



AWS MULTI-ACCOUNT FOUNDATION · SAMPLE DELIVERABLE

Operations Runbooks and Handover

Week 4 of 4: Hand over · prepared for Tidepost, Inc.

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

February 13, 2026 · AWS Multi-Account Foundation: The Build, as an add-on to the Audit (four 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 five runbooks 3
 - RB-1: Vend an account..... 5
 - RB-2: Move an account into the organization 5
 - RB-3: Change a policy 5
 - RB-4: Break glass..... 6
 - RB-5: Suspend an account..... 6
- Break-glass custody 7
- The handover workshop..... 7
- The operator role was deleted 8
- Hours against the cap 10
- Handoffs to the other engagements 11
 - Security Audit and Hardening 11
 - Well-Architected Review and Remediation 12
 - Cost Analysis and Optimization..... 12
- What remains for Tidepost 12
 - The risk register at close 13

Summary

The foundation is yours to run. Dev Raman, Kofi Brandvold, Sasha Ilyin, and Gwen Tallis: this report hands over five runbooks that Kofi Brandvold’s team and Sasha Ilyin’s team can follow without us, the custody of the break-glass access, and a list of what stays with Tidepost and when. Two of the runbooks were proved in the engagement’s last week in front of the people who will use them. The operator role Vantalect used was deleted by Tidepost on February 13, 2026, so nothing in this report depends on a Vantalect login.

The add-on used 68 of its 70 hours and 27 hours of approved windows. All 12 scored checks are counted as passed (11 pass and 1 is waived in writing), which is covered in the re-scan report.

The handover in numbers. Hours and window time are the add-on's, separate from the security engagement's.

Handover at a glance	Result
Runbooks	5, RB-1 to RB-5
Handover workshop	February 12, 2026, recorded
Closing readout	February 13, 2026
Operator role deleted	February 13, 2026, by Tidepost
Change windows used	6
Consultant hours	68 of 70
Policy-caused denials after any attachment	0
Where the code lives	tidepost-foundation and tidepost-cdk

The five runbooks

A runbook here is a short procedure with an owner who runs it, an approver who says yes, and a rollback. Each was written from something that was done in this engagement, so none is theory: the last column of the table is when and where it was proved. They live in tidepost-foundation, next to the policies they operate on.

The five runbooks, who runs each, who approves it, and where it was proved.

ID	Runbook	Owner	Approver	Trigger	Proved
RB-1	Vend an account	Kofi Brandvold	Dev Raman	A new workload, a data account, or a team that needs separation	February 5, 2026, tp-sandbox-ml
RB-2	Move an account into the organization	Kofi Brandvold	Dev Raman	Tidepost's own migration of a data or staging workload into a vended account, or an acquired account	January 28, 2026, tp-prod
RB-3	Change a policy	Kofi Brandvold	Sasha Ilyin	A request to allow or block something across accounts	February 3, 2026, the February 3 attachment to Sandbox and NonProd
RB-4	Break glass	Sasha Ilyin	Noor Castellanos	Identity Center or the identity provider is down (the vendor key's rotation has its own role and does not use this runbook)	February 12, 2026, a drill in tp-policy-test during the handover workshop
RB-5	Suspend an account	Kofi Brandvold	Sasha Ilyin	A compromised or retired account	February 12, 2026, tp-policy-test, during the handover workshop

RB-1: Vend an account

Owner: Kofi Brandvold, Head of Platform. **Approver:** Dev Raman, Co-founder and Chief Technology Officer. **Use it when:** A new workload, a data account, or a team that needs separation.

1. Record the owner, OU, and a company group alias for the root email in the ticket
2. Provision the Account Factory product with the alias, the OU, and the Identity Center group
3. Wait for enrollment and for the Service Quotas template
4. Run MAF-02 through MAF-08 against the new account with the read-only role
5. Add the account to the account map in tidepost-foundation

Rollback. Move the account to Suspended; nothing deletes an account. **Proved:** February 5, 2026, tp-sandbox-ml.

RB-2: Move an account into the organization

Owner: Kofi Brandvold, Head of Platform. **Approver:** Dev Raman, Co-founder and Chief Technology Officer. **Use it when:** Tidepost's own migration of a data or staging workload into a vended account, or an acquired account.

