

AWS WELL-ARCHITECTED FRAMEWORK REVIEW · SAMPLE DELIVERABLE

Reliability: Three Zones, Backups, Restore, and Recovery

Week 3 of 6: Reliability · prepared for Tidepost, Inc.

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

March 13, 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 eight Reliability HRIs	3
Three zones, before and after	4
Backups	5
The recovery plan and the proofs	6
What was declined	7
What the reliability changes add to the bill	8
Closed this week, outside Reliability	9
Where all 25 stand on March 13.....	10
What happens next.....	11

Summary

2 of the 8 Reliability HRIs are closed on March 13, and the other 6 are scheduled to close by March 25. Dev Raman and Kofi Brandvold: this is the Remediation’s week 3 report, and it follows the six-pillar scorecard you saw at the March 6 readout, where Reliability was the weakest pillar with 8 HRIs among its 13 questions.

The work this week is about zones. The NAT gateways, the cache, and the search domain already run across them, the API tier and the Kubernetes nodes are scheduled to follow, and the database is scheduled for a cutover on Sunday, March 22, from 2:00 AM CDT. Backups run daily into tp-backup and are copied to us-west-2. The two proofs that matter, a restore test on March 24 and a zone evacuation drill on March 25, have not run yet, and this report says so rather than guess at what they will show.

The week at a glance, as of March 13, 2026. Nothing in this table is a measured result of a drill or the cutover; those are scheduled.

Reliability on March 13	Result
Reliability HRIs agreed at the readout	8
Closed	2
Scheduled to close, last on March 25	6
Zone changes in place, of 6	3
Reliability changes in place, of 11	6
Recovery point and recovery time agreed inside us-east-1	15 minutes and 4 hours
Recovery point and recovery time for a Region loss	Up to 24 hours, and not yet proven
Added to the monthly bill at list, once all are in	\$10,300
All 25 agreed HRIs: closed, accepted, scheduled	4, 5, 16

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, or, where noted, in Tidepost’s console. 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 eight Reliability HRIs

Every Reliability HRI has an owner, an agreed fix, and a date. The list is the one agreed on March 6; a question stays "High risk" in the Tool until its change lands and the answers are saved again at milestone two, on March 30.

The 8 Reliability questions rated "High risk" in the AWS Well-Architected Framework lens. A question is closed when the change is in place and the owner has confirmed it.

Question	Owner	Agreed fix	State on March 13
REL01 How do you manage Service Quotas and constraints?	Kofi Brandvold	Quota alarms and raised limits for Rekognition, SageMaker, and EC2 vCPUs	Closed March 13
REL02 How do you plan your network topology?	Kofi Brandvold	Subnets and NAT gateways in three zones (NAT1 to 3)	Closed March 10
REL07 How do you design your workload to adapt to changes in demand?	Kofi Brandvold	Target tracking on the API, Karpenter on EKS, and queue-depth scaling for the transcoders	Scheduled for March 17
REL09 How do you back up data?	Kofi Brandvold	AWS Backup to tp-backup with vault lock, DynamoDB point-in-time recovery, and a timed restore test	Scheduled for March 24
REL10 How do you use fault isolation to protect your workload?	Kofi Brandvold	The API tier, EKS nodes, NAT, Redis, OpenSearch, and RDS across zones, proved by a zone evacuation drill	Scheduled for March 25
REL11 How do you design your workload to withstand component failures?	Kofi Brandvold	Redis replicas, OpenSearch dedicated masters, and RDS Multi-AZ failover, completed by the PostgreSQL 16 cutover	Scheduled for March 22
REL12 How do you test reliability?	Kofi Brandvold	Playbooks, and the zone drill and the restore test run as game days	Scheduled for March 25
REL13 How do you plan for disaster recovery (DR)?	Dev Raman	A recovery plan with written recovery point and recovery time objectives, and database and DynamoDB backups copied to us-west-2	Scheduled for March 24

Closed: REL02 on March 10, REL01 on March 13. Still open, in order of date: REL07, REL11, REL09, REL13, REL10, and REL12. Each one waits on a change or a proof listed below, and the table above gives its date.

Three zones, before and after

Before this week the network, the cache, the search domain, the API tier, the Kubernetes nodes, and the database all ran in one Availability Zone. The table puts each tier's start beside where it ends up and the day it changes.

The zone map. The first four tiers split their capacity evenly across three zones; the database gets a standby in a second zone.

