



AWS WELL-ARCHITECTED FRAMEWORK REVIEW · SAMPLE DELIVERABLE

Six-Pillar Review: Every Question, Its Evidence, and the HRI and MRI Register

Week 2 of 6: Review · prepared for Tidepost, Inc.

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

March 5, 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
How the questions were answered	3
The scorecard	4
The six pillars, question by question	6
Operational Excellence	6
Security	8
Reliability	9
Performance Efficiency	11
Cost Optimization	12
Sustainability	13
The register of high-risk issues	14
The register of medium-risk issues	17
The roadmap by week	22
Decisions to take at the readout	22

Summary

25 of the 57 questions are high-risk issues, 21 are medium-risk issues, and 11 identify no improvements. Dev Raman, Kofi Brandvold, Sasha Ilyin, Yuki Sorensen, Lior Haddad, Amara Delacroix, and Gwen Tallis: this is the Review's finding for the Brief across the six pillars of the AWS Well-Architected Framework lens, with the evidence behind every answer, the register of high-risk issues (HRIs) with a proposed fix, an owner, and a week for each, and the improvement plan of medium-risk issues (MRIs).

Reliability carries the most high-risk issues (8 of its 13 questions). The Security pillar starts with 2, because the security engagement closed the critical exposures first.

We propose that 20 of the 25 HRIs close in weeks three to five, the last on March 27: 16 by a change that Tidepost's engineers ship through pull requests in `tidepost-cdk`, and 4 (OPS07, OPS10, COST01, and SEC07) by a runbook, a process, or a standard that the owner writes and adopts. The other 5 have a fix that is a cost change; we propose at the readout that each be

accepted in writing, so that the cost engagement (April 6 to May 15, readout April 17) takes the change up once, and no engagement counts it twice. The scorecard and the registers are for decision at the sponsor readout on March 6.

The scorecard in numbers. The answers are saved as milestone one at the readout on March 6.

Milestone one at a glance	Result
Questions answered (Well-Architected Framework lens)	57
High risk	25
Medium risk	21
No improvements identified	11
Best practices not selected, in all	102
HRIs proposed to close by a change in code	20
HRIs proposed for acceptance in writing	5
Last proposed close by change	March 27
Sponsor readout (milestone one is saved)	March 6
Milestone two, the gate (scheduled)	March 30

How the questions were answered

Every answer rests on evidence we read, not on a view of how Tidepost works. Each of the 57 questions in the Well-Architected Framework lens lists best practices. We selected the ones that are in place for the Brief; the Tool calls a question **High risk** when important best practices are missing, **Medium risk** when some are, and **No improvements identified** when none are. We recorded in the Tool's notes the evidence for each answer, and the best practices not selected.

- **Evidence.** The read-only inspection role in tp-prod, CloudWatch, billing data, the tidepost-cdk repository, and the 4 sessions held before today (listed below), as set out in the week-one report.
- **The Machine Learning Lens** is read for context. Its questions are not answered and nothing in it is counted.
- **Scope.** The Brief only. Staging, developer instances, and the data science sandbox are out of the workload.

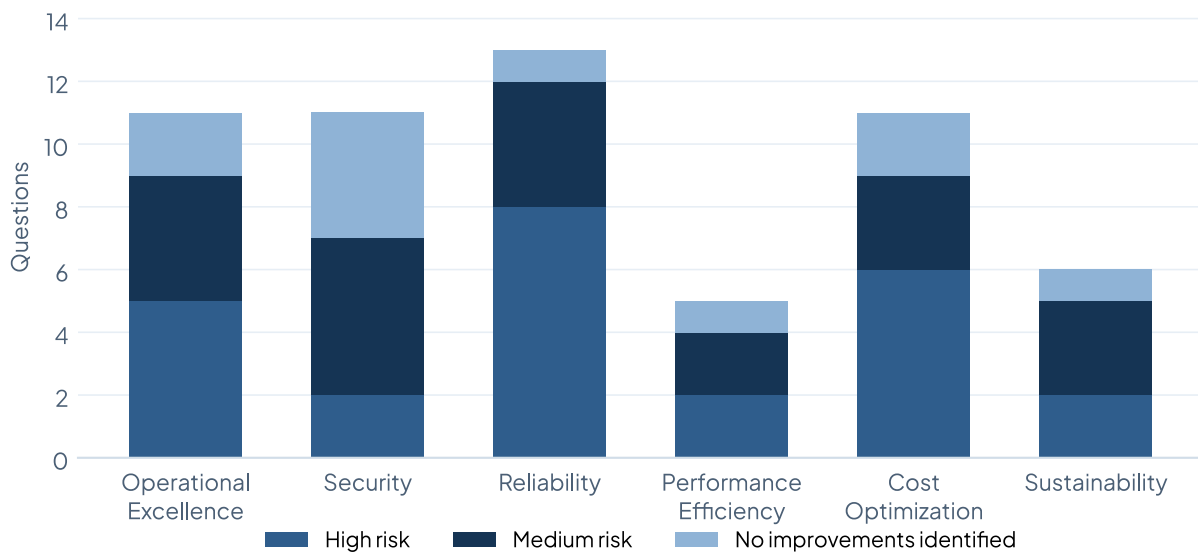
- **Access.** Vantalect works through a read-only role and writes nothing to production. The only thing we record in Tidepost's account is the workload in Tidepost's own Well-Architected Tool. Every fix below lands as a pull request in tidepost-cdk (or in Tidepost's console where noted), reviewed by the owning engineer and shipped by Tidepost's pipeline.

