

AWS WELL-ARCHITECTED FRAMEWORK REVIEW · SAMPLE DELIVERABLE

Runbooks, the Milestone Cadence, and Handover

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

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

March 31, 2026 · AWS Well-Architected Framework Review: The Remediation (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

- What Tidepost owns now 2
- The runbooks 2
- The milestone cadence 3
- The improvement plan 4
- The SOC 2 technical map, as of March 31, 2026 8
 - The two controls planned after the window opens 12
- What the cost engagement takes up 12
- Hours and the fee 13

What Tidepost owns now

The Brief now runs in three Availability Zones, restores from backup inside its in-Region recovery objective, deploys with automatic rollback, and is defined in code; Kofi Brandvold’s team runs all of it from here. Dev Raman: this is the Remediation’s handover, walked through today in the two-hour handover workshop, which was recorded with the attendees’ permission. Milestone two (March 30, 2026) met the gate: 20 HRIs closed by change and 5 accepted in writing. What follows is what your team keeps: 10 runbooks, a milestone cadence, an improvement plan of 19 medium-risk questions with an owner each, the SOC 2 technical map as of today, and the 5 accepted HRIs the cost engagement takes up.

Everything stays in Tidepost’s accounts and repositories: the workload and both milestones in your AWS Well-Architected Tool, every change in tidepost-cdk, and the runbooks beside the code they operate. Vantalect never held write access to production, and the read-only inspection role is the only access we have.

The runbooks

10 runbooks, each tied to the HRI it came from; 4 have already been run end to end in a drill, a test, or the cutover.

The runbooks handed over on March 31, 2026. A runbook not yet run is exercised at the first quarterly review or the first real event, whichever comes first.

Runbook	From	Owner	Exercised so far
Availability Zone evacuation	REL10	Kofi Brandvold	Run in the zone drill March 25
Restore from AWS Backup (database, volumes, DynamoDB)	REL09	Kofi Brandvold	Run in the restore test March 24
Regional recovery to us-west-2	REL13	Dev Raman	Not yet run
The PostgreSQL 16 cutover and Multi-AZ failover	REL11	Kofi Brandvold	Run in the cutover March 22
Canary rollback on EKS and the target-group swap on the EC2 tiers	OPS06	Kofi Brandvold	Canary deploys in use since March 25
Incident process: severity, commander, escalation, customer message	OPS10	Kofi Brandvold	Run in the tabletop March 26
On-call rotation and alarm response	OPS07	Kofi Brandvold	Rotation in use since March 19
Quota alarm response and limit increases	REL01	Kofi Brandvold	Alarms in place since March 13
Monthly cost review	COST01	Gwen Tallis	First review held March 17
Decommissioning and the unattached-resource review	COST04	Kofi Brandvold	Not yet run

The regional recovery runbook has never been run end to end. It restores the database and DynamoDB tables from the us-west-2 copies and rebuilds the stateless tiers from the CDK; the originals bucket is not copied, which Noor Castellanos accepted in writing as a residual risk under REL13. We recommend running it once in tp-staging before the end of the second quarter.

The milestone cadence

The Tool stays useful only if the answers stay true, so the cadence below is part of the handover, not a suggestion.

How Tidepost keeps the workload’s answers current. Each review answers the affected questions again and saves a milestone, so the history stays in the Tool.

When	What	Who
When the cost engagement’s changes are in (planned for May 14, 2026)	Save milestone three: answer the five accepted HRIs’ questions again once their changes land	Kofi Brandvold
Every quarter	Review every question with the workload owners and save a milestone	Kofi Brandvold
After a major release or an architecture change	Answer the affected pillars again and save a milestone	Kofi Brandvold
After any SEV1 or SEV2 incident	Update OPS10 and the affected Reliability answers in the Tool	Kofi Brandvold

The improvement plan

19 questions are at medium risk at milestone two. None is in the guarantee; each has an owner and the best practices still open.

The improvement plan as recorded in the Tool at milestone two, with the owner agreed at the handover.

Question	Pillar	Best practices still open	Owner	Note
OPS02 How do you structure your organization to support your business outcomes?	Operational Excellence	OPS02–BP01 Resources have identified owners; OPS02–BP07 Responsibilities between teams are predefined or negotiated	Kofi Brandvold	Unchanged. The on-call rotation names a primary and a secondary each week, but responsibilities between teams stay unwritten.
OPS03 How does your organizational culture support your business outcomes?	Operational Excellence	OPS03–BP04 Communications are timely, clear, and actionable; OPS03–BP07 Resource teams appropriately	Dev Raman	Unchanged. Hiring a third platform engineer is Tidepost’s decision.
OPS04 How do you implement observability in your workload?	Operational Excellence	OPS04–BP03 Implement user experience telemetry	Bea Okafor	Medium risk remains for user experience telemetry, which depends on a mobile release (Bea Okafor).

