

AWS SECURITY, COMPLIANCE & GOVERNANCE · SAMPLE DELIVERABLE

Runbooks, the Evidence Index, and Handover

Week 6 of 6: Hand over · prepared for Tidepost, Inc.

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

February 12, 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

Summary	3
The handover workshop	4
The runbooks	4
SR-1: A credential is leaked or misused	5
SR-2: A bucket, snapshot, or database is public	6
SR-3: An instance or a container is compromised	7
SR-4: A root sign-in, a break-glass sign-in, or an IAM change nobody planned	8
SR-5: A detection service stops, or an account drops out of it	9
The evidence index	10
tp-audit	10
tp-backup	11
tp-log-archive	11
tp-management	11
tp-prod	12
Evidence that is not an AWS control	14
The SOC 2 technical map, as of February 12, 2026	15
The controls that begin after the window opens	19
What is Tidepost's	20
What remains	20
Declined	22
Checks that still fail, by decision	22
Keeping it where it is	23
The monthly review	23
What recurs	24
The guardrails Tidepost now owns	25
The new-account baseline	25
Vantalect's access ends	26
What Tidepost keeps	26

Summary

This is the handover. In six weeks the Audit’s 50–check scan went from 12 checks passing to 45 (24% to 90%), and all 10 critical findings agreed at the readout are closed or accepted in writing: 9 closed, 1 accepted until the cutover, so the gate set at the readout is met. This report is what Tidepost keeps: **5 security runbooks**, the **evidence index** for the auditor, the **SOC 2 technical map** as of February 12, 2026, and the list of what remains, each with an owner and a date.

Two parts of this report carry the most weight. The first is the SOC 2 technical map. Vantalect is not the auditor and does not issue, predict, or influence a SOC 2 report; it provides dated technical evidence of AWS controls and says where that evidence is. Of the 35 controls in the map, **22 are in place on February 12** and 13 are planned, each with the date it begins operating. Of those planned, 11 begin before the observation window opens on April 1 and 2 begin after it: the C1.2 disposal controls, on May 20, set out in [The controls that begin after the window opens](#). The second is the list of what remains, in [What remains](#).

The one thing to know: **the score does not hold itself**. A new account, a new workload, or a new engineer adds failing checks faster than anyone expects, and the guardrails stop only the failures they were written for. What holds it is a monthly review of about an hour, a quarterly access review and re-scan, and exceptions that expire. All three are in [Keeping it where it is](#).

The state of the register and the map at the end of week 6.

Handover at a glance	Result
Findings in the register	47
Closed	42
Accepted in writing	3
Deferred with written acceptance	2
Critical findings: closed, accepted	9, 1
Scan checks passing, week one to week six	12 to 45 of 50
Security runbooks	5
SOC 2 map: controls in place on February 12	22 of 35
SOC 2 map: controls planned, and of those, after April 1	13, 2
First date a remaining finding is due	March 22, 2026 (C-4)

Handover at a glance	Result
Last date a remaining finding is due	May 20, 2026 (H-12)

The handover workshop

The workshop on February 12, 2026 is recorded, so a new engineer in a year can watch the part that is theirs. Kofi Brandvold, Sasha Ilyin, and Dev Raman attend. It covers the Foundation’s runbooks and this report’s; the part below is the security hour of it. Nothing is shown that its owner has not seen before, the live test uses a sample finding and never a real one, and every date in the remaining list is confirmed aloud by its owner, because a date nobody has said aloud is a hope.

The security part of the handover workshop: 60 minutes.

Time	Topic	Led by	What the room leaves with
0:00 to 0:10	The result, and what is now Tidepost’s	Dev Raman and Charles Sieg	The re-scan, the gate, and the one-page list of what Vantalect no longer touches
0:10 to 0:25	SR-1 to SR-3, with a live sample finding that becomes a page	Sasha Ilyin	Three runbooks each read aloud, and the time the page took
0:25 to 0:35	SR-4 and SR-5, and the alarms the guardrails raise (G-5 and G-6)	Kofi Brandvold	Who answers a root sign-in and a stopped trail
0:35 to 0:45	Identity: joiners, movers, leavers, and the quarterly access review	Sasha Ilyin	The first access review on the calendar
0:45 to 0:55	The evidence index and the SOC 2 technical map: what is in place, and what is Tidepost’s	Sasha Ilyin and Charles Sieg	The map, the evidence locations, and the two controls after the window opens
0:55 to 1:00	What remains, and the monthly review	Dev Raman	Every date confirmed aloud, and the first review on the calendar

The runbooks

There are 5. The first three are the ones the SOC 2 map names for the incident response row: a leaked credential, a public data store, and a compromised instance. Each has a trigger, an owner, and the first fifteen minutes of response. They live in the tidepost–foundation repository beside

the alarms that trigger them, so changing the alarm and changing the procedure happen in one pull request. Two rules apply to every one: **contain first and ask questions second**, and **never delete evidence**.

