

AWS SECURITY, COMPLIANCE & GOVERNANCE · SAMPLE DELIVERABLE

Week-Six Re-Scan

Week 6 of 6: Re-scan · 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
How the re-scan was run	4
Score before and after	5
By standard	5
By severity	6
The checks that still fail	6
Every critical, with its closure evidence	7
C-1: Root user with two active access keys and no MFA	8
C-2: tp-media-originals public-read, and location metadata on 61% of images	8
C-3: tp-exports public with listing on: 104,318 user records	8
C-4: RDS PostgreSQL publicly accessible from 0.0.0.0/0	9
C-5: OpenSearch domain with a public endpoint and an open access policy	9
C-6: Link-preview SSRF reaches IMDSv1 and an instance role with AdministratorAccess	9
C-7: Seven IAM users with administrator access and long-lived keys, two of them departed	9
C-8: Database password and a third-party API key in the repository and in launch template user data	10
C-9: No CloudTrail trail	10
C-10: A forgotten g5.12xlarge with SSH open and a Jupyter server without a token	11
The critical accepted in writing	11
The other findings accepted or deferred	12
What we declined	13
What the Foundation closed	13
The SOC 2 technical map, after	14
The gate, and what follows	16
What follows	16

Summary

The gate is met. Every one of the 10 critical findings agreed at the January 16, 2026 readout is closed or accepted in writing: 9 closed and verified by this re-scan, and 1 (C-4) accepted by Dev Raman on January 16, 2026 until the March 22, 2026 cutover. The second invoice is issued on February 13, 2026.

We ran the same scan as week one, the same way: the same 50 checks from the same two standards, in the same 2 Regions, with the same read-only collector. **The score rose from 24.0% (12 of 50 checks) to 90.0% (45 of 50), and the failed resources fell from 207 to 45.** The account count did not stay the same: 1 account on January 5, 2026, 9 on February 12, 2026, because the organization now exists.

Of the 47 findings in the register, **42 are closed, 3 are accepted in writing, and 2 are deferred with written acceptance.** Tidepost’s engineers closed 5 on notice, the Hardening closed 34, and the Foundation add-on closed 3, the three that only an organization can finish.

The week-one scan and the week-six re-scan, side by side.

Week six at a glance	Week one	Week six
Checks passing, of 50	12	45
Pass rate	24.0%	90.0%
Checks failing	38	5
Failed resources	207	45
Accounts scanned	1	9
Critical checks passing, of 10	3	9
High checks passing, of 13	1	13
Critical findings closed or accepted, of 10	0	10

The gate

The second half of the Hardening's \$29,750 fee, \$14,875, is invoiced only when this holds: Every critical finding agreed at the January 16 readout is closed, verified by the week-six re-scan, or accepted in writing by a named Tidepost signer with a closing date. It holds. The gate was decided on February 12, 2026. Beyond the gate, no particular outcome is promised: the Hardening reduces risk, and it is not a SOC 2 report, a certification, or a penetration test.