Tier	Before	After	Change	State on March 13
API tier	6 in one zone	9, 3 in each of 3 zones	March 16	Scheduled
EKS production node group	9 in one zone	12, 4 in each of 3 zones	March 17	Scheduled
NAT gateways	1 in one zone	3, one in each zone	March 10	In place
ElastiCache for Redis OSS	2 shards, no replicas	2 shards, 1 replica each in a second zone	March 11	In place
OpenSearch Service	3 data nodes in one zone, no dedicated masters	3 data nodes, one per zone, and 3 dedicated masters	March 12	In place
RDS for PostgreSQL	Single-AZ PostgreSQL 13 writer	Multi-AZ PostgreSQL 16 writer with a standby in a second zone	March 22	Scheduled

NAT gateways, ElastiCache for Redis OSS, and OpenSearch Service are done. API tier, EKS production node group, and RDS for PostgreSQL are scheduled. The API tier and the node group add capacity as well as zones: the API tier grows from 6 to 9 c6i.4xlarge instances and the production node group from 9 to 12 m5.4xlarge nodes, so that losing a zone leaves two thirds of the capacity standing.

Backups

Backups are running, and they are copied out of the Region. Until March 10 the databases and volumes had no AWS Backup plan and DynamoDB had no point-in-time recovery, which is why RELO9 was rated "High risk".

The three backup changes, all in place on March 13. The AWS Backup line is warm storage in the vaults of tp-backup, in us-east-1 and in the us-west-2 copies.

Backup	What it covers	In place	Monthly at list
AWS Backup	A daily backup plan for the database, the volumes, and the DynamoDB tables in tp-prod: recovery points are taken in tp-prod and copied cross-account to the tp-backup vault, which has vault lock.	March 10	\$512
DynamoDB point-in-time recovery	Point-in-time recovery on the DynamoDB tables.	March 10	\$410
Cross-Region backup copies	Database and DynamoDB backups copied to us-west-2. The originals bucket is not copied (declined).	March 12	\$164

Two properties matter more than the plan itself. The vault lock means nobody, including a compromised administrator, can delete a recovery point before its retention ends, and the daily copies in us-west-2 mean a Regional loss does not take the backups with it, though it can take up to a day of data. A backup nobody has restored is still only a hope, so REL09 stays open until the restore test on March 24.

The recovery plan and the proofs

The recovery plan sets its numbers by scope. Inside us-east-1: a 15-minute recovery point for the database and a 4-hour recovery time for the workload. For the loss of the Region: a recovery point of up to 24 hours, and a recovery time not yet proven. Dev Raman agreed both scopes as the owner of REL13. The restore test runs in us-east-1 and measures the in-Region recovery time against a 4-hour objective, and the point-in-time recovery on the database and on DynamoDB is what makes the in-Region recovery point reachable. The us-west-2 copies are made once a day, so a Region loss can cost up to a day of data, and its recovery time stays unproven until the regional recovery runbook runs end to end.

Three proofs are scheduled. None has happened, and each closes the question it names.

The scheduled proofs. The cutover runs in a Sunday maintenance window, announced to Tidepost's engineers a week ahead; Tidepost's team runs all three and Vantalect pairs and reviews.

Date	Proof	Closes	Run by
Sunday, March 22, from 2:00 AM CDT	The PostgreSQL 16 Multi-AZ cutover: a new encrypted, private writer with a synchronous standby in a second zone takes over from PostgreSQL 13	REL11, and the database part of REL10	Kofi Brandvold and the platform team
March 24	The restore test: restore the database, volumes, and DynamoDB tables from AWS Backup into a clean environment and time it against the 4-hour objective	REL09, and REL13	Kofi Brandvold
March 25	The zone evacuation drill: take one Availability Zone out of service by manual failover and watch the other two carry traffic	REL10, and REL12	Kofi Brandvold

The cutover is the largest single change in the Remediation, and it is the reason the database is last. The new instance is built beside the old one, loaded from a snapshot, and kept current until the window, so the work inside the window is the switch itself. We will not call it a success until it has run; the next report states what happened.

What was declined

Of the Reliability decisions to leave a risk in place, 2 were declined and 1 deferred, each decided by a named person on a named day. A decision to leave a risk in place is part of the plan, not a gap in it.

Declined and deferred decisions on the Reliability questions as of March 13.

Decision	Decided by	Date	Why	What it leaves
Cross-Region replication of the originals bucket (declined)	Noor Castellanos	March 9	The one-time copy of the originals and holding them in Glacier Instant Retrieval cost more than Tidepost will pay to cover a Region loss, which the plan already treats as the slow case: up to 24 hours of database and DynamoDB data from the daily us-west-2 copies, and a recovery time not yet proven.	Accepted in writing as a residual risk under REL13. Revisit: after the retention schedule.
Moving the moderation pipeline's Lambda chain onto Step Functions (deferred)	Dev Raman	March 6	A multi-quarter rewrite of the pipeline that the Trust and Safety team depends on every day.	Left as a medium risk (RELO4). Revisit: Tidepost's planning for the third quarter.
Multi-Region active-active (declined)	Dev Raman	March 6	The four-hour recovery time is for failures inside us-east-1 and is planned as a restore. For a Region loss Tidepost accepts a restore in us-west-2 from the daily copies, and active-active would double the estate.	Declined. Revisit: not scheduled.