The Review's sessions. The two in week two take the answers to the engineers and then to the sponsor.

Date	Session	MinutesWho	Status
February 23	Kickoff	60Dev Raman, Kofi Brandvold, Yuki Sorensen, Lior Haddad, Amara Delacroix, Marcus Oyelaran	Held
February 24	Architecture and reliability session	90Kofi Brandvold, Marcus Oyelaran, Yuki Sorensen, Lior Haddad, Amara Delacroix	Held
February 25	Security and operations session	90Sasha Ilyin, Kofi Brandvold, Marcus Oyelaran	Held
February 26	Performance, cost, and sustainability session	60Kofi Brandvold, Yuki Sorensen, Lior Haddad, Gwen Tallis	Held
March 5	HRI and roadmap review	90Kofi Brandvold, Marcus Oyelaran, Yuki Sorensen, Lior Haddad, Amara Delacroix, Sasha Ilyin, Gwen Tallis	Today
March 6	Sponsor readout	60Dev Raman, Noor Castellanos, Kofi Brandvold, Gwen Tallis	Scheduled

The scorecard

Reliability and Cost Optimization together hold 14 of the 25 high-risk issues. Each pillar's questions are scored on their own; the totals add across the six.



Risk by pillar at milestone one. Each bar sums to the number of questions in the pillar.

The six-pillar scorecard at milestone one, from the answers recorded in the Tool.

Pillar	Questions	High risk	Medium risk	No improvements identified
Operational Excellence	11	5	4	2
Security	11	2	5	4
Reliability	13	8	4	1
Performance Efficiency	5	2	2	1
Cost Optimization	11	6	3	2
Sustainability	6	2	3	1
Total	57	25	21	11

The six pillars, question by question

Every one of the 57 questions is below, with its risk, the evidence behind it, and the best practices we did not select. The appendix repeats each answer with the name of every best practice not selected and the notes recorded in the Tool.

Operational Excellence

Of 11 questions, 5 are high-risk issues, 4 are medium-risk issues, and 2 identify no improvements. The HRIs are OPS04, OPS05, OPS06, OPS07, OPS10.

The Operational Excellence pillar at milestone one: 11 questions.

Question	Risk	Evidence	Best practices not selected
OPS01 How do you determine what your priorities are?	No improvements identified	Priorities are written down and ranked: the Series A conditions (every critical finding closed, a SOC 2 Type 2 report within nine months), the 18 newsroom customers whose vendor reviews ask for one, and the exposures the security engagement found. Dev Raman signs risk acceptances and, by a written delegation, lets the heads of data, machine learning, and finance (Lior Haddad, Yuki Sorensen, and Gwen Tallis) sign those inside their own areas; Noor Castellanos signs any above her monthly threshold.	None
OPS02 How do you structure your organization to support your business outcomes?	Medium risk	Workload owners are named for each part of the Brief (Marcus Oyelaran for the API and web tier, Yuki Sorensen for ranking and embedding, Lior Haddad for telemetry, Amara Delacroix for moderation, Kofi Brandvold for the platform). The tag policy of February 10 adds an owner tag, but resources created before it carry none outside the accounts the Foundation tagged. The platform team is 2 engineers, and hand-offs between platform and the machine learning team are agreed in conversation, not written down.	OPS02-BP01, OPS02-BP07
OPS03 How does your organizational culture support your business outcomes?	Medium risk	Executive sponsorship is visible: Dev Raman sponsors all four engagements and attends every readout. Engineers can stop a release. Escalation and staffing are thin: 2 platform engineers carry every change window, the network, EKS, and every page that arrives after hours.	OPS03-BP04, OPS03-BP07