1. Run the join pre-flight (the January 28 window's list) and attach the results to the approval request
2. Get written approval from the sponsor and the management account's owner two business days ahead
3. Invite, accept, place in the target OU, and enroll
4. Run MAF-02 through MAF-08 for the account
5. Keep the removal call ready as the rollback until the first denial watch ends

Rollback. Remove the account from the organization; leaving needs contact information, a current payment method, and a support plan of its own, which the pre-flight confirms before the join. **Proved:** January 28, 2026, tp-prod.

RB-3: Change a policy

Owner: Kofi Brandvold, Head of Platform. **Approver:** Sasha Ilyin, Head of Security and Compliance. **Use it when:** A request to allow or block something across accounts.

1. Change the policy in tidepost-foundation and open a pull request reviewed by Kofi Brandvold and Sasha Ilyin

2. Validate with IAM Access Analyzer and run the Policy Staging cases
3. Attach to Sandbox and NonProd, then watch CloudTrail for 24 hours
4. Attach to Prod, then watch again
5. Record the staging cases and both watch results in the pull request. VPC Block Public Access is not in the set until the public load balancers have exclusions (decision D-3)

Rollback. Detach the policy from the OU: one management-account call. **Proved:** February 3, 2026, the February 3 attachment to Sandbox and NonProd.

RB-4: Break glass

Owner: Sasha Ilyin, Head of Security and Compliance. **Approver:** Noor Castellanos, Co-founder and Chief Executive Officer. **Use it when:** Identity Center or the identity provider is down (the vendor key's rotation has its own role and does not use this runbook).

1. Two people open the sealed credential: Sasha Ilyin and Noor Castellanos
2. Sign in as bg-admin in tp-management with the hardware key
3. Assume TidepostBreakGlass in the target account and do only the ticketed action
4. The alarm posts to the platform channel; Dev Raman, who holds no part of the credential, reviews the session within one business day
5. Reseal the credential and rotate it

Rollback. Not applicable; the session expires after one hour. **Proved:** February 12, 2026, a drill in tp-policy-test during the handover workshop.

RB-5: Suspend an account

Owner: Kofi Brandvold, Head of Platform. **Approver:** Sasha Ilyin, Head of Security and Compliance. **Use it when:** A compromised or retired account.

1. Move the account to the Suspended OU, where the deny-all policy applies at once
2. Revoke Identity Center assignments and open an incident if it is a compromise
3. Keep the account and its data; closing is a separate decision

Rollback. Move the account back to its OU. **Proved:** February 12, 2026, tp-policy-test, during the handover workshop.

Break-glass custody

Break-glass is the way in when the normal way is down, and its design is that it is hard to use quietly. The access is a user, `bg-admin`, in `tp-management`, and a role, `TidepostBreakGlass`, in every member account. Sasha Ilyin (Head of Security and Compliance) and Noor Castellanos (Co-founder and Chief Executive Officer) hold it, so opening it takes two people. It was created on January 22, 2026 and its hardware key sealed the same day.

- **It is the broad exemption in the guardrails.** The break-glass role is exempt from the SCP baseline's detection, Region, and instance-metadata-change statements and from the IAM-user policy, so it still works when a policy would block everyone else. That is why custody matters more than any other control in this report. The only other exemption is narrow: `TidepostVendorKeyRotation` may create access keys for the vendor's user and no one else.
- **Every use is announced.** Every sign-in and every `AssumeRole` posts to the platform channel and opens a ticket. Dev Raman reviews the session within one business day; Dev Raman holds no part of the credential, so the people who opened it never review their own session.
- **It has no routine use.** The waived vendor key (MAF-05) is rotated every 90 days through `TidepostVendorKeyRotation`, next due May 12, 2026, by Kofi Brandvold signed in through Identity Center, so a rotation never opens the sealed credential or sets off its alarm.
- **It was drilled, not just written.** RB-4 was run as a drill in `tp-policy-test` during the handover workshop on February 12, 2026.
- **Root is separate.** No root credential is held by anyone but Tidepost. `tp-management`'s root has two FIDO2 keys in separate places, and member accounts have no root credential at all.

