

AWS WELL-ARCHITECTED FRAMEWORK REVIEW · SAMPLE DELIVERABLE

Week-Six Milestone, Pillar by Pillar

Week 6 of 6: Milestone two · 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

The gate is met

Pillar by pillar

Operational Excellence

Security

Reliability

Performance Efficiency

Cost Optimization

Sustainability

What the drills proved

The five that remain

What the milestone cost

2310111313

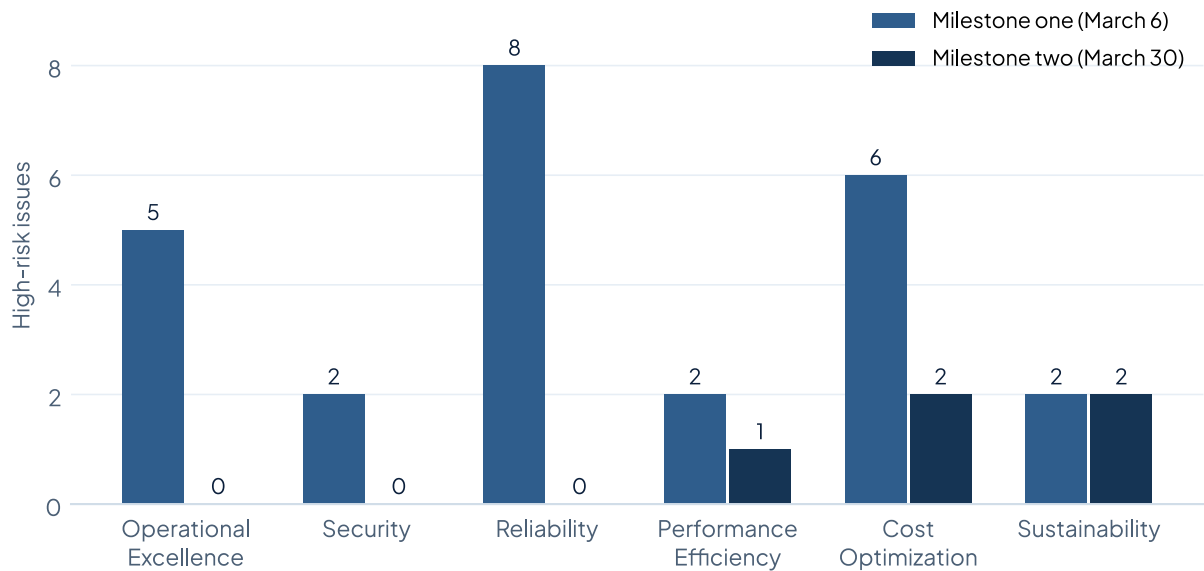
The gate is met

Milestone two, saved in Tidepost’s AWS Well-Architected Tool on March 30, 2026, shows 5 high-risk issues, down from 25, and every one of the 25 HRIs agreed at the March 6 readout is closed or accepted in writing. Dev Raman: of the 25, 20 closed by change and were verified against live configuration and telemetry on March 30, and the 5 accepted in writing are the 5 that remain, as the readout said they would. None is unresolved. The second half of the fee is invoiced at the end of the week.

The two milestones the gate compares, on the 57 questions of the AWS Well-Architected Framework lens. The gate’s rule: Every agreed HRI is closed or accepted in writing, verified in milestone two.

Measure	Milestone one (March 6)	Milestone two (March 30)
High-risk issues	25	5
Medium-risk issues	21	19
No improvements identified	11	33
Agreed HRIs closed by change	0	20
Agreed HRIs accepted in writing	0	5
Agreed HRIs unresolved	25	0

The 19 MRIs are 12 that were medium at the baseline and are unchanged, and 7 HRIs whose high-risk part closed while a medium-risk part remains. And 9 questions that were medium at the baseline now have no improvements identified, because the HRI work fixed them too.



High-risk issues by pillar, milestone one against milestone two. The 5 left are the HRIs accepted in writing.

Pillar by pillar

Operational Excellence

5 high, 4 medium, and 2 with no improvements identified at milestone one; 0, 4, and 7 at milestone two.

The Operational Excellence HRIs agreed at the readout and their answers at milestone two.

