account that has to leave again needs a plan, contact information, and a current payment method of its own	Gwen Tallis
FR-5	Service quotas	Low	Quotas move with the account; a vended account starts at the defaults	Kofi Brandvold
FR-6	Account-level dependencies	Low	There was no source organization, so no policy conditioned on a source organization ID	Kofi Brandvold
FR-7	Root email and MFA custody	Medium	tp-prod held two active root keys and no MFA on January 5	Sasha Ilyin
FR-8	SCP and RCP blast radius	High	Production runs in one account; a wrong deny stops it, and the error surfaces only as access denied	Kofi Brandvold
FR-9	Control Tower enrollment	Low	One existing account to enroll, with Config off	Kofi Brandvold
FR-10	SOC 2 timing	Medium	The observation window opens April 1	Sasha Ilyin

Deliverable 3: the target organization

The path: a new organization, with the founders' account joining it

We recommend the **greenfield** path over a **retrofit**, and the sponsor decides it at the readout on January 16, 2026.

- 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 founders' account joins as the production member, so no workload moves and no commitment or credit is lost (there were none: no Savings Plan, no Reserved Instance, and the Activate credits ran out in June 2025).

Moving the staging and data workloads out of tp-prod is workload migration, a change order or another statement of work. The add-on vends the accounts; Tidepost moves into them on its own calendar (the data accounts wait for the third quarter).

The accounts

9 accounts, in 9 organizational units. Account IDs are masked to their last four digits.

The nine accounts and where each sits.

Account	ID	Unit	Purpose	Owner	When
tp-management	...7702	Root	Payer, Control Tower, IAM Identity Center, and the Cost and Usage Report data export	Kofi Brandvold	Created January 12
tp-log-archive	...7715	Security	The organization trail and AWS Config history	Sasha Ilyin	Planned January 21
tp-audit	...7723	Security	Delegated GuardDuty, Security Hub, IAM Access Analyzer, the Config aggregator, and Inspector	Sasha Ilyin	Planned January 21
tp-backup	...7738	Infrastructure	The central backup vault (vault lock in compliance mode) and delegated AWS Backup	Kofi Brandvold	Planned February 10
tp-prod	...4417	Workloads/Prod	The founders' account, joined and enrolled: production, and until June the old staging	Kofi Brandvold	Joins January 28
tp-staging	...7746	Workloads/NonProd	Staging, empty until the June rebuild (EC2-1a)	Kofi Brandvold	Planned January 29
tp-dev	...7751	Workloads/NonProd	Developer instances, moved by Tidepost's engineers on February 4	Kofi Brandvold	Planned February 3
tp-sandbox-ml	...7769	Sandbox	Notebooks and experiments; vended through Account Factory untouched by hand (MAF-09)	Yuki Sorensen	Planned February 5
tp-policy-test	...7774	Policy Staging	Proving every policy before it is attached	Kofi Brandvold	Planned January 29

The organizational units

The units, created with the landing zone. Suspended and Exceptions stay empty and ready.

Unit	Parent	Accounts	Note
Security	Root	tp-log-archive, tp-audit	Created with the landing zone
Infrastructure	Root	tp-backup	Empty until tp-backup on February 10
Workloads	Root	None	Holds Prod and NonProd; no policy is attached at this level
Workloads/Prod	Workloads	tp-prod	Empty until tp-prod joined on January 28
Workloads/NonProd	Workloads	tp-staging, tp-dev	Empty until tp-staging on January 29
Sandbox	Root	tp-sandbox-ml	Created with the landing zone; empty until tp-sandbox-ml on February 5
Policy Staging	Root	tp-policy-test	Every policy is proven here before any other OU
Suspended	Root	None	Empty and ready; a deny-all policy is attached
Exceptions	Root	None	Empty and ready; the only OU without the IAM-user policy

The policy set

11 policies in 5 kinds go in through a Policy Staging unit first: nothing is attached to production until it has run in tp-policy-test, and nothing goes to a unit that holds workloads until it has run for 24 hours without a denial the policy caused. The Foundation's policy set appendix holds every policy as code and says what each blocks. 40 Control Tower controls are enabled on top.

The policy set by kind.