Question	Risk	Evidence	Best practices not selected
OPS04 How do you implement observability in your workload?	High risk	Custom metrics and logs are collected, but nothing measures what a contributor or reader feels: no objective for upload-to-timeline time or playback start, no tracing across the Lambda orchestrators, the EKS collector, and the API, and alarms exist on host CPU only.	OPS04-BP01, OPS04-BP02, OPS04-BP03, OPS04-BP05
OPS05 How do you reduce defects, ease remediation, and improve flow into production?	High risk	About half of the estate was built in the console: the moderation pipeline, the data stores, and the network. Application code is in version control, but the infrastructure under it cannot be reviewed, tested, or rebuilt from a repository.	OPS05-BP03, OPS05-BP10
OPS06 How do you mitigate deployment risks?	High risk	The API and web tier deploy by rolling replacement from CI and are rolled back by hand; EKS workloads apply manifests directly. No change has a written rollback plan.	OPS06-BP01, OPS06-BP03, OPS06-BP04
OPS07 How do you know that you are ready to support a workload?	High risk	Business Support+ is in place, but there are no runbooks, no playbooks for the failures the team has already had, and no readiness review before launches. Only security findings page anyone, the two responders the security engagement named (Sasha Ilyin first, Kofi Brandvold second); the workload itself has no on-call rotation.	OPS07-BP02, OPS07-BP03, OPS07-BP04
OPS08 How do you utilize workload observability in your organization?	Medium risk	Logs and metrics are searched after an incident. Alerts fire on CPU, not on user-visible symptoms, and there are no shared dashboards.	OPS08-BP04, OPS08-BP05
OPS09 How do you understand the health of your operations?	Medium risk	Availability is the only operations goal, and it is read from a hosting dashboard. There is no operations review and no status shared with the business.	OPS09-BP02, OPS09-BP03
OPS10 How do you manage workload and operations events?	High risk	Incidents are handled in a shared chat channel. There are no severity levels, no escalation path, and no way to tell newsroom customers that something is wrong.	OPS10-BP01, OPS10-BP04, OPS10-BP05
OPS11 How do you evolve operations?	No improvements identified	A post-incident review was written after the July 14, 2025 graphic-video incident (it added the second moderation path), and lessons are kept in the engineering wiki. Platform improvements are scheduled in the weekly planning meeting.	None

Security

Of 11 questions, 2 are high-risk issues, 5 are medium-risk issues, and 4 identify no improvements. The HRIs are SEC07, SEC11.

The Security pillar at milestone one: 11 questions.

Question	Risk	Evidence	Best practices not selected
SEC01 How do you securely operate your workload?	Medium risk	Root keys were deleted January 6 and root credentials removed January 29. Production is one of nine accounts under service control policies. The staging copy still runs inside tp-prod, and the data stores have not moved to their own accounts.	SEC01-BP01
SEC02 How do you manage authentication for people and machines?	No improvements identified	People sign in through IAM Identity Center with MFA (from January 26), and no human IAM user remains after February 10. Secrets are in Secrets Manager (January 9); CI assumes roles through OIDC federation; workloads use instance and pod roles.	None
SEC03 How do you manage permissions for people and machines?	No improvements identified	Permission sets map to roles in Identity Center, service control policies and a resource control policy set the data perimeter, and IAM Access Analyzer in tp-audit reports public and cross-account access. The link-preview instance role was cut to 14 actions on January 8 (C-6).	None
SEC04 How do you detect and investigate security events?	No improvements identified	The organization trail and AWS Config history are in tp-log-archive from January 28 and kept 400 days. GuardDuty and Security Hub are delegated to tp-audit, and High and Critical findings page the two named security responders (Sasha Ilyin first, Kofi Brandvold second) by SMS, as the security engagement set up in February.	None
SEC05 How do you protect your network resources?	Medium risk	WAF protects the API and the data stores are private, with one exception: the production database is still publicly reachable from the BI vendor's four published ranges with TLS required, accepted in writing by Dev Raman (C-4) until the cutover.	SEC05-BP02

Question	Risk	Evidence	Best practices not selected
SEC06 How do you protect your compute resources?	Medium risk	Amazon Inspector has run on EC2 and ECR since January 29, and IMDSv2 is required. Some EKS nodes and EC2 volumes predate default encryption and are patched by hand.	SEC06–BP04
SEC07 How do you classify your data?	High risk	Nothing is classified. User location (EXIF), contributor records, credentials, and public news content are handled alike.	SEC07–BP01, SEC07–BP02, SEC07–BP04
SEC08 How do you protect your data at rest?	Medium risk	S3 default encryption and EBS default encryption are on. The production PostgreSQL 13 database is not encrypted, and encryption cannot be added in place (H-1).	SEC08–BP02
SEC09 How do you protect your data in transit?	No improvements identified	TLS is required on every public endpoint, certificates are in ACM, and the database has required TLS since January 7 (C-4).	None
SEC10 How do you anticipate, respond to, and recover from incidents?	Medium risk	Counsel and the CTO know whom to call, but there are no security playbooks and no one has rehearsed one.	SEC10–BP04, SEC10–BP07
SEC11 How do you incorporate and validate the security properties of applications throughout the design, development, and deployment lifecycle?	High risk	No dependency scanning or static analysis runs in CI, and code review is the only check. The link-preview SSRF (C-6) reached an administrator role.	SEC11–BP01, SEC11–BP02, SEC11–BP03, SEC11–BP08