HRI	Milestone two	What is in place now	Closed
OPS04 How do you implement observability in your workload?	Medium risk	Objectives are set for upload-to-timeline time and playback start. Traces cross the Lambda orchestrators, the collector, and the API, and burn-rate alarms page the on-call engineer. Closed March 20. Real-user telemetry from the mobile apps is not collected yet.	March 20, Kofi Brandvold
OPS05 How do you reduce defects, ease remediation, and improve flow into production?	No improvements identified	142 console-built resources were imported into the CDK by March 27, so production changes go through a pull request and the pipeline: in tp-prod the developer, machine learning, and data permission sets are read-only, the pipeline's role is the only routine writer, and CloudFormation drift detection reports a console change made through the platform administrator's permission set or the break-glass role. Staging still runs inside tp-prod until its rebuild in tp-staging and is covered by the same import.	March 27, Kofi Brandvold
OPS06 How do you mitigate deployment risks?	No improvements identified	EKS workloads deploy as canaries with automatic rollback on a failed health or error-rate check, and the EC2 tiers swap a target group with rollback on alarm. Closed March 25. Every change record states its rollback.	March 25, Kofi Brandvold
OPS07 How do you know that you are ready to support a workload?	No improvements identified	Runbooks and playbooks for the failures the team has already had live in the repository, an on-call rotation names a primary and a secondary each week, and a readiness checklist gates launches. Closed March 19.	March 19, Kofi Brandvold
OPS10 How do you manage workload and operations events?	No improvements identified	An incident process defines severity levels, an incident commander, an escalation path to Dev Raman and Noor Castellanos for the top severity, and a status message for newsroom customers. It was tested in the March 26 tabletop. Closed March 26.	March 26, Kofi Brandvold

Operational Excellence questions the Remediation fixed on the way.

Question	Medium risk at milestone one; now no improvements identified
OPS08 How do you utilize workload observability in your organization?	One dashboard per objective shows the symptom, the error budget, and the trace link, and alerts fire on burn rate. The platform team reviews them weekly.

Medium risk at milestone two: OPS02, OPS03, OPS04, OPS09. Each stays in the Tool's improvement plan; the handover report gives the best practices still open and an owner for each.

Security

2 high, 5 medium, and 4 with no improvements identified at milestone one; 0, 3, and 8 at milestone two.

The Security HRIs agreed at the readout and their answers at milestone two.

HRI	Milestone two	What is in place now	Closed
SEC07 How do you classify your data?	Medium risk	A data-class standard defines four classes (public news content, user personal data, contributor location, credentials) and a data-class tag is applied to every bucket, table, and database. Closed March 20. Classification is not automated, and the retention schedule waits on counsel.	March 20, Sasha Ilyin
SEC11 How do you incorporate and validate the security properties of applications throughout the design, development, and deployment lifecycle?	Medium risk	Dependency scanning and static analysis run in CI and block on high severity; the link-preview service has an SSRF test. Closed March 17. No penetration test has been run.	March 17, Marcus Oyelaran

Security questions the Remediation fixed on the way.

Question	Medium risk at milestone one; now no improvements identified
SEC05 How do you protect your network resources?	The new database launched private in the Sunday, March 22 cutover and the BI vendor moved to PrivateLink, which closed C-4.
SEC06 How do you protect your compute resources?	Nodes were replaced from patched images when the EKS node group grew to 12 and the cluster was upgraded (March 17 to March 19), so every volume is encrypted.
SEC08 How do you protect your data at rest?	The new PostgreSQL 16 instance is encrypted with a customer managed key; the old instance was retired after the March 22 cutover.
SEC10 How do you anticipate, respond to, and recover from incidents?	Playbooks cover credential exposure and a public bucket. The March 26 tabletop ran a leaked-access-key scenario with Sasha Ilyin as incident lead.

Medium risk at milestone two: SEC01, SEC07, SEC11. Each stays in the Tool's improvement plan; the handover report gives the best practices still open and an owner for each.

Reliability

8 high, 4 medium, and 1 with no improvements identified at milestone one; 0, 5, and 8 at milestone two.

The Reliability HRIs agreed at the readout and their answers at milestone two.