The runbooks, who owns each, and whom each pages. The pair on the phone is Sasha Ilyin first and Kofi Brandvold second, until the Well-Architected Review sets an on-call rotation.

ID	Runbook	Owner	Second	Pages	Tested
SR-1	A credential is leaked or misused	Sasha Ilyin	Kofi Brandvold	Page	Feb 12
SR-2	A bucket, snapshot, or database is public	Kofi Brandvold	Sasha Ilyin	Page for user data; business day otherwise	Feb 12
SR-3	An instance or a container is compromised	Kofi Brandvold	Sasha Ilyin	Page	Feb 12
SR-4	A root sign-in, a break-glass sign-in, or an IAM change nobody planned	Sasha Ilyin	Kofi Brandvold	Page	Feb 12
SR-5	A detection service stops, or an account drops out of it	Sasha Ilyin	Kofi Brandvold	Page	Feb 5

SR-1: A credential is leaked or misused

Owner: Sasha Ilyin. Second: Kofi Brandvold. Pages: Page. Tested February 12 on a sample finding in a scratch account.

It starts when:

- A GuardDuty finding about instance or user credentials used from outside AWS or from an unexpected place
- A secret-scanning alert, or a key or token found in a repository, a ticket, a chat, or a screenshot
- The video analytics vendor's key used outside its prefix or address range

Contain, in the first minutes.

1. Open a ticket named for the finding and the time, and post it in the security channel. Delete nothing.
2. An IAM user's access key: set it Inactive. Inactive, not deleted, so the key can still be shown to have been used.
3. A role session (an instance profile, a pipeline role, a permission set): add the revoke-older-sessions policy to the role.

4. An Identity Center user: disable the user in the identity provider, then delete the user's active sessions in IAM Identity Center.
5. A secret or API key: rotate it at the source, then in Secrets Manager.

Preserve. Export the principal's activity: `lookup-events` by access key or user name for the last 90 days, and Athena over the organization trail in `tp-log-archive` for anything older or any data event.

Scope.

- List every call that changes something (`Create*`, `Put*`, `Attach*`, `Delete*`, `RunInstances`, `GetSecretValue`, `AssumeRole`), the Regions, and the source addresses against the ones expected.
- Look for new users, access keys, roles, and trust policy edits, which are how an intruder keeps access.

Recover. Rotate every secret the principal could read, redeploy what reads it, and fix the cause: the repository, the laptop, or the integration. Reactivate nothing without the security lead's sign-off in the ticket.

Tell. If personal data may have been reached, tell counsel the same day. Whether to notify anyone is Tidepost's decision, made by Dev Raman with counsel.

BASH

```
aws iam update-access-key --user-name <user> --access-key-id <key-id> --status Inactive
aws iam put-role-policy --role-name <role> --policy-name AWSRevokeOlderSessions --policy-
document \
  '{"Version":"2012-10-17","Statement":[{"Effect":"Deny","Action":["*"],"Resource":
  ["*"],"Condition":{"DateLessThan":{"aws:TokenIssueTime":"<now-in-UTC>"}}}]}'
aws cloudtrail lookup-events --lookup-attributes AttributeKey=AccessKeyId,AttributeValue=<key-
id> --max-results 50
```

SR-2: A bucket, snapshot, or database is public

Owner: Kofi Brandvold. Second: Sasha Ilyin. Pages: Page for user data; business day otherwise. Tested February 12 on a sample finding in a scratch account.

It starts when:

- An Access Analyzer external-access finding
- A GuardDuty finding such as `Policy:S3/BucketAnonymousAccessGranted`
- A Security Hub failure of S3.2, S3.8, EC2.1, or RDS.2 on a resource that is not already an accepted exception

Contain, in the first minutes.

1. Block first, then look. A bucket: Block Public Access on the bucket. An EBS snapshot: remove the all group from its create-volume permission. An RDS snapshot: remove all from its restore attribute. A security group: revoke the rule that admits 0.0.0.0/0.

Preserve. Before changing anything, save the bucket policy and ACL (or the snapshot attributes, or the group's rules) into the ticket.

Scope.

- How long was it public? `get-resource-config-history` for the resource, then the trail for `PutBucketPolicy`, `PutBucketAcl`, and `DeletePublicAccessBlock`.
- Who read it? Object-level trail events exist only for the two buckets that hold user data. For any other resource exposure cannot be ruled out, and the ticket says so in those words, as C-3 did.

Recover. Find what made it public and fix that: a template, a person's console change, a script. Check that account-level Block Public Access (G-1) is still on.

Tell. If the resource held user data, tell counsel the same day.