Reliability

Of 13 questions, 8 are high-risk issues, 4 are medium-risk issues, and 1 identifies no improvements. The HRIs are RELO1, RELO2, RELO7, RELO9, REL10, REL11, REL12, REL13.

The Reliability pillar at milestone one: 13 questions.

Question	Risk	Evidence	Best practices not selected
REL01 How do you manage Service Quotas and constraints?	High risk	Recognition throughput limits were reached at peak upload times, and nobody tracks quotas or sets alarms on them.	REL01–BP01, REL01–BP04, REL01–BP05
REL02 How do you plan your network topology?	High risk	One NAT gateway and every tier in one Availability Zone; the load balancers and subnets span no second zone.	REL02–BP01, REL02–BP03
REL03 How do you design your workload service architecture?	No improvements identified	The Brief is segmented by business function (upload, moderation, embedding, ranking, timeline, playback), and each API has a written contract.	None
REL04 How do you design interactions in a distributed system to prevent failures?	Medium risk	The moderation pipeline is a chain of Lambda orchestrators that call each other, so a failure in a late step leaves an upload half moderated.	REL04–BP02
REL05 How do you design interactions in a distributed system to mitigate or withstand failures?	Medium risk	Clients have timeouts. If the ranking endpoint is unavailable, the API returns errors instead of a cached or chronological timeline, and write traffic is not throttled.	REL05–BP01, REL05–BP02
REL06 How do you monitor workload resources?	Medium risk	Host metrics are collected, alarms are few, and a request cannot be followed across services.	REL06–BP03, REL06–BP07
REL07 How do you design your workload to adapt to changes in demand?	High risk	The API tier, EKS nodes, and transcoders are fixed in size, and election-week traffic was met by hand.	REL07–BP01, REL07–BP03, REL07–BP04
REL08 How do you implement change?	Medium risk	Deployments are scripted partly and run from a laptop in some cases; infrastructure changes are made in the console.	REL08–BP01, REL08–BP05
REL09 How do you back up data?	High risk	RDS keeps automated snapshots only. An EBS snapshot cron job never deletes, DynamoDB has no point-in-time recovery, and no restore has ever been tested.	REL09–BP03, REL09–BP04
REL10 How do you use fault isolation to protect your workload?	High risk	Every stateful service and every EC2 tier sits in one Availability Zone.	REL10–BP01, REL10–BP03

Question	Risk	Evidence	Best practices not selected
REL11 How do you design your workload to withstand component failures?	High risk	Redis, OpenSearch, and RDS have no standby; a failed node means manual recovery.	REL11-BP02, REL11-BP03
REL12 How do you test reliability?	High risk	No failure has ever been rehearsed and there are no playbooks for the failures the team has seen.	REL12-BP01, REL12-BP05, REL12-BP06
REL13 How do you plan for disaster recovery (DR)?	High risk	No recovery objectives are defined, there is nothing outside us-east-1, and recovery has never been tested.	REL13-BP01, REL13-BP02, REL13-BP03

Performance Efficiency

Of 5 questions, 2 are high-risk issues, 2 are medium-risk issues, and 1 identifies no improvements. The HRIs are PERFO2, PERFO3.

The Performance Efficiency pillar at milestone one: 5 questions.

Question	Risk	Evidence	Best practices not selected
PERF01 How do you select appropriate cloud resources and architecture for your workload?	Medium risk	Instance families were chosen at launch and not benchmarked since. The ranking endpoint on GPUs sat at 9% GPU utilization.	PERF01-BP06, PERF01-BP07
PERF02 How do you select and use compute resources in your workload?	High risk	The ranking endpoint runs on 2 ml.g5.2xlarge instances at 9% GPU utilization, chosen without a test.	PERF02-BP03, PERF02-BP04
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.	PERF03-BP03, PERF03-BP04
PERF04 How do you select and configure networking resources in your workload?	Medium risk	CloudFront serves renditions and originals through origin access control since January 6. The video rendition ladder is fixed in the app, and network settings are not tuned from metrics.	PERF04-BP05, PERF04-BP07
PERF05 What process do you use to support more performance efficiency for your workload?	No improvements identified	The API's p99 latency and playback start time are tracked, the team reviews them before releases, and load tests are run for the changes that need them.	None

Cost Optimization

Of 11 questions, 6 are high-risk issues, 3 are medium-risk issues, and 2 identify no improvements. The HRIs are COST01, COST02, COST03, COST04, COST06, COST07.