Kind	CountPolicies
SCP	4tp-scp-baseline, tp-scp-no-member-root, tp-scp-no-iam-users, tp-scp-suspended-deny-all
RCP	3tp-rcp-s3-perimeter, tp-rcp-kms-perimeter, tp-rcp-sts-perimeter
declarative (EC2)	2tp-decl-ec2-iams, tp-decl-ec2-no-public-sharing
tag policy	1tp-tag-baseline
backup policy	1tp-backup-prod

The change windows

Six windows, each approved in writing two business days ahead, each run through the time-boxed VantalectFoundationOperator role in tp-management. The approvers are Dev Raman and Kofi Brandvold.

The change windows. W1 is approved on January 16, 2026, after the readout.

Window	Date	Hours (CST)	What happens
W1	Jan 21	09:00 to 15:00	Landing zone
W2	Jan 23	09:00 to 12:00	IAM Identity Center and the identity provider
W3	Jan 28	09:00 to 15:00	The join and enrollment
W4	Feb 3	09:00 to 12:00	Policies to Sandbox and NonProd
W5	Feb 5	09:00 to 13:00	Policies to Prod, and the vended account
W6	Feb 10	09:00 to 14:00	Backup and tag policies; the backup account

How Vantalect’s access is limited

Vantalect holds one role, VantalectFoundationOperator, and no write access to any member account. Its trust is limited: Charles’s named principal only; MFA required; a source identity naming him; aws:CurrentTime bounds from the window’s start to one hour before its end, the condition AWS checks when a session starts; sessions of at most one hour, so the last one ends when the window does. It explicitly cannot: closing accounts; deleting the organization; changing payment methods or billing contacts; creating IAM users or access keys; leaving the organization.

Every call lands in the organization trail, and an EventBridge rule posts each AssumeRole to the platform channel. Tidepost also keeps a break-glass role, TidepostBreakGlass, in every member account, held by Sasha Ilyin and Noor Castellanos, with an alarm on every use.

Deliverable 4: the SOC 2 technical map

What this map is and is not

Vantalect is not the auditor and does not issue, predict, or influence a SOC 2 report. SOC 2 reports are issued by licensed CPA firms. This map lists controls that are in place on AWS, the date each began operating, and where the evidence is; the auditor tests them. It is readiness evidence, not an opinion, and nothing here predicts how the auditor will weigh any of it. Tidepost’s SOC 2 Type 2 examination covers the Security, Availability, and Confidentiality Trust Services Categories; of their criteria, AWS controls reach CC6, CC7, CC8, A1, and C1, and this map covers only those.

The map lists 35 controls. On January 15, 2026, 4 are in place and operating, and 31 are planned. Of the whole map, 33 are operating or planned to be operating before the observation window opens on April 1, 2026, the latest on March 27, 2026; 2 begin after it opens (C1.2).

The controls by criteria group. Dates are when each control began or is planned to begin operating.

Criteria	Group	Controls	Operating onOperating from, first to January 15last
CC6.1, CC6.2, CC6.3	Logical access	7	2January 8 to February 9
CC6.6, CC6.7	Boundaries and transmission	9	2January 6 to March 22
CC6.8	Unauthorized software	1	0January 29
CC7.1, CC7.2	Monitoring	5	0January 20 to March 20
CC7.3, CC7.4, CC7.5	Incidents	3	0February 12 to March 26
CC8.1	Change management	1	0March 27
A1.1, A1.2, A1.3	Availability and recovery	6	0February 10 to March 25
C1.1, C1.2	Confidential information	3	0March 20 to May 20

Every control

The 35 controls. Planned means not yet operating on January 15.

Criterion	Control	Account	Owner	Operating from	Evidence is in
CC6.1	Database and third-party credentials in Secrets Manager, read at runtime; none in code or launch template user data	tp-prod	Marcus Oyelaran	January 9	Secrets Manager inventory and the repository secret-scan results
CC6.1	Root user holds no access keys, and root credentials are removed from member accounts under centralized root access	tp-log-archive	Sasha Ilyin	January 29 (planned)	IAM credential reports and root-task records in the organization trail
CC6.2	People sign in through IAM Identity Center permission sets with MFA required; departed people removed	tp-management	Sasha Ilyin	January 28 (planned)	Identity Center assignments and sign-in events
CC6.2	Organization policies deny new IAM users and long-lived keys outside the Exceptions OU; one vendor user in tp-prod remains under a written waiver, its key rotated only through a role scoped to that user	tp-management	Sasha Ilyin	February 5 (planned)	Service control policy attachments and the exception signed February 11
CC6.3	Link-preview service role cut to 14 actions; IMDSv2 required	tp-prod	Marcus Oyelaran	January 8	IAM policy versions and Access Analyzer findings
CC6.3	EKS endpoints private, and developers on namespace-scoped access entries instead of cluster administrator	tp-prod	Kofi Brandvold	January 30 (planned)	EKS access entries and cluster configuration history