How the re-scan was run

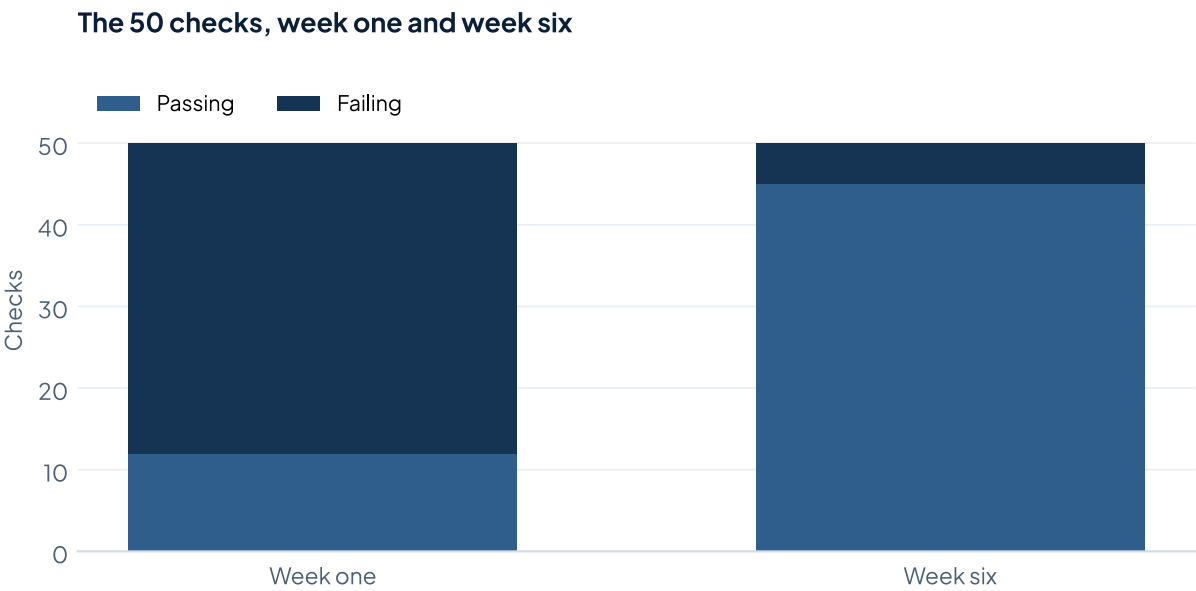
The re-scan is the week-one scan repeated: the same collector, the same 50 checks, the same two standards, and the same us-east-1 and us-west-2. Four things decide whether the comparison is honest.

- **Nothing was suppressed.** No check was dropped, no threshold changed, and no resource was excluded. The two declines still fail their checks and are counted as failures below.
- **The account count changed, and so did the way two checks count.** An account-level check counts the account in each Region. At week one that was 1 account in 2 Regions; at week six it is 9 accounts in 2 Regions, so a setting that is off in every account fails 18 times instead of 2. EC2.172 and Macie.1 are the two, and they are declines, not regressions.
- **The root user's MFA checks read each account's credential report.** IAM.6 and IAM.9 look at the root row: a member account whose root credentials were removed under centralized root access has no password, key, or MFA device, and the scan counts it as passing both, because there is nothing left to sign in with. The management account's root user keeps its password and two hardware keys and passes on those. The scan applies this rule itself instead of taking Security Hub's finding for those accounts, so anyone can repeat the count from the 9 credential reports.
- **The one IAM user left passes IAM.3 on a fresh key.** The video analytics vendor's user, kept under the written exception for MAF-05, had its key rotated on February 11, when the exception was signed, so the key is 1 day old at the re-scan. The next rotation is due May 12, 90 days later; a missed rotation fails IAM.3 on the first re-scan after it.
- **A finding meets the gate when it is closed, or when it is accepted in writing.** It is closed only when its changes are in and none of its original failed checks still fails. We did not accept an owner's word.

- **The score is a count of checks, not of risk**, and of 50, not of every control the standards define. A check passes when no resource fails it, so one failing resource fails the check.

AWS Security Hub CSPM is now on, administered from `tp-audit`, and `SecurityHub.1` and `GuardDuty.1` pass because the services are on. The collector still evaluates the same documented conditions it did at week one, so the comparison holds.

Score before and after



The 50 checks, passing and failing, at week one and week six.

By standard

The score by standard. A check in both standards is counted once in the last row.

Standard	Checks	Passing at week one	Passing at week six
CIS AWS Foundations Benchmark v5.0.0	27	4	24
AWS Foundational Security Best Practices v1.0.0	50	12	45
All checks, each counted once	50	12	45

By severity

Checks and failed resources by severity.

Severity	Checks	Passing at week one	Passing at week six	Failed resources, week one	Failed resources, week six
Critical	10	3	9	12	1
High	13	1	13	97	0
Medium	24	7	20	81	44
Low	3	1	3	17	0
Total	50	12	45	207	45

The checks that still fail

5 checks fail at week six. Every one is a decision recorded in writing, not an open defect.

The checks that fail at week six. The total is the week-six failed resources.