HRI	Milestone two	What is in place now	Closed
REL01 How do you manage Service Quotas and constraints?	No improvements identified	Quota alarms fire at 80% for Rekognition, SageMaker, and EC2 vCPUs, and the limits were raised with headroom for a zone failover. Closed March 13.	March 13, Kofi Brandvold
REL02 How do you plan your network topology?	No improvements identified	Private subnets in three zones, one NAT gateway per zone (1 to 3), and load balancers across all three. Closed March 10.	March 10, Kofi Brandvold
REL07 How do you design your workload to adapt to changes in demand?	Medium risk	Target tracking scales the API tier, Karpenter scales EKS nodes, and queue depth scales the transcoders. Closed March 17. Only the ranking endpoint has been load tested (March 18); the API tier has no full-path load test.	March 17, Kofi Brandvold
REL09 How do you back up data?	No improvements identified	AWS Backup takes recovery points in tp-prod and copies them cross-account to the vault in tp-backup (vault lock in compliance mode) and DynamoDB point-in-time recovery is on, both from March 10. The March 24 restore test took 52 minutes against a 4-hour objective. Closed March 24.	March 24, Kofi Brandvold
REL10 How do you use fault isolation to protect your workload?	No improvements identified	The API tier (6 to 9 c6i.4xlarge), the EKS node group (9 to 12 m5.4xlarge), the NAT gateways (1 to 3), Redis, OpenSearch, and RDS span three zones or two (RDS Multi-AZ). The March 25 zone evacuation drill took one zone out of service without an outage. Closed March 25.	March 25, Kofi Brandvold
REL11 How do you design your workload to withstand component failures?	No improvements identified	Redis shards have replicas in a second zone, OpenSearch has 3 dedicated master nodes, RDS fails over to a Multi-AZ standby, and instance health checks replace failed EC2 nodes. Closed March 22.	March 22, Kofi Brandvold
REL12 How do you test reliability?	Medium risk	Playbooks exist, and the March 25 zone drill and the March 24 restore test are the first game days. Closed March 25. The drills used manual failover; fault injection with AWS FIS was considered and not priced.	March 25, Kofi Brandvold

HRI	Milestone two	What is in place now	Closed
REL13 How do you plan for disaster recovery (DR)?	Medium risk	The plan sets objectives by scope. Inside us-east-1, a 15-minute recovery point for the database and a 4-hour recovery time for the Brief, the recovery time proved by the March 24 restore in 52 minutes. For the loss of the Region, a recovery point of up to 24 hours, because the database and DynamoDB backups are copied to us-west-2 once a day, and a recovery time that stays unproven until the regional runbook runs. Closed March 24. The originals bucket is not copied to a second Region.	March 24, Dev Raman

Reliability questions the Remediation fixed on the way.

Question	Medium risk at milestone one; now no improvements identified
RELO6 How do you monitor workload resources?	Alarms notify the on-call engineer from the objective dashboards, and traces follow a request from the API through the orchestrators.
RELO8 How do you implement change?	Production changes go through a pull request and the pipeline, with runbooks for the standard changes and the 142 imported resources in the CDK; in tp-prod the developer, machine learning, and data permission sets are read-only, the pipeline's role is the only routine writer, and CloudFormation drift detection reports a console change made through the platform administrator's permission set or the break-glass role.

Medium risk at milestone two: RELO4, RELO5, RELO7, REL12, REL13. Each stays in the Tool's improvement plan; the handover report gives the best practices still open and an owner for each.

Performance Efficiency

2 high, 2 medium, and 1 with no improvements identified at milestone one; 1, 1, and 3 at milestone two.

The Performance Efficiency HRIs agreed at the readout and their answers at milestone two.

HRI	Milestone two	What is in place now	Closed
PERF02 How do you select and use compute resources in your workload?	No improvements identified	After a load test on March 18 (p99 38 ms against a 50 ms budget) the endpoint moved to 6 ml.c6i.2xlarge. The embedding endpoint and the notebooks are sized by the cost engagement. Closed.	March 18, Yuki Sorensen
PERF03 How do you store, manage, and access data in your workload?	High risk	Telemetry lands as raw JSON and Athena reads it without partition pruning or a columnar format, so each query scans far more than it needs.	Accepted in writing March 9 by Lior Haddad

Performance Efficiency questions the Remediation fixed on the way.