Question	Pillar	Best practices still open	Owner	Note
OPS09 How do you understand the health of your operations?	Operational Excellence	OPS09–BP02 Communicate status and trends to ensure visibility into operation; OPS09–BP03 Review operations metrics and prioritize improvement	Kofi Brandvold	Medium risk remains until the first review has been held and its actions prioritized.
SEC01 How do you securely operate your workload?	Security	SEC01–BP01 Separate workloads using accounts	Sasha Ilyin	Unchanged. Moving staging (June) and the data accounts (third quarter) is workload migration on Tidepost's calendar, outside the Foundation add-on.
SEC07 How do you classify your data?	Security	SEC07–BP03 Automate identification and classification; SEC07–BP04 Define data lifecycle management	Sasha Ilyin	Medium risk remains: automated classification (Macie) was considered and not run, and disposal depends on the originals' retention schedule, which waits on counsel.
SEC11 How do you incorporate and validate the security properties of applications throughout the design, development, and deployment lifecycle?	Security	SEC11–BP03 Perform regular penetration testing; SEC11–BP08 Build a program that embeds security ownership in workload teams	Marcus Oyelaran	Medium risk remains for penetration testing and for security ownership in the workload teams; both are Tidepost's to schedule.
REL04 How do you design interactions in a distributed system to prevent failures?	Reliability	REL04–BP02 Implement loosely coupled dependencies	Amara Delacroix	Unchanged. Moving the chain onto Step Functions is a multi-quarter rewrite, deferred by Dev Raman at the readout.

Question	Pillar	Best practices still open	Owner	Note
REL05 How do you design interactions in a distributed system to mitigate or withstand failures?	Reliability	REL05–BP01 Implement graceful degradation to transform applicable hard dependencies into soft dependencies; REL05–BP02 Throttle requests	Marcus Oyelaran	A fallback to a cached ranking is Marcus Oyelaran's next-quarter item.
REL07 How do you design your workload to adapt to changes in demand?	Reliability	REL07–BP04 Load test your workload	Marcus Oyelaran	Medium risk remains until a full-path load test runs.
REL12 How do you test reliability?	Reliability	REL12–BP05 Test resiliency using chaos engineering	Kofi Brandvold	Medium risk remains for automated fault injection.
REL13 How do you plan for disaster recovery (DR)?	Reliability	REL13–BP02 Use defined recovery strategies to meet the recovery objectives	Dev Raman	Medium risk remains for the originals: Noor Castellanos declined cross-Region replication and accepted the residual risk in writing, to be revisited once the originals have a retention schedule.
PERF04 How do you select and configure networking resources in your workload?	Performance Efficiency	PERF04–BP05 Choose network protocols to improve performance; PERF04–BP07 Optimize network configuration based on metrics	Bea Okafor	Unchanged. The rendition ladder is Bea Okafor's and belongs to the cost engagement.
COST03 How do you monitor usage and cost?	Cost Optimization	COST03–BP06 Allocate costs based on workload metrics	Gwen Tallis	Medium risk remains for unit costs, which the cost engagement's reports begin.
COST05 How do you evaluate cost when you select services?	Cost Optimization	COST05–BP02 Analyze all components of the workload; COST05–BP06 Perform cost analysis for different usage over time	Gwen Tallis	Unchanged. The cost engagement analyzes the moderation paths.

Question	Pillar	Best practices still open	Owner	Note
COST08 How do you plan for data transfer charges?	Cost Optimization	COST08–BP01 Perform data transfer modeling; COST08–BP03 Implement services to reduce data transfer costs	Kofi Brandvold	Medium risk remains; the cost engagement measures the transfer the new topology causes.
COST09 How do you manage demand, and supply resources?	Cost Optimization	COST09–BP03 Supply resources dynamically	Kofi Brandvold	Medium risk remains for the fixed GPU and developer compute (COST06 and SUS02).
SUS03 How do you take advantage of software and architecture patterns to support your sustainability goals?	Sustainability	SUS03–BP02 Remove or refactor workload components with low or no use	Amara Delacroix	Re-reviewed on March 30; nothing changed since March 6.
SUS05 How do you select and use cloud hardware and services in your architecture to support your sustainability goals?	Sustainability	SUS05–BP02 Use instance types with the least impact; SUS05–BP04 Optimize your use of hardware-based compute accelerators	Yuki Sorensen	Re-reviewed on March 30; nothing changed since March 6.