BASH

```
aws s3api get-bucket-policy --bucket <bucket> > evidence-policy.json && aws s3api get-bucket-acl --bucket <bucket> > evidence-acl.json
aws s3api put-public-access-block --bucket <bucket> --public-access-block-configuration BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true
aws ec2 modify-snapshot-attribute --snapshot-id <snapshot-id> --attribute createVolumePermission --operation-type remove --group-names all
aws rds modify-db-snapshot-attribute --db-snapshot-identifier <snapshot-id> --attribute-name restore --values-to-remove all
aws ec2 revoke-security-group-ingress --group-id <sg-id> --protocol tcp --port <port> --cidr 0.0.0.0/0
aws configservice get-resource-config-history --resource-type AWS::S3::Bucket --resource-id <bucket>
```

SR-3: An instance or a container is compromised

Owner: Kofi Brandvold. Second: Sasha Ilyin. Pages: Page. Tested February 12 on a sample finding in a scratch account.

It starts when:

- A GuardDuty finding about command-and-control traffic, cryptocurrency mining, or a backdoor on an instance
- An EKS runtime-monitoring finding such as `Execution:Runtime/NewBinaryExecuted`

Contain, in the first minutes.

1. Do not terminate it. Replace the instance's security groups with the empty quarantine group. A rule change stops new connections; an established one can outlive it, so stop the instance after the snapshots finish if its owner agrees.
2. Revoke older sessions on the instance's role (SR-1), because its credentials may already be out.
3. A pod: cordon the node, apply a deny-all network policy to the pod's namespace, and leave the pod running.

Preserve. Snapshot every volume with a hold tag naming the ticket. Session Manager sessions are logged, so use it for any look inside.

Scope.

- Read the finding's details, then VPC flow logs for the instance (kept 90 days in tp-prod) and the trail for its role's calls. Check the other instances in the same group and subnet.

Recover. Replace from the image rather than cleaning in place. Rotate every secret the role could read. Terminate the original only after the snapshots complete and the security lead agrees in the ticket.

Tell. If the instance could reach user data, tell counsel the same day.

BASH

```
aws ec2 modify-instance-attribute --instance-id <instance-id> --groups <quarantine-sg-id>
aws ec2 create-snapshots --instance-specification InstanceId=<instance-id> --description 'SR-3
<ticket>' \
  --tag-specifications 'ResourceType=snapshot,Tags=[{Key=hold,Value=<ticket>}]'
kubectrl cordon <node-name>
```

SR-4: A root sign-in, a break-glass sign-in, or an IAM change nobody planned

Owner: Sasha Ilyin. Second: Kofi Brandvold. Pages: Page. Tested February 12 on a sample finding in a scratch account.

It starts when:

- The root sign-in alarm, or any `sts:AssumeRoot`
- The TidepostBreakGlass role assumed
- An IAM user, access key, or administrator policy created outside the pipeline

Contain, in the first minutes.

1. Match the event to a ticket. A break-glass use or a root task has a ticket written before it starts (the Foundation's RB-4); no ticket within 10 minutes means treat the principal that made the call as compromised and run SR-1 on it.

Preserve. Copy the matching trail events into the ticket.

Scope.

- For an unplanned IAM change, list what it created and who called it: CreateUser, CreateAccessKey, AttachUserPolicy, UpdateAssumeRolePolicy.

Recover. Revert from the repository or the trail, not by hand, and record the revert in the ticket.

Tell. A root sign-in nobody can explain is reported to the sponsor the same day.

BASH

```
aws cloudtrail lookup-events --lookup-attributes
AttributeKey=EventName,AttributeValue=AssumeRole --max-results 20
aws cloudtrail lookup-events --lookup-attributes
AttributeKey=EventName,AttributeValue=CreateAccessKey --max-results 20
```

SR-5: A detection service stops, or an account drops out of it

Owner: Sasha Ilyin. Second: Kofi Brandvold. Pages: Page. Tested February 5 by stopping logging on a scratch trail.

It starts when:

- StopLogging, DeleteTrail, DeleteDetector, DisableSecurityHub, Or StopConfigurationRecorder
- A member account missing from GuardDuty or Security Hub

Contain, in the first minutes.

1. Start the service again from its delegated administrator or the trail console, never by hand in the member account: start-logging for a trail; for GuardDuty and Security Hub, re-enroll the member from tp-audit.

Preserve. Record the exact start and end of the gap. The gap is itself evidence, and the auditor may ask for its dates.

Scope.

- Who called it? The organization policy set denies these calls to everyone but the Control Tower execution role and the break-glass role from February 5, so a call that succeeded after that day means one of those two acted, or a policy is not attached where it should be.

Recover. Find out why it was stopped. If the caller is unknown, run SR-1 on it.

Tell. Tell the sponsor if the gap exceeded an hour.