Criterion	Control	Account	Owner	Operating from	Evidence is in
CC6.3	One execution role per moderation function, each limited to its own buckets and endpoints	tp-prod	Amara Delacroix	February 9 (planned)	IAM role policies and Config history
CC6.6	Block Public Access on the account and every bucket; CloudFront origin access control in front of the media bucket	tp-prod	Kofi Brandvold	January 6	The account trail's PutPublicAccessBlock and PutBucketPolicy calls for January 6 to 28, then Config history for the S3 public-access rules
CC6.6	RDS reachable only from the BI vendor's four published ranges, with TLS required, until the new private instance replaces it	tp-prod	Kofi Brandvold	January 7	Security group history and the written acceptance of January 16
CC6.6	OpenSearch inside the VPC with fine-grained access control	tp-prod	Marcus Oyelaran	January 21 (planned)	The account trail's OpenSearch configuration calls, then Config history for the domain
CC6.6	Redis with in-transit encryption and an AUTH token from Secrets Manager	tp-prod	Marcus Oyelaran	January 27 (planned)	The account trail's ElastiCache calls, then Config history for the replication group
CC6.6	No inbound SSH; shell access through Session Manager with session logs	tp-prod	Kofi Brandvold	January 20 (planned)	Session Manager logs and security group history
CC6.6	AWS WAF on both public load balancers, with managed rule groups and a rate limit	tp-prod	Marcus Oyelaran	February 4 (planned)	WAF logs and web ACL associations

Criterion	Control	Account	Owner	Operating from	Evidence is in
CC6.6	Production database private (PubliclyAccessible false) in the new encrypted PostgreSQL 16 instance	tp-prod	Kofi Brandvold	March 22 (planned)	RDS configuration and the March 22 cutover record
CC6.7	TLS required in transit: TLS-only bucket statements and a CloudFront minimum of TLS 1.2	tp-prod	Kofi Brandvold	January 30 (planned)	S3 bucket policies and CloudFront distribution configuration
CC6.7	Organization data perimeter (resource control policies for S3, KMS, and STS) that admits the CloudFront origin access control	tp-management	Kofi Brandvold	February 5 (planned)	Resource control policy attachments
CC6.8	Inspector on EC2 and ECR, and GuardDuty runtime monitoring on EKS, delegated to tp-audit	tp-audit	Sasha Ilyin	January 29 (planned)	Inspector and GuardDuty findings in tp-audit
CC7.1	Organization trail, multi-Region, into tp-log-archive	tp-log-archive	Sasha Ilyin	January 28 (planned)	The organization trail in tp-log-archive
CC7.1	AWS Config recording in every governed account, with the aggregator in tp-audit	tp-audit	Sasha Ilyin	January 29 (planned)	Config history and the aggregator in tp-audit
CC7.2	GuardDuty and Security Hub findings reviewed from tp-audit	tp-audit	Sasha Ilyin	January 29 (planned)	Security Hub and GuardDuty in tp-audit
CC7.2	Alarms on root sign-in, unauthorized API calls, and IAM changes, over VPC flow logs and the trail	tp-prod	Kofi Brandvold	January 20 (planned)	CloudWatch alarm history and flow logs

