

AWS WELL-ARCHITECTED FRAMEWORK REVIEW · SAMPLE DELIVERABLE

Operational Excellence: Code, Deployments, Observability, and Incidents

Week 4 of 6: Operations · prepared for Tidepost, Inc.

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

March 20, 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

Summary	2
The seven HRIs	3
What closed	4
What is scheduled	5
The week’s changes to the estate.....	6
Other items closed this week	7
Where all 25 stand on March 20	8
What happens next.....	9

Summary

4 of the 7 Operational Excellence and Security HRIs are closed on March 20, and the other 3 are scheduled for March 25, March 26, and March 27. Dev Raman and Kofi Brandvold: this is the Remediation’s week 4 report. The four that closed are the ones that keep the workload observable and defensible while it changes: service-level objectives with alarms, runbooks and an on-call rotation, dependency and static analysis in the pipeline, and a data-class standard. The three still open are the ones that need a day of proof: canary deploys, the incident tabletop, and the import of the console-built resources into the CDK.

The week at a glance, as of March 20, 2026. The three scheduled items are plans, not results.

Operations and Security on March 20	Result
HRIs in these two pillars	7
Closed	4
Scheduled, last on March 27	3
Other HRIs that reached a final state this week	4
Changes to the estate this week, in place of 8	5
All 25 agreed HRIs: closed, accepted, scheduled	12, 5, 8

How the changes get made

Vantalect works in Tidepost's account through a read-only inspection role. Every change to the estate in this report lands as code in Tidepost's `tidepost-cdk` pull requests, reviewed by the owning engineer and shipped by Tidepost's pipeline. A fix that is a document, such as a runbook or a standard, is written and adopted by its owner. We pair on the design and review the result; we do not write to production. The only thing we record in your account is the workload in your own AWS Well-Architected Tool.

The seven HRIs

The two pillars carry 7 HRIs between them: 5 in Operational Excellence and 2 in Security. The list is the one agreed on March 6.

The 7 Operational Excellence and Security questions rated "High risk" in the AWS Well-Architected Framework lens. A question stays "High risk" in the Tool until its change lands and the answers are saved again.

Question	Owner	Fix	State on March 20
SEC11 How do you incorporate and validate the security properties of applications throughout the design, development, and deployment lifecycle?	Marcus Oyelaran	Dependency scanning and static analysis in CI, blocking on high severity	Closed March 17
OPS07 How do you know that you are ready to support a workload?	Kofi Brandvold	Runbooks, playbooks, and an on-call rotation with a primary and a secondary	Closed March 19
OPS04 How do you implement observability in your workload?	Kofi Brandvold	SLOs for upload-to-timeline time and playback start, with tracing and burn-rate alarms	Closed March 20
SEC07 How do you classify your data?	Sasha Ilyin	A data-class standard with a data-class tag on every bucket, table, and database	Closed March 20
OPS06 How do you mitigate deployment risks?	Kofi Brandvold	Canary deploys with automatic rollback on EKS, and a target-group swap with rollback on the EC2 tiers	Scheduled for March 25
OPS10 How do you manage workload and operations events?	Kofi Brandvold	An incident process (severity levels, commander, escalation, customer message), tested in a tabletop	Scheduled for March 26
OPS05 How do you reduce defects, ease remediation, and improve flow into production?	Kofi Brandvold	Import the console-built resources (the moderation pipeline, the data stores, and the network) into the CDK	Scheduled for March 27

What closed

The four that closed are in place and confirmed by their owners. They are listed in the order they closed.

- **SEC11, closed March 17 by Marcus Oyelaran.** Dependency scanning and static analysis in CI, blocking on high severity.

- **OPS07, closed March 19 by Kofi Brandvold.** Runbooks, playbooks, and an on-call rotation with a primary and a secondary.
- **OPS04, closed March 20 by Kofi Brandvold.** SLOs for upload-to-timeline time and playback start, with tracing and burn-rate alarms.
- **SEC07, closed March 20 by Sasha Ilyin.** A data-class standard with a data-class tag on every bucket, table, and database.

What each one changes for the people running the workload:

- **Observability (OPS04).** With objectives written for upload-to-timeline time and playback start, a burn-rate alarm fires when an objective is being spent too fast, and tracing shows which stage is slow, so the team hears about a slow upload from an alarm instead of from a customer.
- **Readiness to support (OPS07).** A runbook turns "who knows how to fix this" into a page anyone on call can follow, and the rotation has a primary and a secondary so one missed page does not become an outage. The runbooks are the ones in the handover set at the end of the engagement.
- **Dependency and static analysis in CI (SEC11).** The pipeline now blocks a merge on a high-severity finding, so a vulnerable dependency or an unsafe pattern is stopped in the pull request, where the fix is cheapest.
- **Data classification (SEC07).** The standard names the data classes, and a data-class tag on every bucket, table, and database means a policy, a backup rule, or a retention schedule can select by class instead of by a list someone keeps by hand.

What is scheduled

Three HRIs are open, each with a date, an owner, and one proof that closes it. None of them has run yet.

The three scheduled items in Operational Excellence. Tidepost's team runs each; Vantalect pairs and reviews.