The Cost Optimization pillar at milestone one: 11 questions.

Question	Risk	Evidence	Best practices not selected
COST01 How do you implement cloud financial management?	High risk	Nobody owns AWS cost. Finance receives the invoice, and engineering is not shown it.	COST01-BP01, COST01-BP02, COST01-BP03
COST02 How do you govern usage?	High risk	One account, no budgets, no anomaly detection, and no limit on who launches what.	COST02-BP01, COST02-BP05
COST03 How do you monitor usage and cost?	High risk	Most resources carry no tag, there is no Cost and Usage Report, and cost cannot be attributed to a team.	COST03-BP01, COST03-BP03, COST03-BP06
COST04 How do you decommission resources?	High risk	A forgotten GPU instance with an open Jupyter server, three departed employees' keys, unattached volumes, and a snapshot job that never deletes all went unnoticed.	COST04-BP01, COST04-BP02, COST04-BP03
COST05 How do you evaluate cost when you select services?	Medium risk	Services were chosen for speed to launch. Every video is moderated twice, and every post goes to Transcribe and Comprehend.	COST05-BP02, COST05-BP06
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.	COST06-BP01, COST06-BP02, COST06-BP03
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.	COST07-BP01, COST07-BP04
COST08 How do you plan for data transfer charges?	Medium risk	Data transfer was never modeled. One NAT gateway, in one zone, carries all private egress.	COST08-BP01, COST08-BP03

Question	Risk	Evidence	Best practices not selected
COST09 How do you manage demand, and supply resources?	Medium risk	Capacity is fixed at the launch-event peak for every tier.	COST09-BP03
COST10 How do you evaluate new services?	No improvements identified	New AWS services and features are reviewed in the platform team's weekly meeting, and adoption goes through a pull request.	None
COST11 How do you evaluate the cost of effort?	No improvements identified	Managed services are used wherever the 2-engineer platform team would otherwise run the software, and build-versus-buy is a recorded decision.	None

Sustainability

Of 6 questions, 2 are high-risk issues, 3 are medium-risk issues, and 1 identifies no improvements. The HRIs are SUS02, SUS04.

The Sustainability pillar at milestone one: 6 questions.

Question	Risk	Evidence	Best practices not selected
SUS01 How do you select Regions to support your sustainability goals?	No improvements identified	us-east-1 was chosen for latency to the user base and service availability. The Foundation's design compared Regions, and us-west-2 holds backup copies only.	None
SUS02 How do you align cloud resources to your demand?	High risk	GPU endpoints and notebooks run all day and night, and every developer instance runs around the clock.	SUS02-BP01, SUS02-BP03, SUS02-BP05
SUS03 How do you take advantage of software and architecture patterns to support your sustainability goals?	Medium risk	Uploads are processed asynchronously and scheduled work runs off-peak, but the frame-sampling path duplicates the whole-video moderation path.	SUS03-BP02
SUS04 How do you take advantage of data management policies and patterns to support your sustainability goals?	High risk	Nothing expires: logs, the telemetry stream, and the raw telemetry have no retention, and nothing is classified.	SUS04-BP01, SUS04-BP03, SUS04-BP05
SUS05 How do you select and use cloud hardware and services in your architecture to support your sustainability goals?	Medium risk	Stateless tiers run on Intel instances where Graviton would do, and the GPU accelerators are mostly idle.	SUS05-BP02, SUS05-BP04
SUS06 How do your organizational processes support your sustainability goals?	Medium risk	Production runs PostgreSQL 13 and EKS 1.30, both past standard support.	SUS06-BP02

The register of high-risk issues

All 25 HRIs, each with a proposed fix, an owner, and the week it is planned for. The gate in the engagement terms: Every agreed HRI is closed or accepted in writing, verified in milestone two. Milestone two is scheduled for March 30.

The HRI register on March 5, 2026. "Planned" is the day the fix is scheduled to land, or for the five acceptances, the day the signer is asked to sign.