Criterion	Control	Account	Owner	Operating from	Evidence is in
CC7.2	Alarms on the service-level objectives for the API and the ranking endpoint	tp-prod	Kofi Brandvold	March 20 (planned)	CloudWatch alarm history
CC7.3	Security runbooks for a leaked credential, a public bucket, and a compromised instance	tp-prod	Sasha Ilyin	February 12 (planned)	The runbooks and the evidence index handed over February 12
CC7.4	On-call rotation and the incident process, exercised in a tabletop	tp-prod	Kofi Brandvold	March 26 (planned)	The on-call schedule and the tabletop record
CC7.5	Post-incident review step in the incident process	tp-prod	Kofi Brandvold	March 26 (planned)	The tabletop record and the review template
CC8.1	Production changes through a pull request and the pipeline: read-only permission sets in tp-prod for developers, machine learning, and data, console-built resources imported into the CDK, and drift reports on console changes	tp-prod	Kofi Brandvold	March 27 (planned)	Pull requests, pipeline runs, and CloudFormation drift reports
A1.1	Service quota alarms at 80% for Rekognition, SageMaker, and EC2 vCPUs, with the limits raised to leave headroom for a zone failover	tp-prod	Kofi Brandvold	March 13 (planned)	CloudWatch alarm history and the Service Quotas request history
A1.1	Capacity follows demand: target tracking on the API tier, Karpenter on EKS, and queue-depth scaling for the transcoders	tp-prod	Kofi Brandvold	March 17 (planned)	Auto Scaling activity, Karpenter events, and CloudWatch capacity metrics

Criterion	Control	Account	Owner	Operating from	Evidence is in
A1.2	AWS Backup plan with a locked vault in tp-backup and cross-Region copies to us-west-2	tp-backup	Kofi Brandvold	February 10 (planned)	AWS Backup job history in tp-backup
A1.2	Production database in a Multi-AZ instance	tp-prod	Kofi Brandvold	March 22 (planned)	RDS configuration and the March 22 cutover record
A1.3	Restore test from the central vault	tp-backup	Kofi Brandvold	March 24 (planned)	The restore test record and timings
A1.3	Availability Zone failure drill	tp-prod	Kofi Brandvold	March 25 (planned)	The drill record and service dashboards
C1.1	Data-class standard, with a data-class tag on every data store	tp-management	Sasha Ilyin	March 20 (planned)	Tag policy compliance and the standard
C1.2	Retention schedule for user content, written with counsel	tp-prod	Amara Delacroix	May 20 (planned)	The signed schedule
C1.2	Deletion pipeline for removed posts' media, across originals, renditions, and backups	tp-prod	Marcus Oyelaran	May 20 (planned)	Pipeline job history and a sampled deletion check

The C1.2 disposal controls are planned to begin after the window opens (2 of the map). The retention schedule and the deletion pipeline are planned for May 20, 2026, after the window opens on April 1, 2026. They wait on counsel and on the app team (H-12, proposed for a written deferral). Whether a control that begins operating inside the window matters to the report is the auditor's decision, and we do not predict it.

What is Tidepost's

No Vantalect engagement touches these. They are Tidepost's, and the auditor tests them.

What no engagement touches.

Criterion	What it covers	Owner
CC1	The control environment and board oversight	Noor Castellanos
CC1.4	Background checks and the HR side of hiring; removing a leaver's AWS access is mapped under CC6.2 and CC6.3	Noor Castellanos
CC2	Communication and information	Noor Castellanos
CC3	The risk assessment program	Sasha Ilyin
CC4	Monitoring activities: Tidepost's own evaluation of whether its controls work. The Security Hub and Config conformance results under CC7.1 and CC7.2 are evidence it can use for CC4.1	Sasha Ilyin
CC5	Control activities: the written policies	Sasha Ilyin
CC9	Vendor management	Sasha Ilyin
System description	The system description the auditor reads first	Sasha Ilyin

Amazon Web Services is a carved-out subservice organization. AWS operates the data centers, the hardware, and the virtualization under every account, and those controls are carved out of Tidepost's system description. AWS's own SOC 2 report covers them; it is in AWS Artifact, and Tidepost's CPA firm reads it alongside Tidepost's evidence. The controls in this map are the complementary subservice organization controls: what Tidepost runs on AWS so that AWS's controls are enough.

The audit window runs April 1, 2026 to September 30, 2026. Tidepost's CPA firm runs its own readiness assessment from February 17, 2026 to March 6, 2026, and this map is the evidence Sasha Ilyin gives it for the AWS controls.

What happens next

The readout on January 16, 2026 agrees the register and the 10 Critical findings as the gate's set, takes the greenfield decision, and signs the acceptances. Weeks 3 to 6 then carry the plan above: week 3 is the Critical findings and the workload guardrails, week 4 identity, week 5 detection and response, and week 6 the re-scan. The Foundation add-on starts on January 20, 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.