What the reliability changes add to the bill

All of the Reliability work adds \$10,300 a month at list price. Every one of these lines is a deliberate cost: redundancy is what a second zone, a replica, or a backup copy is, and each row is the price of the specific risk it removes. Prices are at list, as a monthly run rate once the change is in place.

The bill increase from the Reliability changes. Rows are rounded to the dollar; the total is the sum of the unrounded amounts. \$3,829 of it is already running.

Change	Date	State on March 13	Monthly at list
AWS Backup	March 10	In place	\$512
DynamoDB point-in-time recovery	March 10	In place	\$410
NAT gateways in three zones	March 10	In place	\$66
ElastiCache replicas	March 11	In place	\$2,397

Change	Date	State on March 13	Monthly at list
Cross-Region backup copies	March 12	In place	\$164
OpenSearch dedicated masters	March 12	In place	\$280
Three more API instances	March 16	Scheduled	\$1,551
Cross-zone traffic	March 17	Scheduled	\$1,536
Three more EKS nodes	March 17	Scheduled	\$1,836
Production PostgreSQL 16 runs Multi-AZ	March 22	Scheduled	\$1,313
Allocated database storage doubled	March 22	Scheduled	\$236
Total once all are in			\$10,300

The largest line is the cache replicas, \$2,397, because the cluster's nodes are large. Cross-zone data transfer is the one with no switch to flip: it is the traffic between tiers, replicas, and the standby that now crosses zone lines. The cost engagement that starts April 6 reviews the whole bill, these lines included.

Closed this week, outside Reliability

Outside Reliability, 7 HRIs reached a final state in week 3. Each is also in the register below.

Week 3, from March 9, outside Reliability. An HRI accepted in writing counts as resolved for the guarantee gate; in the Tool its question stays "High risk" until the change lands.

Question	Pillar	Owner	State	Date
PERF03	Performance Efficiency	Lior Haddad	Accepted in writing	March 9
SUS04	Sustainability	Lior Haddad	Accepted in writing	March 9
COST06	Cost Optimization	Gwen Tallis	Accepted in writing	March 10
COST07	Cost Optimization	Gwen Tallis	Accepted in writing	March 10
COST03	Cost Optimization	Kofi Brandvold	Closed	March 11
SUS02	Sustainability	Yuki Sorensen	Accepted in writing	March 11
COST02	Cost Optimization	Gwen Tallis	Closed	March 13

Where all 25 stand on March 13

4 are closed, 5 are accepted in writing, and 16 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 13.

Question	Pillar	Owner	State	Date
OPS04	Operational Excellence	Kofi Brandvold	Scheduled	March 20
OPS05	Operational Excellence	Kofi Brandvold	Scheduled	March 27
OPS06	Operational Excellence	Kofi Brandvold	Scheduled	March 25
OPS07	Operational Excellence	Kofi Brandvold	Scheduled	March 19
OPS10	Operational Excellence	Kofi Brandvold	Scheduled	March 26
SEC07	Security	Sasha Ilyin	Scheduled	March 20
SEC11	Security	Marcus Oyelaran	Scheduled	March 17
REL01	Reliability	Kofi Brandvold	Closed	March 13
REL02	Reliability	Kofi Brandvold	Closed	March 10
REL07	Reliability	Kofi Brandvold	Scheduled	March 17
REL09	Reliability	Kofi Brandvold	Scheduled	March 24
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	Scheduled	March 18
PERF03	Performance Efficiency	Lior Haddad	Accepted in writing	March 9
COST01	Cost Optimization	Gwen Tallis	Scheduled	March 17
COST02	Cost Optimization	Gwen Tallis	Closed	March 13
COST03	Cost Optimization	Kofi Brandvold	Closed	March 11

Question	Pillar	Owner	State	Date
COST04	Cost Optimization	Kofi Brandvold	Scheduled	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. March 17 to March 25: the remaining changes land in the order of the zone table, and each owner confirms their question in the Tool.
2. Sunday, March 22, from 2:00 AM CDT: the PostgreSQL 16 cutover.
3. March 24 and March 25: the restore test and the zone evacuation drill.
4. The week 4 report covers Operational Excellence and Security, and states what happened on March 22.

© 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.