Question	Proposed fix	Owner	Planned
OPS04 How do you implement observability in your workload?	Service-level objectives for upload-to-timeline time and playback start, with tracing and burn-rate alarms	Kofi Brandvold	Week 4, March 20
OPS05 How do you reduce defects, ease remediation, and improve flow into production?	Import the console-built resources (the moderation pipeline, the data stores, and the network) into the CDK	Kofi Brandvold	Week 5, March 27
OPS06 How do you mitigate deployment risks?	Canary deploys with automatic rollback on EKS, and a target-group swap with rollback on the EC2 tiers	Kofi Brandvold	Week 5, March 25
OPS07 How do you know that you are ready to support a workload?	Runbooks, playbooks, and an on-call rotation with a primary and a secondary	Kofi Brandvold	Week 4, March 19
OPS10 How do you manage workload and operations events?	An incident process (severity levels, commander, escalation, customer message), tested in a tabletop	Kofi Brandvold	Week 5, March 26
SEC07 How do you classify your data?	A data-class standard, with a data-class tag on every bucket, table, and database	Sasha Ilyin	Week 4, March 20
SEC11 How do you incorporate and validate the security properties of applications throughout the design, development, and deployment lifecycle?	Dependency scanning and static analysis in CI, blocking on high severity	Marcus Oyelaran	Week 4, March 17
REL01 How do you manage Service Quotas and constraints?	Quota alarms, and raised limits for Rekognition, SageMaker, and EC2 vCPUs	Kofi Brandvold	Week 3, March 13
REL02 How do you plan your network topology?	Subnets and NAT gateways in three zones	Kofi Brandvold	Week 3, March 10
REL07 How do you design your workload to adapt to changes in demand?	Target tracking on the API, Karpenter on EKS, and queue-depth scaling for the transcoders	Kofi Brandvold	Week 4, March 17

Question	Proposed fix	Owner	Planned
REL09 How do you back up data?	AWS Backup to tp-backup with vault lock, DynamoDB point-in-time recovery, and a timed restore test	Kofi Brandvold	Week 5, March 24
REL10 How do you use fault isolation to protect your workload?	The API tier, EKS nodes, NAT, Redis, OpenSearch, and RDS across zones, proved by a zone evacuation drill	Kofi Brandvold	Week 5, March 25
REL11 How do you design your workload to withstand component failures?	Redis replicas, OpenSearch dedicated masters, and RDS Multi-AZ failover, completed by the PostgreSQL 16 cutover	Kofi Brandvold	Week 4, March 22
REL12 How do you test reliability?	Playbooks, and the zone drill and the restore test run as game days	Kofi Brandvold	Week 5, March 25
REL13 How do you plan for disaster recovery (DR)?	A recovery plan with written recovery point and recovery time objectives, and database and DynamoDB backups copied to us-west-2	Dev Raman	Week 5, March 24
PERF02 How do you select and use compute resources in your workload?	Move the ranking endpoint off GPUs if a load test shows CPU instances meet its latency budget	Yuki Sorensen	Week 4, March 18
PERF03 How do you store, manage, and access data in your workload?	Store raw telemetry in a columnar, partitioned format and point Athena at it, so a query reads only the columns and days it needs. Proposed for acceptance in writing at the readout. While it waits: Each Athena query keeps scanning raw JSON.	Lior Haddad, who signs the acceptance	Week 3, March 9, signature
COST01 How do you implement cloud financial management?	A monthly cost review owned by Gwen Tallis and Kofi Brandvold	Gwen Tallis	Week 4, March 17
COST02 How do you govern usage?	Budgets and Cost Anomaly Detection per account	Gwen Tallis	Week 3, March 13
COST03 How do you monitor usage and cost?	Cost allocation tags activated (team, environment, service)	Kofi Brandvold	Week 3, March 11
COST04 How do you decommission resources?	A decommissioning runbook, an owner tag on every resource, and a monthly unattached-resource review	Kofi Brandvold	Week 4, March 19

Question	Proposed fix	Owner	Planned
COST06 How do you meet cost targets when you select resource type, size and number?	Size the GPU endpoints, the notebooks, and the EC2 tiers to measured use. Proposed for acceptance in writing at the readout. While it waits: Oversized compute keeps running at its current size.	Gwen Tallis, who signs the acceptance	Week 3, March 10, signature
COST07 How do you use pricing models to reduce cost?	Commit to a Savings Plan for the steady compute once it is sized, so the commitment fits what runs. Proposed for acceptance in writing at the readout. While it waits: Everything keeps billing at On-Demand rates.	Gwen Tallis, who signs the acceptance	Week 3, March 10, signature
SUS02 How do you align cloud resources to your demand?	Scale the GPU endpoints and notebooks to demand instead of running them around the clock. Proposed for acceptance in writing at the readout. While it waits: GPU endpoints and notebooks keep running around the clock.	Yuki Sorensen, who signs the acceptance	Week 3, March 11, signature
SUS04 How do you take advantage of data management policies and patterns to support your sustainability goals?	Set retention on application logs, the telemetry stream, raw telemetry, and the originals. Proposed for acceptance in writing at the readout. While it waits: Logs, the telemetry stream, and raw telemetry keep growing without limit.	Lior Haddad, who signs the acceptance	Week 3, March 9, signature