Question	Medium risk at milestone one; now no improvements identified
PERF01 How do you select appropriate cloud resources and architecture for your workload?	The load-test method used for the ranking endpoint (March 18) is the written standard for resource choices.

Medium risk at milestone two: PERF04. Each stays in the Tool's improvement plan; the handover report gives the best practices still open and an owner for each.

Cost Optimization

6 high, 3 medium, and 2 with no improvements identified at milestone one; 2, 4, and 5 at milestone two.

The Cost Optimization HRIs agreed at the readout and their answers at milestone two.

HRI	Milestone two	What is in place now	Closed
COST01 How do you implement cloud financial management?	No improvements identified	A monthly cost review is owned by Gwen Tallis and Kofi Brandvold; the first was held March 17. Closed.	March 17, Gwen Tallis
COST02 How do you govern usage?	No improvements identified	Budgets and Cost Anomaly Detection run per account, and a spend-per-active-user target is set in the monthly review. Closed March 13.	March 13, Gwen Tallis
COST03 How do you monitor usage and cost?	Medium risk	The Cost and Usage Report export has run in tp-management since January 28, and cost allocation tags (team, environment, service) were activated March 11. Closed. Costs are not yet allocated per video or per active user.	March 11, Kofi Brandvold
COST04 How do you decommission resources?	No improvements identified	A decommissioning runbook, an owner tag on every resource, and a monthly review of unattached resources are in place. Closed March 19.	March 19, Kofi Brandvold
COST06 How do you meet cost targets when you select resource type, size and number?	High risk	Compute was sized once, at launch. The embedding endpoint uses one of four GPUs on its ml.g5.12xlarge instances, notebooks never stop, and the EC2 fleet is On-Demand and never resized.	Accepted in writing March 10 by Gwen Tallis
COST07 How do you use pricing models to reduce cost?	High risk	Everything is On-Demand: no Savings Plan, no Reserved Instance, no Spot. AWS Activate credits ran out in June 2025.	Accepted in writing March 10 by Gwen Tallis

Medium risk at milestone two: COST03, COST05, COST08, COST09. Each stays in the Tool's improvement plan; the handover report gives the best practices still open and an owner for each.

Sustainability

2 high, 3 medium, and 1 with no improvements identified at milestone one; 2, 2, and 2 at milestone two.

The Sustainability HRIs agreed at the readout and their answers at milestone two.

HRI	Milestone two	What is in place now	Closed
SUS02 How do you align cloud resources to your demand?	High risk	The API tier, EKS nodes, and transcoders now scale with load, but the GPU endpoints, the notebooks, and the developer instances still do not.	Accepted in writing March 11 by Yuki Sorensen
SUS04 How do you take advantage of data management policies and patterns to support your sustainability goals?	High risk	The data-class standard of March 20 classifies the data, but nothing expires yet.	Accepted in writing March 9 by Lior Haddad

Sustainability questions the Remediation fixed on the way.

Question	Medium risk at milestone one; now no improvements identified
SUS06 How do your organizational processes support your sustainability goals?	Production left PostgreSQL 13 in the March 22 cutover and left extended support on EKS, upgraded to 1.33, on March 19. Staging stays on both until it is retired.

Medium risk at milestone two: SUS03, SUS05. Each stays in the Tool’s improvement plan; the handover report gives the best practices still open and an owner for each.