Control	Check	Severity	FailedWhy it still fails resources
S3.9	S3 buckets should have server access logging enabled	Medium	7M-7, accepted in writing
RDS.2	RDS DB instances should prohibit public access	Critical	1C-4, accepted in writing
RDS.3	RDS DB instances should have encryption at rest enabled	Medium	1H-1, deferred with written acceptance
EC2.172	EC2 VPC Block Public Access settings should block internet gateway traffic	Medium	18Declined (D-3, February 5)
Macie.1	Amazon Macie should be enabled	Medium	18Declined (D-1, January 16)
			45Total failed resources

Every critical, with its closure evidence

The 10 critical findings, how each closed, and the failed resources on its checks at week one and week six.

ID	Finding	Status	Closed through	Checks, week one to week six
C-1	Root user with two active access keys and no MFA	Closed January 29	Foundation	IAM.4 2 to 0; IAM.6 1 to 0; IAM.9 1 to 0
C-2	tp-media-originals public-read, and location metadata on 61% of images	Closed January 14	Hardening	S3.2 2 to 0; S3.8 17 to 0
C-3	tp-exports public with listing on: 104,318 user records	Closed January 6	Tidepost on notice	S3.2 2 to 0
C-4	RDS PostgreSQL publicly accessible from 0.0.0.0/0	Accepted in writing January 16	Accepted in writing	RDS.2 2 to 1
C-5	OpenSearch domain with a public endpoint and an open access policy	Closed January 21	Hardening	Opensearch.2 1 to 0
C-6	Link-preview SSRF reaches IMDSv1 and an instance role with AdministratorAccess	Closed January 8	Hardening	IAM.1 4 to 0
C-7	Seven IAM users with administrator access and long-lived keys, two of them departed	Closed February 10	Foundation	IAM.1 4 to 0; IAM.2 16 to 0
C-8	Database password and a third-party API key in the repository and in launch template user data	Closed January 9	Hardening	No check covers it
C-9	No CloudTrail trail	Closed January 28	Foundation	CloudTrail.1 1 to 0; CloudTrail.2 1 to 0; CloudTrail.4 1 to 0
C-10	A forgotten g5.12xlarge with SSH open and a Jupyter server without a token	Closed January 6	Tidepost on notice	EC2.13 6 to 0; EC2.19 3 to 0

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

Closed January 29. Closed through Foundation. **Owner:** Kofi Brandvold. **SOC 2:** CC6.1.

- January 6, Tidepost on notice: Both root access keys deleted after the pipeline and the script moved to roles; two FIDO2 keys registered
- 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

Re-scan evidence. IAM. 4 (IAM root user access key should not exist): 2 failed resources at week one, passing at week six. IAM. 6 (Hardware MFA should be enabled for the root user): 1 failed resource at week one, passing at week six. IAM. 9 (MFA should be enabled for the root user): 1 failed resource at week one, passing at week six. Evidence for the auditor is in: IAM credential reports and root-task records in the organization trail.

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

Closed January 14. Closed through Hardening. **Owner:** Amara Delacroix. **SOC 2:** CC6.6.

- 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
- January 14, Hardening: Location metadata stripped from 9,800,000 image originals by an S3 Batch Operations job that ran January 7 to 14

Re-scan evidence. S3. 2 (S3 buckets should prohibit public read access): 2 failed resources at week one, passing at week six. S3. 8 (S3 buckets should have block public access settings enabled): 17 failed resources at week one, passing at week six. Evidence for the auditor is in: The account trail's PutPublicAccessBlock and PutBucketPolicy calls for January 6 to 28, then Config history for the S3 public-access rules.

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

Closed January 6. Closed through Tidepost on notice. **Owner:** Lior Haddad.

- 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)

Re-scan evidence. S3. 2 (S3 buckets should prohibit public read access): 2 failed resources at week one, passing at week six.

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

Accepted in writing January 16. Owner: Kofi Brandvold. **SOC 2:** CC6.6.

- 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

Re-scan evidence. RDS. 2 (RDS DB instances should prohibit public access): 2 failed resources at week one, 1 at week six (accepted in writing). Evidence for the auditor is in: Security group history and the written acceptance of January 16.

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

Closed January 21. Closed through Hardening. **Owner:** Marcus Oyelaran. **SOC 2:** CC6.6.

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

Re-scan evidence. opensearch. 2 (OpenSearch domains should not be publicly accessible): 1 failed resource at week one, passing at week six. Evidence for the auditor is in: The account trail's OpenSearch configuration calls, then Config history for the domain.