The five acceptances. PERF03, COST06, COST07, SUS02, SUS04 have a fix that is a cost change: resizing, a commitment, retention, or a data format. The cost engagement prices and schedules each one, and counts each change exactly once. We propose that the named owner accept each risk in writing between March 9 and March 11, and that the cost engagement take them up at its readout on April 17. A risk accepted in writing counts as closed for the gate. In the Tool, the question stays High risk until the change lands, so it still shows as an HRI after it is accepted.

The register of medium-risk issues

21 MRIs, kept as the improvement plan. They are outside the guarantee and are not required to close. We list them so that Tidepost's own reviews can take them in order, with the best practices that would close each.

The 21 medium-risk issues at milestone one, with 34 best practices not selected between them.

Question	Pillar	Evidence	Best practices not selected
OPS02 How do you structure your organization to support your business outcomes?	Operational Excellence	Workload owners are named for each part of the Brief (Marcus Oyelaran for the API and web tier, Yuki Sorensen for ranking and embedding, Lior Haddad for telemetry, Amara Delacroix for moderation, Kofi Brandvold for the platform). The tag policy of February 10 adds an owner tag, but resources created before it carry none outside the accounts the Foundation tagged. The platform team is 2 engineers, and hand-offs between platform and the machine learning team are agreed in conversation, not written down.	OPS02-BP01 Resources have identified owners; OPS02-BP07 Responsibilities between teams are predefined or negotiated
OPS03 How does your organizational culture support your business outcomes?	Operational Excellence	Executive sponsorship is visible: Dev Raman sponsors all four engagements and attends every readout. Engineers can stop a release. Escalation and staffing are thin: 2 platform engineers carry every change window, the network, EKS, and every page that arrives after hours.	OPS03-BP04 Communications are timely, clear, and actionable; OPS03-BP07 Resource teams appropriately
OPS08 How do you utilize workload observability in your organization?	Operational Excellence	Logs and metrics are searched after an incident. Alerts fire on CPU, not on user-visible symptoms, and there are no shared dashboards.	OPS08-BP04 Create actionable alerts; OPS08-BP05 Create dashboards
OPS09 How do you understand the health of your operations?	Operational Excellence	Availability is the only operations goal, and it is read from a hosting dashboard. There is no operations review and no status shared with the business.	OPS09-BP02 Communicate status and trends to ensure visibility into operation; OPS09-BP03 Review operations metrics and prioritize improvement
SEC01 How do you securely operate your workload?	Security	Root keys were deleted January 6 and root credentials removed January 29. Production is one of nine accounts under service control policies. The staging copy still runs inside tp-prod, and the data stores have not moved to their own accounts.	SEC01-BP01 Separate workloads using accounts
SEC05 How do you protect your network resources?	Security	WAF protects the API and the data stores are private, with one exception: the production database is still publicly reachable from the BI vendor's four published ranges with TLS required, accepted in writing by Dev Raman (C-4) until the cutover.	SEC05-BP02 Control traffic at all layers

Question	Pillar	Evidence	Best practices not selected
SEC06 How do you protect your compute resources?	Security	Amazon Inspector has run on EC2 and ECR since January 29, and IMDSv2 is required. Some EKS nodes and EC2 volumes predate default encryption and are patched by hand.	SEC06-BP04 Automate compute protection
SEC08 How do you protect your data at rest?	Security	S3 default encryption and EBS default encryption are on. The production PostgreSQL 13 database is not encrypted, and encryption cannot be added in place (H-1).	SEC08-BP02 Enforce encryption at rest
SEC10 How do you anticipate, respond to, and recover from incidents?	Security	Counsel and the CTO know whom to call, but there are no security playbooks and no one has rehearsed one.	SEC10-BP04 Develop and test security incident response playbooks; SEC10-BP07 Run simulations
REL04 How do you design interactions in a distributed system to prevent failures?	Reliability	The moderation pipeline is a chain of Lambda orchestrators that call each other, so a failure in a late step leaves an upload half moderated.	REL04-BP02 Implement loosely coupled dependencies
REL05 How do you design interactions in a distributed system to mitigate or withstand failures?	Reliability	Clients have timeouts. If the ranking endpoint is unavailable, the API returns errors instead of a cached or chronological timeline, and write traffic is not throttled.	REL05-BP01 Implement graceful degradation to transform applicable hard dependencies into soft dependencies; REL05-BP02 Throttle requests
REL06 How do you monitor workload resources?	Reliability	Host metrics are collected, alarms are few, and a request cannot be followed across services.	REL06-BP03 Send notifications (real-time processing and alarming); REL06-BP07 Monitor end-to-end tracing of requests through your system
REL08 How do you implement change?	Reliability	Deployments are scripted partly and run from a laptop in some cases; infrastructure changes are made in the console.	REL08-BP01 Use runbooks for standard activities such as deployment; REL08-BP05 Deploy changes with automation