BASH

```
aws cloudtrail start-logging --name <trail-name>
aws guardduty list-members --detector-id <detector-id> --only-associated=false --query
'Members[?RelationshipStatus!=`Enabled`]'
```

What the runbooks cannot do

They cannot reach what was never logged. Object-level events exist for the two buckets that hold user data and nowhere else, and flow logs are kept 90 days in `tp-prod`, so for an older or less watched resource the honest answer in the ticket is "exposure cannot be ruled out." A runbook that says so in those words is working.

The evidence index

The auditor tests controls by asking for evidence, and the question is always the same: where is it, what does it show, and how far back does it go? This index answers the first two for each control in the map. For the third, the organization trail and the Config history are in `tp-log-archive` and are kept 400 days, so evidence from the first day of the observation window, April 1, stays available through May 6, 2027. The map in [The SOC 2 technical map, as of February 12, 2026](#) lists the same controls by criterion; this index lists them by where the evidence lives.

tp-audit

Delegated GuardDuty, Security Hub, IAM Access Analyzer, the Config aggregator, and Inspector.

Evidence held in tp-audit.

Evidence	Criteria	Operating from	Owner	On February 12
Inspector and GuardDuty findings in tp-audit	CC6.8	Jan 29	Sasha Ilyin	In place
Config history and the aggregator in tp-audit	CC7.1	Jan 29	Sasha Ilyin	In place
Security Hub and GuardDuty in tp-audit	CC7.2	Jan 29	Sasha Ilyin	In place

tp-backup

The central backup vault (vault lock in compliance mode) and delegated AWS Backup.

Evidence held in tp-backup.

Evidence	Criteria	Operating from	Owner	On February 12
AWS Backup job history in tp-backup	A1.2	Feb 10	Kofi Brandvold	In place
The restore test record and timings	A1.3	Mar 24	Kofi Brandvold	Planned

tp-log-archive

The organization trail and AWS Config history.

Evidence held in tp-log-archive.

Evidence	Criteria	Operating from	Owner	On February 12
The organization trail in tp-log-archive	CC7.1	Jan 28	Sasha Ilyin	In place
IAM credential reports and root-task records in the organization trail	CC6.1	Jan 29	Sasha Ilyin	In place

tp-management

Payer, Control Tower, IAM Identity Center, and the Cost and Usage Report data export.

Evidence held in tp-management.

Evidence	Criteria	Operating from	Owner	On February 12
Identity Center assignments and sign-in events	CC6.2	Jan 28	Sasha Ilyin	In place
Service control policy attachments and the exception signed February 11	CC6.2	Feb 5	Sasha Ilyin	In place
Resource control policy attachments	CC6.7	Feb 5	Kofi Brandvold	In place
Tag policy compliance and the standard	C1.1	Mar 20	Sasha Ilyin	Planned

tp-prod

The founders' account, joined and enrolled: production, and until June the old staging.

Evidence held in tp-prod.

Evidence	Criteria	Operating from	Owner	On February 12
The account trail's PutPublicAccessBlock and PutBucketPolicy calls for January 6 to 28, then Config history for the S3 public-access rules	CC6.6	Jan 6	Kofi Brandvold	In place
Security group history and the written acceptance of January 16	CC6.6	Jan 7	Kofi Brandvold	In place
IAM policy versions and Access Analyzer findings	CC6.3	Jan 8	Marcus Oyelaran	In place
Secrets Manager inventory and the repository secret-scan results	CC6.1	Jan 9	Marcus Oyelaran	In place
Session Manager logs and security group history	CC6.6	Jan 20	Kofi Brandvold	In place
CloudWatch alarm history and flow logs	CC7.2	Jan 20	Kofi Brandvold	In place
The account trail's OpenSearch configuration calls, then Config history for the domain	CC6.6	Jan 21	Marcus Oyelaran	In place
The account trail's ElastiCache calls, then Config history for the replication group	CC6.6	Jan 27	Marcus Oyelaran	In place