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

Closed January 8. Closed through Hardening. **Owner:** Marcus Oyelaran. **SOC 2:** CC6.3.

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

Re-scan evidence. IAM. 1 (IAM policies should not allow full '*' administrative privileges): 4 failed resources at week one, passing at week six. Evidence for the auditor is in: IAM policy versions and Access Analyzer findings.

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

Closed February 10. Closed through Foundation. **Owner:** Sasha Ilyin. **SOC 2:** CC6.2.

- January 6, Tidepost on notice: The two departed users' passwords and keys deleted, and the users with them
- January 26, Hardening: The 14 current staff provisioned into IAM Identity Center over SCIM, by group (Identity Center connected January 23)

- 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
- February 10, Foundation: The five IAM users deleted after the policy set that denies new IAM users and keys reached Prod on February 5

Re-scan evidence. IAM.1 (IAM policies should not allow full '*' administrative privileges): 4 failed resources at week one, passing at week six. IAM.2 (IAM users should not have IAM policies attached): 16 failed resources at week one, passing at week six. Evidence for the auditor is in: Identity Center assignments and sign-in events.

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

Closed January 9. Closed through Hardening. **Owner:** Marcus Oyelaran. **SOC 2:** CC6.1.

- 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

Re-scan evidence. No scan control covers this finding. Evidence for the auditor is in: Secrets Manager inventory and the repository secret-scan results.

C-9: No CloudTrail trail

Closed January 28. Closed through Foundation. **Owner:** Sasha Ilyin. **SOC 2:** CC7.1.

- January 6, Hardening: An account trail created, multi-Region, writing to a locked bucket
- January 28, Foundation: Replaced by the organization trail into tp-log-archive when the account joined

Re-scan evidence. CloudTrail.1 (CloudTrail should be enabled and configured with at least one multi-Region trail): 1 failed resource at week one, passing at week six. CloudTrail.2 (CloudTrail should have encryption at rest enabled): 1 failed resource at week one, passing at week six. CloudTrail.4 (CloudTrail log file validation should be enabled): 1 failed resource at week one, passing at week six. Evidence for the auditor is in: The organization trail in tp-log-archive.

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

Closed January 6. Closed through Tidepost on notice. **Owner:** Yuki Sorensen.

- 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

Re-scan evidence. EC2.13 (Security groups should not allow ingress from 0.0.0.0/0 to port 22): 6 failed resources at week one, passing at week six. EC2.19 (Security groups should not allow unrestricted access to high-risk ports): 3 failed resources at week one, passing at week six.

The critical accepted in writing

Risk acceptance for C-4

RDS PostgreSQL publicly accessible from 0.0.0.0/0. Dev Raman accepted it in writing on January 16, 2026: 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. The acceptance ends on March 22, 2026, the cutover that the Well-Architected Review performs; it does not extend itself, and the gate does not pass on it after that date.

It meets the gate as accepted in writing, and it stays on the register and on the SOC 2 map as an open item. The check that tests it, RDS.2, still fails on 1 resource, the production writer; the other instance that failed at week one now passes. Until the cutover the database admits only the BI vendor's four published address ranges and requires TLS. Kofi Brandvold owns the finding, and Sasha Ilyin holds the acceptance.

The other findings accepted or deferred

The 5 findings that are not closed, with who signed each and when each ends or is reviewed.

ID	Severity	Status	Signed by	Runs to	Owner	Why
C-4	Critical	Accepted in writing January 16	Dev Raman	March 22 (Well-Architected Review)	Kofi Brandvold	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	Deferred in writing January 16	Dev Raman	March 22 (Well-Architected Review)	Kofi Brandvold	The production database cannot be encrypted in place; the new encrypted PostgreSQL 16 instance replaces it at the March 22 cutover
H-12	High	Deferred in writing January 16	Sasha Ilyin	May 20 (Tidepost)	Marcus Oyelaran	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	Accepted in writing January 21	Sasha Ilyin	Reviewed June 30	Kofi Brandvold	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	Accepted in writing January 21	Sasha Ilyin	Reviewed June 30	Kofi Brandvold	S3 bucket names cannot be changed in place, and the names disclose nothing that is not already in public contracts

What we declined

Three things we considered and did not do. Each is a decision, with a date and a name.