Question	Pillar	Evidence	Best practices not selected
PERF01 How do you select appropriate cloud resources and architecture for your workload?	Performance Efficiency	Instance families were chosen at launch and not benchmarked since. The ranking endpoint on GPUs sat at 9% GPU utilization.	PERF01–BP06 Use benchmarking to drive architectural decisions; PERF01–BP07 Use a data-driven approach for architectural choices
PERF04 How do you select and configure networking resources in your workload?	Performance Efficiency	CloudFront serves renditions and originals through origin access control since January 6. The video rendition ladder is fixed in the app, and network settings are not tuned from metrics.	PERF04–BP05 Choose network protocols to improve performance; PERF04–BP07 Optimize network configuration based on metrics
COST05 How do you evaluate cost when you select services?	Cost Optimization	Services were chosen for speed to launch. Every video is moderated twice, and every post goes to Transcribe and Comprehend.	COST05–BP02 Analyze all components of the workload; COST05–BP06 Perform cost analysis for different usage over time
COST08 How do you plan for data transfer charges?	Cost Optimization	Data transfer was never modeled. One NAT gateway, in one zone, carries all private egress.	COST08–BP01 Perform data transfer modeling; COST08–BP03 Implement services to reduce data transfer costs
COST09 How do you manage demand, and supply resources?	Cost Optimization	Capacity is fixed at the launch–event peak for every tier.	COST09–BP03 Supply resources dynamically
SUS03 How do you take advantage of software and architecture patterns to support your sustainability goals?	Sustainability	Uploads are processed asynchronously and scheduled work runs off-peak, but the frame-sampling path duplicates the whole-video moderation path.	SUS03–BP02 Remove or refactor workload components with low or no use

Question	Pillar	Evidence	Best practices not selected
SUS05 How do you select and use cloud hardware and services in your architecture to support your sustainability goals?	Sustainability	Stateless tiers run on Intel instances where Graviton would do, and the GPU accelerators are mostly idle.	SUS05-BP02 Use instance types with the least impact; SUS05-BP04 Optimize your use of hardware-based compute accelerators
SUS06 How do your organizational processes support your sustainability goals?	Sustainability	Production runs PostgreSQL 13 and EKS 1.30, both past standard support.	SUS06-BP02 Keep your workload up-to-date

The roadmap by week

The 20 fixes land in weeks three to five, and the 5 acceptances are asked for in week three. Week two ends with the readout on March 6, where the register is agreed. Week six runs from March 30 to April 3 and verifies the gate.

The proposed sequence by engagement week.

WeekDates	HRIs fixed by a change	HRIs accepted in writing
3March 9 to March 13	REL01, REL02, COST02, COST03 (4)	PERF03, COST06, COST07, SUS02, SUS04 (5)
4March 16 to March 20	OPS04, OPS07, SEC07, SEC11, REL07, REL11, PERF02, COST01, COST04 (9)	None
5March 23 to March 27	OPS05, OPS06, OPS10, REL09, REL10, REL12, REL13 (7)	None

Decisions to take at the readout

Dev Raman decides on March 6; we recommend the following.

- **Agree the register and the roadmap.** All 25 HRIs, their owners, and their weeks, as above.
- **Accept the five cost-change HRIs in writing.** PERF03 (Lior Haddad), COST06 (Gwen Tallis), COST07 (Gwen Tallis), SUS02 (Yuki Sorensen), SUS04 (Lior Haddad). This is what lets the cost engagement count each change once.

The two larger options we recommend not taking now. Each is Tidepost’s decision on March 6.

Decision	We recommend	Why	Decides	Revisit
Moving the moderation pipeline’s Lambda chain onto Step Functions (REL04)	Defer	A multi-quarter rewrite of the pipeline that the Trust and Safety team depends on every day.	Dev Raman	Tidepost’s planning for the third quarter.
Multi-Region active-active (REL13)	Decline	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.	Dev Raman	Not scheduled.

If either is taken, it changes the plan and the effort, not the evidence on this page.

© 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.