Evidence	Criteria	Operating from	Owner	On February 12
EKS access entries and cluster configuration history	CC6.3	Jan 30	Kofi Brandvold	In place
S3 bucket policies and CloudFront distribution configuration	CC6.7	Jan 30	Kofi Brandvold	In place
WAF logs and web ACL associations	CC6.6	Feb 4	Marcus Oyelaran	In place
IAM role policies and Config history	CC6.3	Feb 9	Amara Delacroix	In place
The runbooks and the evidence index handed over February 12	CC7.3	Feb 12	Sasha Ilyin	In place
CloudWatch alarm history and the Service Quotas request history	A1.1	Mar 13	Kofi Brandvold	Planned
Auto Scaling activity, Karpenter events, and CloudWatch capacity metrics	A1.1	Mar 17	Kofi Brandvold	Planned
CloudWatch alarm history	CC7.2	Mar 20	Kofi Brandvold	Planned
RDS configuration and the March 22 cutover record	CC6.6, A1.2	Mar 22	Kofi Brandvold	Planned
The drill record and service dashboards	A1.3	Mar 25	Kofi Brandvold	Planned
The on-call schedule and the tabletop record	CC7.4	Mar 26	Kofi Brandvold	Planned
The tabletop record and the review template	CC7.5	Mar 26	Kofi Brandvold	Planned
Pull requests, pipeline runs, and CloudFormation drift reports	CC8.1	Mar 27	Kofi Brandvold	Planned
The signed schedule	C1.2	May 20	Amara Delacroix	Planned
Pipeline job history and a sampled deletion check	C1.2	May 20	Marcus Oyelaran	Planned

Evidence that is not an AWS control

Supporting evidence: scans, the register, reviews, and the change record.

Evidence	Where	From	Owner	Status
The Audit's scans: the week-one scan and the week-six re-scan, 50 checks each, check by check	The security reports security-1-scan and security-7-rescan	Feb 12	Sasha Ilyin	In place
The findings register, with every step, owner, and signed acceptance	security-2-audit and the findings register file delivered with it	Feb 12	Sasha Ilyin	In place
The quarterly access review: the Identity Center assignment export compared with the HR roster	The access review folder, kept by the security lead	Mar 31	Sasha Ilyin	Planned
Runbook test records and the alert route test times	The security reports security-6-detection-response and security-8-runbooks-handover	Feb 12	Sasha Ilyin	In place
Pull requests and pipeline runs for every production change	Pull requests, pipeline runs, and CloudFormation drift reports	Mar 27	Kofi Brandvold	Planned

The SOC 2 technical map, as of February 12, 2026

What this map is

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.

For each criterion in scope, the table gives the AWS control, the date it began operating or will, where its evidence is, and who owns it. "In place" means operating on February 12; "Planned" carries the date it begins. The criteria cover Security, Availability, and Confidentiality, tested over a window from April 1 to September 30.

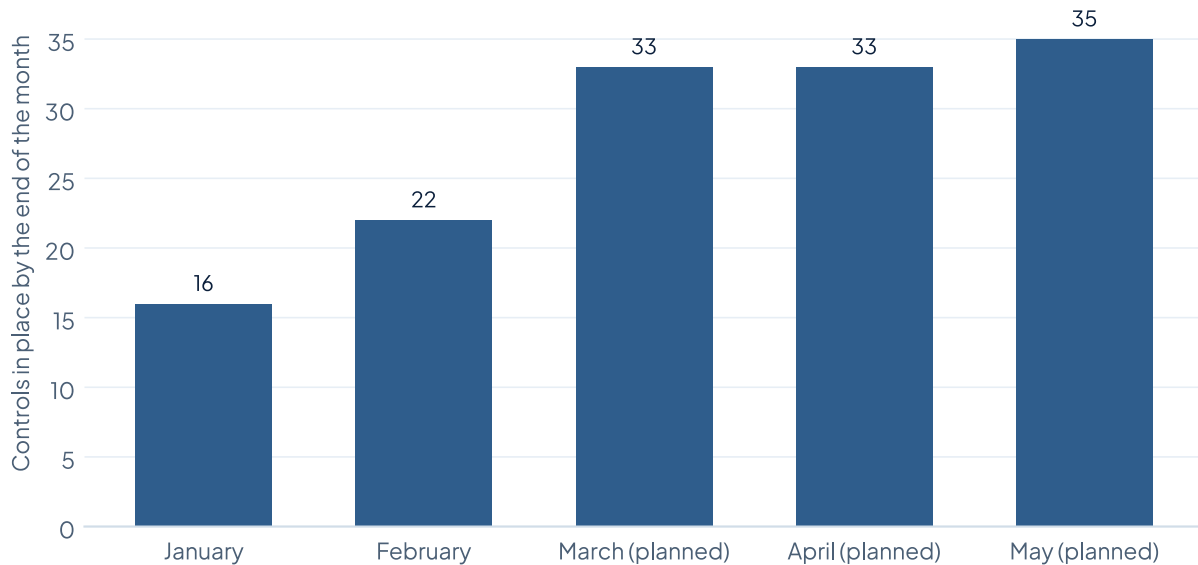
35 controls: 22 in place and 13 planned on February 12. The planned ones belong to the Foundation and the Well-Architected Review, and to Tidepost for C1.2.