ID	What	Decided	By	Why
D-1	Amazon Macie across the media buckets	January 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	January 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	February 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.

What the Foundation closed

The Foundation add-on closed 3 of the critical findings, and they are counted here, once, in the Audit's gate. Each needed an organization.

The critical findings the Foundation finished.

ID	Closed	Why only an organization can close it
C-1	January 29	Centralized root access removes root credentials from member accounts, which only an organization can do.
C-7	February 10	The permission sets live in IAM Identity Center in tp-management, and the policy set that denies new IAM users and keys is an organization policy.
C-9	January 28	The organization trail writes to tp-log-archive, which only an organization provides.

The add-on's own scan, MAF-01 to MAF-13, is not among the 50 checks. It is scored on the add-on's own gate, and it re-runs on February 13, 2026, the day after this report; 12 of its checks are in scope.

The SOC 2 technical map, after

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. The map lists controls that are in place on AWS, from what date, and where the evidence is. The auditor tests them.

The map lists 35 controls. On February 12, 2026, **22 are in place and operating, and 13 are planned**. The Audit and the Foundation account for 22; the rest belong to the Well-Architected Review and to Tidepost. 33 are operating or planned to operate before the observation window opens on April 1, 2026, the latest on March 27, 2026. 2 begin after it opens.

The controls by criteria group.

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

The controls still planned are the Well-Architected Review’s and Tidepost’s, and each has a date:

The planned controls on February 12.

Criterion	Control	Owner	Operating from
CC6.6	Production database private (PubliclyAccessible false) in the new encrypted PostgreSQL 16 instance	Kofi Brandvold	March 22
CC7.2	Alarms on the service-level objectives for the API and the ranking endpoint	Kofi Brandvold	March 20
CC7.4	On-call rotation and the incident process, exercised in a tabletop	Kofi Brandvold	March 26
CC7.5	Post-incident review step in the incident process	Kofi Brandvold	March 26
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	Kofi Brandvold	March 27
A1.1	Service quota alarms at 80% for Rekognition, SageMaker, and EC2 vCPUs, with the limits raised to leave headroom for a zone failover	Kofi Brandvold	March 13
A1.1	Capacity follows demand: target tracking on the API tier, Karpenter on EKS, and queue-depth scaling for the transcoders	Kofi Brandvold	March 17
A1.2	Production database in a Multi-AZ instance	Kofi Brandvold	March 22
A1.3	Restore test from the central vault	Kofi Brandvold	March 24
A1.3	Availability Zone failure drill	Kofi Brandvold	March 25
C1.1	Data-class standard, with a data-class tag on every data store	Sasha Ilyin	March 20
C1.2	Retention schedule for user content, written with counsel	Amara Delacroix	May 20
C1.2	Deletion pipeline for removed posts' media, across originals, renditions, and backups	Marcus Oyelaran	May 20

C1.2 is the exception worth naming: the retention schedule and the deletion pipeline are planned for May 20, 2026, after the window opens, because they wait on counsel and the app team (H-12, deferred in writing). Whether that matters to the report is the auditor’s decision, and we do not predict it. What no engagement touches is Tidepost’s: CC1, CC1.4, CC2, CC3, CC4, CC5, CC9, System description.

The gate, and what follows

The gate, as agreed at the readout.

Item	Result
Critical findings agreed on January 16, 2026	10
Closed, verified by this re-scan	9
Accepted in writing, with a signer and a closing date	1 (C-4, Dev Raman, until March 22, 2026)
Still open	0
Result	PASS
Decided	February 12, 2026
Second invoice, \$14,875	February 13, 2026

What follows

3 items remain after the engagement ends, each with an owner and a date:

- **C-4**, due March 22, 2026, closed through Well-Architected: RDS PostgreSQL publicly accessible from 0.0.0.0/0.
- **H-1**, due March 22, 2026, closed through Well-Architected: RDS and EBS volumes unencrypted at rest.
- **H-12**, due May 20, 2026, closed through Tidepost: No deletion pipeline for removed posts’ media.

The runbooks, the evidence index for the auditor, and the handover are in the next report. The re-scan raised no new failing check, so nothing was added to the register.

© 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.