The SOC 2 technical map, as of March 31, 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.

33 of the map's 35 controls are in place on March 31, against 22 when the security engagement handed the map over on February 12. The 11 that moved to in place since then are this engagement's, for CC6.6, CC7.2, CC7.4, CC7.5, CC8.1, A1.1, A1.2, A1.3, and C1.1; the two A1.1 rows are the capacity controls from RELO1 and RELO7. The 2 still planned are Tidepost's C1.2 disposal controls.

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 March 31, and "new" marks a row that moved to in place after February 12; "Planned" carries the date it begins. The criteria cover Security, Availability, and Confidentiality, and the auditor tests them over a window from April 1 to September 30.

35 controls: 33 in place and 2 planned on March 31, 11 of them new since February 12. Every row before the window opens is in place.

Criterion	Control	Operating from	On March 31	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	Secrets Manager inventory and the repository secret-scan results (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	IAM credential reports and root-task records in the organization trail (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	Identity Center assignments and sign-in events (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	Service control policy attachments and the exception signed February 11 (tp-management)	Sasha Ilyin

Criterion	Control	Operating from	On March 31	Evidence is in	Owner
CC6.3	Link-preview service role cut to 14 actions; IMDSv2 required	Jan 8	In place	IAM policy versions and Access Analyzer findings (tp-prod)	Marcus Oyelaran
CC6.3	EKS endpoints private, and developers on namespace-scoped access entries instead of cluster administrator	Jan 30	In place	EKS access entries and cluster configuration history (tp-prod)	Kofi Brandvold
CC6.3	One execution role per moderation function, each limited to its own buckets and endpoints	Feb 9	In place	IAM role policies and Config history (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	The account trail's PutPublicAccessBlock and PutBucketPolicy calls for January 6 to 28, then Config history for the S3 public-access rules (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	Security group history and the written acceptance of January 16 (tp-prod)	Kofi Brandvold
CC6.6	OpenSearch inside the VPC with fine-grained access control	Jan 21	In place	The account trail's OpenSearch configuration calls, then Config history for the domain (tp-prod)	Marcus Oyelaran
CC6.6	Redis with in-transit encryption and an AUTH token from Secrets Manager	Jan 27	In place	The account trail's ElastiCache calls, then Config history for the replication group (tp-prod)	Marcus Oyelaran
CC6.6	No inbound SSH; shell access through Session Manager with session logs	Jan 20	In place	Session Manager logs and security group history (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	WAF logs and web ACL associations (tp-prod)	Marcus Oyelaran
CC6.6	Production database private (PubliclyAccessible false) in the new encrypted PostgreSQL 16 instance	Mar 22	In place (new)	RDS configuration and the March 22 cutover record (tp-prod)	Kofi Brandvold

Criterion	Control	Operating from	On March 31	Evidence is in	Owner
CC6.7	TLS required in transit: TLS-only bucket statements and a CloudFront minimum of TLS 1.2	Jan 30	In place	S3 bucket policies and CloudFront distribution configuration (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	Resource control policy attachments (tp-management)	Kofi Brandvold
CC6.8	Inspector on EC2 and ECR, and GuardDuty runtime monitoring on EKS, delegated to tp-audit	Jan 29	In place	Inspector and GuardDuty findings in tp-audit (tp-audit)	Sasha Ilyin
CC7.1	Organization trail, multi-Region, into tp-log-archive	Jan 28	In place	The organization trail in tp-log-archive (tp-log-archive)	Sasha Ilyin
CC7.1	AWS Config recording in every governed account, with the aggregator in tp-audit	Jan 29	In place	Config history and the aggregator in tp-audit (tp-audit)	Sasha Ilyin
CC7.2	GuardDuty and Security Hub findings reviewed from tp-audit	Jan 29	In place	Security Hub and GuardDuty in tp-audit (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	CloudWatch alarm history and flow logs (tp-prod)	Kofi Brandvold
CC7.2	Alarms on the service-level objectives for the API and the ranking endpoint	Mar 20	In place (new)	CloudWatch alarm history (tp-prod)	Kofi Brandvold
CC7.3	Security runbooks for a leaked credential, a public bucket, and a compromised instance	Feb 12	In place	The runbooks and the evidence index handed over February 12 (tp-prod)	Sasha Ilyin
CC7.4	On-call rotation and the incident process, exercised in a tabletop	Mar 26	In place (new)	The on-call schedule and the tabletop record (tp-prod)	Kofi Brandvold
CC7.5	Post-incident review step in the incident process	Mar 26	In place (new)	The tabletop record and the review template (tp-prod)	Kofi Brandvold