Criterion	Control	Operating from	On February 12	Evidence is in	Owner
CC6.1	Database and third-party credentials in Secrets Manager, read at runtime; none in code or launch template user data	Jan 9	In place	tp-prod	Marcus Oyelaran
CC6.1	Root user holds no access keys, and root credentials are removed from member accounts under centralized root access	Jan 29	In place	tp-log-archive	Sasha Ilyin
CC6.2	People sign in through IAM Identity Center permission sets with MFA required; departed people removed	Jan 28	In place	tp-management	Sasha Ilyin
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	Feb 5	In place	tp-management	Sasha Ilyin
CC6.3	Link-preview service role cut to 14 actions; IMDSv2 required	Jan 8	In place	tp-prod	Marcus Oyelaran

Criterion	Control	Operating from	On February 12	Evidence is in	Owner
CC6.3	EKS endpoints private, and developers on namespace-scoped access entries instead of cluster administrator	Jan 30	In place	tp-prod	Kofi Brandvold
CC6.3	One execution role per moderation function, each limited to its own buckets and endpoints	Feb 9	In place	tp-prod	Amara Delacroix
CC6.6	Block Public Access on the account and every bucket; CloudFront origin access control in front of the media bucket	Jan 6	In place	tp-prod	Kofi Brandvold
CC6.6	RDS reachable only from the BI vendor's four published ranges, with TLS required, until the new private instance replaces it	Jan 7	In place	tp-prod	Kofi Brandvold
CC6.6	OpenSearch inside the VPC with fine-grained access control	Jan 21	In place	tp-prod	Marcus Oyelaran
CC6.6	Redis with in-transit encryption and an AUTH token from Secrets Manager	Jan 27	In place	tp-prod	Marcus Oyelaran
CC6.6	No inbound SSH; shell access through Session Manager with session logs	Jan 20	In place	tp-prod	Kofi Brandvold
CC6.6	AWS WAF on both public load balancers, with managed rule groups and a rate limit	Feb 4	In place	tp-prod	Marcus Oyelaran
CC6.6	Production database private (PubliclyAccessible false) in the new encrypted PostgreSQL 16 instance	Mar 22	Planned	tp-prod	Kofi Brandvold
CC6.7	TLS required in transit: TLS-only bucket statements and a CloudFront minimum of TLS 1.2	Jan 30	In place	tp-prod	Kofi Brandvold
CC6.7	Organization data perimeter (resource control policies for S3, KMS, and STS) that admits the CloudFront origin access control	Feb 5	In place	tp-management	Kofi Brandvold

Criterion	Control	Operating from	On February 12	Evidence is in	Owner
CC6.8	Inspector on EC2 and ECR, and GuardDuty runtime monitoring on EKS, delegated to tp-audit	Jan 29	In place	tp-audit	Sasha Ilyin
CC7.1	Organization trail, multi-Region, into tp-log-archive	Jan 28	In place	tp-log-archive	Sasha Ilyin
CC7.1	AWS Config recording in every governed account, with the aggregator in tp-audit	Jan 29	In place	tp-audit	Sasha Ilyin
CC7.2	GuardDuty and Security Hub findings reviewed from tp-audit	Jan 29	In place	tp-audit	Sasha Ilyin
CC7.2	Alarms on root sign-in, unauthorized API calls, and IAM changes, over VPC flow logs and the trail	Jan 20	In place	tp-prod	Kofi Brandvold
CC7.2	Alarms on the service-level objectives for the API and the ranking endpoint	Mar 20	Planned	tp-prod	Kofi Brandvold
CC7.3	Security runbooks for a leaked credential, a public bucket, and a compromised instance	Feb 12	In place	tp-prod	Sasha Ilyin
CC7.4	On-call rotation and the incident process, exercised in a tabletop	Mar 26	Planned	tp-prod	Kofi Brandvold
CC7.5	Post-incident review step in the incident process	Mar 26	Planned	tp-prod	Kofi Brandvold
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	Mar 27	Planned	tp-prod	Kofi Brandvold
A1.1	Service quota alarms at 80% for Rekognition, SageMaker, and EC2 vCPUs, with the limits raised to leave headroom for a zone failover	Mar 13	Planned	tp-prod	Kofi Brandvold
A1.1	Capacity follows demand: target tracking on the API tier, Karpenter on EKS, and queue-depth scaling for the transcoders	Mar 17	Planned	tp-prod	Kofi Brandvold

Criterion	Control	Operating from	On February 12	Evidence is in	Owner
A1.2	AWS Backup plan with a locked vault in tp-backup and cross-Region copies to us-west-2	Feb 10	In place	tp-backup	Kofi Brandvold
A1.2	Production database in a Multi-AZ instance	Mar 22	Planned	tp-prod	Kofi Brandvold
A1.3	Restore test from the central vault	Mar 24	Planned	tp-backup	Kofi Brandvold
A1.3	Availability Zone failure drill	Mar 25	Planned	tp-prod	Kofi Brandvold
C1.1	Data-class standard, with a data-class tag on every data store	Mar 20	Planned	tp-management	Sasha Ilyin
C1.2	Retention schedule for user content, written with counsel	May 20 (after the window opens)	Planned	tp-prod	Amara Delacroix
C1.2	Deletion pipeline for removed posts' media, across originals, renditions, and backups	May 20 (after the window opens)	Planned	tp-prod	Marcus Oyelaran



Controls in place by the end of each month, counting the planned ones in the months marked planned. The observation window opens on April 1; nothing begins in April, and the last 2 begin in May.