Date	Closes	What happens	Owner
March 25	OPS06	Canary deploys with automatic rollback on EKS, and a target-group swap with rollback on the EC2 tiers	Kofi Brandvold
March 26	OPS10	An incident process (severity levels, commander, escalation, customer message), tested in a tabletop	Kofi Brandvold
March 27	OPS05	Import the console-built resources (the moderation pipeline, the data stores, and the network) into the CDK	Kofi Brandvold

- **Canary deploys (OPS06, March 25).** A new version takes a small share of traffic first and rolls back automatically when its health checks fail. On the EC2 tiers the same safety comes from swapping a target group, with a rollback that is the swap in reverse.
- **The incident tabletop (OPS10, March 26).** The team walks one realistic failure from the first alarm to the customer message, using the severity levels, the commander role, and the escalation path, and writes down every place the process stumbled. The question closes only after the process has been exercised.
- **The CDK import (OPS05, March 27).** The console-built resources, 142 in all, are imported into tidepost-cdk so that every change to them goes through a pull request. An import changes how a resource is managed, not what it is; the plan before the import has to show no change to the resource.

The week's changes to the estate

This week's changes are mostly the Reliability work landing, with two changes that reduce the bill. The table shows each change, its date, and its monthly effect at list price.

Changes dated in week 4. The scheduled rows are the Sunday cutover window, described in the reliability report. A negative amount is a saving.

Change	Date	State on March 20	What it did	Monthly at list
Three more API instances	March 16	In place	The API tier from 6 to 9 c6i.4xlarge, three in each of three zones.	\$1,551
Cross-zone traffic	March 17	In place	Traffic between tiers, replicas, and the standby now crosses Availability Zones.	\$1,536
Three more EKS nodes	March 17	In place	The production node group from 9 to 12 m5.4xlarge, four in each of three zones.	\$1,836
Ranking endpoint moved to CPU	March 18	In place	2 ml.g5.2xlarge replaced by 6 ml.c6i.2xlarge after a load test with p99 38 ms against a 50 ms budget.	-\$425
Production EKS out of extended support	March 19	In place	The production cluster, in extended support on Kubernetes 1.30 since July 2025, upgraded to 1.33 through 1.31 and 1.32, one minor version at a time, control plane and node groups. Kubernetes 1.33 is in standard support until July 29, 2026, and 1.32 leaves it on March 23. Staging stays on 1.30 until it is retired.	-\$365
Production PostgreSQL 16 runs Multi-AZ	March 22	Scheduled	Part of the Sunday cutover window	\$1,313
Allocated database storage doubled	March 22	Scheduled	Part of the Sunday cutover window	\$236

Other items closed this week

4 HRIs outside these two pillars closed this week. Their pillars have their own reports; they are here so the week reads as one list.

HRIs outside Operational Excellence and Security that closed in week 4, up to March 20.

Question	Pillar	Owner	Closed	What changed
REL07	Reliability	Kofi Brandvold	March 17	Target tracking on the API, Karpenter on EKS, and queue-depth scaling for the transcoders
COST01	Cost Optimization	Gwen Tallis	March 17	A monthly cost review owned by Gwen Tallis and Kofi Brandvold
PERF02	Performance Efficiency	Yuki Sorensen	March 18	The ranking endpoint moved from 2 ml.g5.2xlarge to 6 ml.c6i.2xlarge after a load test (p99 38 ms against a 50 ms budget)
COST04	Cost Optimization	Kofi Brandvold	March 19	A decommissioning runbook, an owner tag on every resource, and a monthly unattached-resource review

Where all 25 stand on March 20

12 are closed, 5 are accepted in writing, and 8 are scheduled. The five accepted in writing are Performance, Cost, and Sustainability items whose fix is a cost change; the cost engagement, which starts April 6, takes each one up at its April 17 readout.

All 25 HRIs agreed at the readout, as of March 20.

Question	Pillar	Owner	State	Date
OPS04	Operational Excellence	Kofi Brandvold	Closed	March 20
OPS05	Operational Excellence	Kofi Brandvold	Scheduled	March 27
OPS06	Operational Excellence	Kofi Brandvold	Scheduled	March 25
OPS07	Operational Excellence	Kofi Brandvold	Closed	March 19
OPS10	Operational Excellence	Kofi Brandvold	Scheduled	March 26
SEC07	Security	Sasha Ilyin	Closed	March 20
SEC11	Security	Marcus Oyelaran	Closed	March 17
REL01	Reliability	Kofi Brandvold	Closed	March 13
REL02	Reliability	Kofi Brandvold	Closed	March 10
REL07	Reliability	Kofi Brandvold	Closed	March 17
REL09	Reliability	Kofi Brandvold	Scheduled	March 24

Question	Pillar	Owner	State	Date
REL10	Reliability	Kofi Brandvold	Scheduled	March 25
REL11	Reliability	Kofi Brandvold	Scheduled	March 22
REL12	Reliability	Kofi Brandvold	Scheduled	March 25
REL13	Reliability	Dev Raman	Scheduled	March 24
PERF02	Performance Efficiency	Yuki Sorensen	Closed	March 18
PERF03	Performance Efficiency	Lior Haddad	Accepted in writing	March 9
COST01	Cost Optimization	Gwen Tallis	Closed	March 17
COST02	Cost Optimization	Gwen Tallis	Closed	March 13
COST03	Cost Optimization	Kofi Brandvold	Closed	March 11
COST04	Cost Optimization	Kofi Brandvold	Closed	March 19
COST06	Cost Optimization	Gwen Tallis	Accepted in writing	March 10
COST07	Cost Optimization	Gwen Tallis	Accepted in writing	March 10
SUS02	Sustainability	Yuki Sorensen	Accepted in writing	March 11
SUS04	Sustainability	Lior Haddad	Accepted in writing	March 9

What happens next

1. Sunday, March 22: the PostgreSQL 16 cutover, described in the reliability report.
2. March 25, March 26, and March 27: canary deploys, the incident tabletop, and the CDK import.
3. The week 5 report covers Performance, Cost, and Sustainability, and the reliability proofs.

© 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.