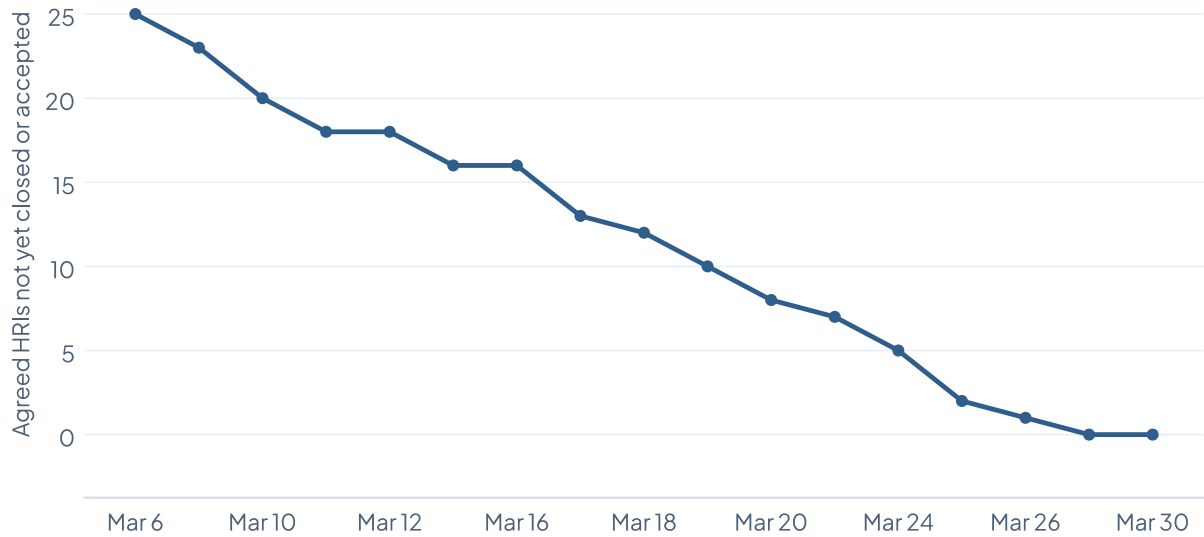
What the drills proved

Every reliability claim in milestone two rests on a test run in week five, not on configuration alone.

The week–five tests behind milestone two. The recovery objectives they were measured against are the in–Region ones: a 15–minute recovery point for the database and a 4–hour recovery time inside us–

east-1. For a Region loss the recovery point is up to 24 hours and the recovery time is unproven until the regional runbook runs.

Test	When	What it showed
PostgreSQL 16 Multi-AZ cutover	Sunday, March 22, 2:00 to 2:14 AM CDT	Writes paused for 14 minutes while the new encrypted, private, Multi-AZ instance took over from PostgreSQL 13; it closed C-4, H-1, REL10 (database part)
Restore from AWS Backup	March 24	The database, volumes, and DynamoDB tables restored in 52 minutes against a 4-hour objective
Availability Zone evacuation	March 25	One zone taken out of service with no outage; failover was manual, not injected
Incident tabletop	March 26	The incident process run end to end: severity, commander, escalation, and the customer message
CDK import	March 27	142 console-built resources now in tidepost-cdk, each one changed only through a pull request



Agreed HRIs still open, weekday by weekday. The five acceptances, signed March 9 to March 11, and the network and backup work came first.

The five that remain

The 5 HRIs accepted in writing are still high risk in the Tool, and they will be until their changes land. Each fix is a cost change, so the cost engagement, which starts on April 6, 2026, prices and schedules all five at its readout on April 17 and counts each change once.

The acceptances the gate counts as closed.

HRI	Accepted by	On	Risk while it waits
PERF03 How do you store, manage, and access data in your workload?	Lior Haddad	March 9	Each Athena query keeps scanning raw JSON.
COST06 How do you meet cost targets when you select resource type, size and number?	Gwen Tallis	March 10	Oversized compute keeps running at its current size.
COST07 How do you use pricing models to reduce cost?	Gwen Tallis	March 10	Everything keeps billing at On-Demand rates.
SUS02 How do you align cloud resources to your demand?	Yuki Sorensen	March 11	GPU endpoints and notebooks keep running around the clock.
SUS04 How do you take advantage of data management policies and patterns to support your sustainability goals?	Lior Haddad	March 9	Logs, the telemetry stream, and raw telemetry keep growing without limit.

What the milestone cost

The Remediation raised the monthly bill by a net \$10,094 at list, the price of running the Brief in more than one zone. It added \$10,300 a month (replicas, standbys, the second and third zones, backups) and removed \$790 (the ranking endpoint off GPUs and the production EKS cluster out of extended support), and production’s PostgreSQL 13 Extended Support, \$2,336 a month, stopped at the cutover. Staging’s \$584 a month continues until Tidepost retires it. Waiting for the cutover rather than upgrading the single-AZ writer in place the week of the readout cost production about \$1,160 of Extended Support, the choice the readout recommended.

© 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.