The controls that begin after the window opens

After April 1

The C1.2 disposal controls, the retention schedule and the deletion pipeline, are planned to begin operating on May 20, 2026, after the observation window opens on April 1, 2026. They wait on counsel and on the app team (H-12, deferred with written acceptance). The auditor decides what that means for the report.

The two controls, both C1.2:

- Retention schedule for user content, written with counsel, operating from May 20, evidence in tp-prod, owned by Amara Delacroix.
- Deletion pipeline for removed posts' media, across originals, renditions, and backups, operating from May 20, evidence in tp-prod, owned by Marcus Oyelaran.

Both wait on the same dependency, which is not an AWS one: counsel's schedule and the app team's work on H-12, which Tidepost deferred with a written acceptance. The map shows the date, and nothing here predicts what follows from it.

What is Tidepost's

No Vantalect engagement touches these. They are Tidepost's, they are part of what the auditor tests, and they are not in the map.

What no Vantalect engagement touches.

Area	What it is	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.

What remains

Every finding that is not closed has a named signer, a reason in writing, and a date. They do not count as closed until the date; the gate counts C-4 because a named signer accepted it with a closing date.

The findings still open at the handover, with the date each closes or is reviewed. Nothing here is overdue.

ID	Severity	Finding	Status	Signed by	Signed	Closes or is reviewed	Owner
C-4	Critical	RDS PostgreSQL publicly accessible from 0.0.0.0/0	Accepted in writing	Dev Raman	Jan 16	Mar 22, through the Well-Architected work	Kofi Brandvold
H-1	High	RDS and EBS volumes unencrypted at rest	Deferred with written acceptance	Dev Raman	Jan 16	Mar 22, through the Well-Architected work	Kofi Brandvold
H-12	High	No deletion pipeline for removed posts' media	Deferred with written acceptance	Sasha Ilyin	Jan 16	May 20, on Tidepost's calendar	Marcus Oyelaran
M-7	Medium	Server access logging off on 7 buckets	Accepted in writing	Sasha Ilyin	Jan 21	reviewed Jun 30	Kofi Brandvold
L-4	Low	Bucket names disclose internal project names	Accepted in writing	Sasha Ilyin	Jan 21	reviewed Jun 30	Kofi Brandvold

- **C-4, Dev Raman's reason.** 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, Dev Raman's reason.** The production database cannot be encrypted in place; the new encrypted PostgreSQL 16 instance replaces it at the March 22 cutover.
- **H-12, Sasha Ilyin's reason.** 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, Sasha Ilyin's reason.** 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, Sasha Ilyin's reason.** S3 bucket names cannot be changed in place, and the names disclose nothing that is not already in public contracts.

Declined

A decline is a decision not to do something, recorded so nobody re-opens it by accident.

The 3 decisions not to do something.

ID	Declined	Decided	By	Why
D-1	Amazon Macie across the media buckets	Jan 16	Sasha Ilyin	Considered, not priced: nearly all of the media is public news by design and the two buckets that hold user data are small. Macie runs on no bucket in this sample.
D-2	A history rewrite of the repository that held the C-8 secrets	Jan 9	Sasha Ilyin	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.
D-3	VPC Block Public Access	Feb 5	Kofi Brandvold	It would block the public load balancers unless every one is listed as an exclusion; deferred to the Foundation's operations runbooks.

Checks that still fail, by decision

At the re-scan, 5 of the 50 checks still fail, each by one of the decisions above. This is the list a reviewer should expect to see, and the only one.

The checks that still fail at week six.

Check	Severity	FailingDisposition resources
S3. 9 S3 buckets should have server access logging enabled	Medium	7Accepted in writing
RDS. 2 RDS DB instances should prohibit public access	Critical	1Accepted in writing
RDS. 3 RDS DB instances should have encryption at rest enabled	Medium	1Deferred with written acceptance
EC2. 172 EC2 VPC Block Public Access settings should block internet gateway traffic	Medium	18Declined
Macie. 1 Amazon Macie should be enabled	Medium	18Declined

Keeping it where it is

The monthly review

An hour, once a month, chaired by Sasha Ilyin, with Kofi Brandvold. The first is on March 10, 2026. The agenda is the same every month so it can be done on a bad day.

The monthly review agenda.