Criterion	Control	Operating from	On March 31	Evidence is in	Owner
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	In place (new)	Pull requests, pipeline runs, and CloudFormation drift reports (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	In place (new)	CloudWatch alarm history and the Service Quotas request history (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	In place (new)	Auto Scaling activity, Karpenter events, and CloudWatch capacity metrics (tp-prod)	Kofi Brandvold
A1.2	AWS Backup plan with a locked vault in tp-backup and cross-Region copies to us-west-2	Feb 10	In place	AWS Backup job history in tp-backup (tp-backup)	Kofi Brandvold
A1.2	Production database in a Multi-AZ instance	Mar 22	In place (new)	RDS configuration and the March 22 cutover record (tp-prod)	Kofi Brandvold
A1.3	Restore test from the central vault	Mar 24	In place (new)	The restore test record and timings (tp-backup)	Kofi Brandvold
A1.3	Availability Zone failure drill	Mar 25	In place (new)	The drill record and service dashboards (tp-prod)	Kofi Brandvold
C1.1	Data-class standard, with a data-class tag on every data store	Mar 20	In place (new)	Tag policy compliance and the standard (tp-management)	Sasha Ilyin
C1.2	Retention schedule for user content, written with counsel	May 20	Planned	The signed schedule (tp-prod)	Amara Delacroix
C1.2	Deletion pipeline for removed posts' media, across originals, renditions, and backups	May 20	Planned	Pipeline job history and a sampled deletion check (tp-prod)	Marcus Oyelaran

The two controls planned after the window opens

- Retention schedule for user content, written with counsel (C1.2), planned to operate from May 20, evidence in tp-prod, owned by Amara Delacroix.
- Deletion pipeline for removed posts’ media, across originals, renditions, and backups (C1.2), planned to operate from May 20, evidence in tp-prod, owned by Marcus Oyelaran.

They wait on counsel and on the app team’s work on H-12, which Tidepost deferred with a written acceptance, so both begin after the observation window opens on April 1. The map shows the date, and the auditor tests the controls from it. What no Vantalect engagement touches is listed in the security handover of February 12 and has not changed.

What the cost engagement takes up

The cost engagement starts on April 6, 2026, and its readout on April 17 prices and schedules the 5 HRIs accepted in writing. Each fix is a cost change, so the cost engagement makes it and counts it, once; this engagement counted none of them. Until each lands, its question stays at high risk in the Tool.

The acceptances the gate counted as closed, handed to the cost engagement.

HRI	The fix	Accepted by	On	Risk while it waits
PERF03	Store raw telemetry in a columnar, partitioned format and point Athena at it, so a query reads only the columns and days it needs	Lior Haddad	March 9	Each Athena query keeps scanning raw JSON.
COST06	Size the GPU endpoints, the notebooks, and the EC2 tiers to measured use	Gwen Tallis	March 10	Oversized compute keeps running at its current size.
COST07	Commit to a Savings Plan for the steady compute once it is sized, so the commitment fits what runs	Gwen Tallis	March 10	Everything keeps billing at On-Demand rates.
SUS02	Scale the GPU endpoints and notebooks to demand instead of running them around the clock	Yuki Sorensen	March 11	GPU endpoints and notebooks keep running around the clock.
SUS04	Set retention on application logs, the telemetry stream, raw telemetry, and the originals	Lior Haddad	March 9	Logs, the telemetry stream, and raw telemetry keep growing without limit.

Three more things go with them. The cost engagement starts from a bill the Remediation raised by a net \$10,094 a month at list, almost all of it the second and third zones, so none of that increase is a saving waiting to be found. Staging’s PostgreSQL 13 Extended Support, \$584 a month, continues until Tidepost retires the old staging in tp-prod. And the cross-zone traffic the new topology causes is measured from the cost engagement’s first week of the Cost and Usage Report, which is the evidence COST08 still lacks.

Hours and the fee

93 consultant hours through last week, and 15 planned for this closing week, which runs to April 3: 108 of the 110 the engagement caps.

Hours by engagement week, from the kickoff on February 23 to the end on April 3. The closing week’s hours are the plan through April 3.

WeekStarting	Hours
1February 23	20
2March 2	20
3March 9	17
4March 16	18
5March 23	18
6March 30	15 (planned)
Total, with the closing week as planned	108

Of the \$29,750 fee, \$14,875 was invoiced at signature, and the second \$14,875 is invoiced on April 3, 2026, now that milestone two has met the gate.

© 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.