What to read	Who	Where it is
The Security Hub score and every control that failed this month	Sasha Ilyin	Security Hub in tp-audit
The detection services that are off, and the newer Security Hub: turn each on, or write down why not	Sasha Ilyin	The cost estimates in security-6-detection-response
Access Analyzer findings still active, each with an owner or an archive reason	Sasha Ilyin	Access Analyzer in tp-audit
Guardrail alarms that fired (G-1 to G-9) and what each turned out to be	Kofi Brandvold	The platform channel history
Exceptions and acceptances nearing their dates	Sasha Ilyin	The acceptance log in the findings register
Any new account since last month, checked against the new-account baseline	Kofi Brandvold	The account map in tidepost-foundation
One runbook read aloud, rotating through SR-1 to SR-5	The runbook's owner	The runbook and the ticket from the last real use

What recurs

The routine that keeps the score where it is. The access review comes first so its evidence exists before the observation window opens.

What	How often	First	Owner
Monthly review	Monthly	Mar 10	Sasha Ilyin
Access review: the assignment export against the HR roster	Quarterly and at each leaver	Mar 31	Sasha Ilyin
Re-scan: the same 50 checks, run the same way	Quarterly	May 12	Sasha Ilyin
Alert route test: a sample finding from each source	Quarterly	With the first re-scan	Sasha Ilyin
Break-glass test (the Foundation's RB-4)	Quarterly	With the first re-scan	Kofi Brandvold

The guardrails Tidepost now owns

The 9 workload guardrails from security-4-criticals-guardrails stay running, and the organization's 11 policies (foundation-6-guardrails-vending) sit above them. The monthly review reads which of them fired.

The workload guardrails Tidepost owns.

ID	Guardrail	Keeps closed	Runs it
G-1	Account-level S3 Block Public Access	C-2, C-3, H-5	Kofi Brandvold
G-2	Media originals reachable only through CloudFront	C-2	Kofi Brandvold
G-3	Secret scanning with push protection	C-8	Marcus Oyelaran
G-4	Open SSH and RDP closed automatically	H-4, C-10	Kofi Brandvold
G-5	Alarms on root, unauthorized calls, IAM changes, and the trail	C-1, C-7, C-9	Kofi Brandvold
G-6	Alarm on any change to the database's security group	C-4	Kofi Brandvold
G-7	EBS encryption by default	H-1	Kofi Brandvold
G-8	IMDSv2 required by default	C-6, H-2	Kofi Brandvold
G-9	Link-preview egress through an allowlisted proxy	C-6	Marcus Oyelaran

The new-account baseline

A new account is the easiest way to lose the score. Accounts are vended through Account Factory, and these are the 5 things true of every one:

The new-account baseline.

What must be true	Who or what does it	How to check
Placed in an OU and enrolled in the landing zone	Account Factory (the Foundation's RB-1)	The account appears in the account map
Organization policies attach by OU, including IMDSv2 by default and no public snapshot sharing	The OU's policy set	<code>list-policies-for-target</code> on the account
GuardDuty, Security Hub, Inspector, Config, and Access Analyzer enroll on their own	Auto-enable from <code>tp-audit</code>	The member appears in each service's member list
People reach it through permission sets, never IAM users	Identity Center assignment and the <code>no-IAM-users</code> policy	The assignment export
Account-level Block Public Access and EBS encryption by default	A step on the vending ticket, done by the platform lead: no organization policy in this set does it	<code>get-public-access-block</code> and <code>get-ebs-encryption-by-default</code> in the new account

Vantalect's access ends

Vantalect's read-only audit access, the role with the `SecurityAudit` and `ViewOnlyAccess` policies it used for every scan, is removed on February 13, 2026, with the Foundation's operator role. Vantalect holds no write access to any member account. On that day Kofi Brandvold confirms in the organization trail that nothing has assumed either role since the removal.

What Tidepost keeps

The 9 security reports, in the order they were written, and the register that sits behind them.

The security reports. The findings register file is delivered with security-2-audit.

Report	Title	Dated
security-1-scan	Week-One Scan, Including the Foundation Checks	Jan 9
security-2-audit	Findings Register, Governance Review, Target Organization, and the SOC 2 Technical Map	Jan 15
security-2-appendix	Audit Appendix: Evidence by Finding	Jan 15
security-3-readout	Audit Sponsor Readout	Jan 16
security-4-criticals-guardrails	Criticals Closed and Workload Guardrails	Jan 23
security-5-identity	Identity: People in Identity Center, Workloads on Roles	Jan 30
security-6-detection-response	Detection and Response from the Audit Account	Feb 6
security-7-rescan	Week-Six Re-Scan	Feb 12
security-8-runbooks-handover	Runbooks, the Evidence Index, and Handover	Feb 12

© 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.