The handover workshop

The workshop was on February 12, 2026, recorded, with Kofi Brandvold, Sasha Ilyin, and Dev Raman. It covered the five runbooks and ran RB-4 (break glass) and RB-5 (suspend an account) live, both against `tp-policy-test`. The recording is Tidepost's, along with the repository and the policies. The closing readout was the next day, February 13, 2026.

Who can do what in the organization is set by permission sets in IAM Identity Center, assigned to groups that mirror the people who need them:

The permission sets at handover.

Permission set	Group	People	Scope
PlatformAdministrator	aws-platform-admins	Kofi Brandvold	Every account; administrator, MFA required
Developer	aws-developers	Marcus Oyelaran, Bea Okafor	tp-dev and tp-staging with power-user access; read-only in tp-prod
MachineLearning	aws-ml	Yuki Sorensen	tp-sandbox-ml with power-user access; read-only in tp-prod
DataEngineer	aws-data	Lior Haddad	Read and query on the telemetry stores in tp-prod; power-user in tp-dev
SecurityAudit	aws-security-audit	Sasha Ilyin, Amara Delacroix	Read-only everywhere; tp-audit and tp-log-archive
BillingViewer	aws-billing	Gwen Tallis	Billing and Cost Explorer in tp-management

The operator role was deleted

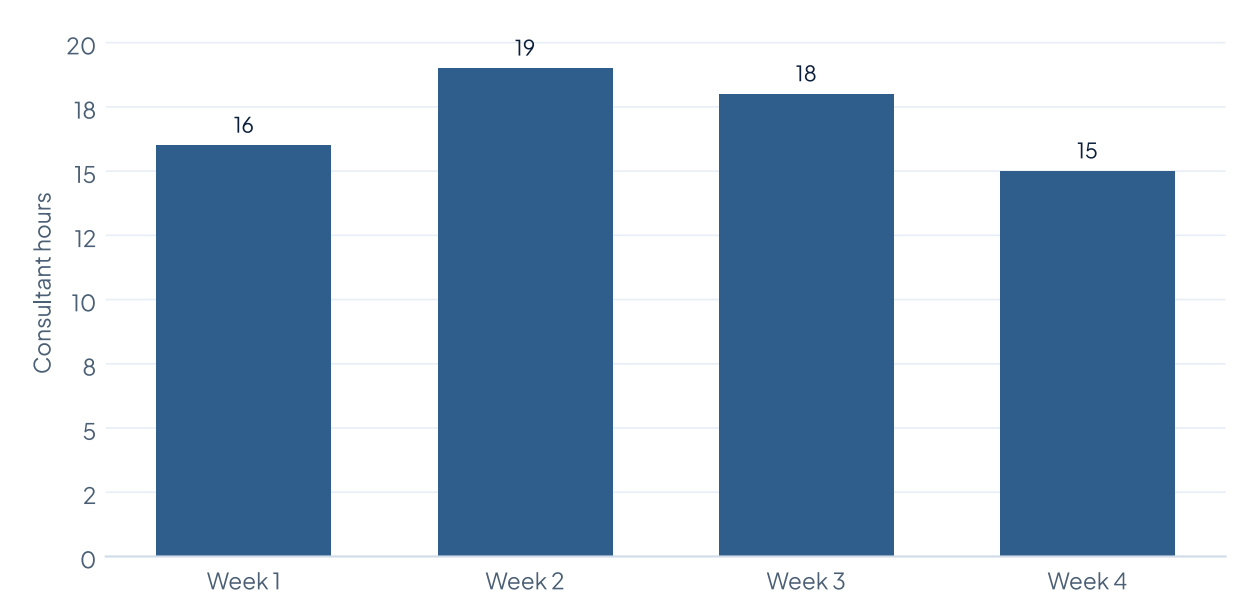
VantalectFoundationOperator was Tidepost's role in tp-management, created by Kofi Brandvold on January 20, 2026 from a template Vantalect sent, and deleted by Kofi Brandvold on February 13, 2026, before the final scan, which is how check MAF-13 passes. While it existed its trust admitted only Charles's named principal with MFA and a source identity, its time conditions equaled each approved window, sessions lasted at most an hour, and these were denied outright: closing accounts; deleting the organization; changing payment methods or billing contacts; creating IAM users or access keys; leaving the organization.

The 6 windows. Each was approved in writing two business days ahead by Dev Raman and Kofi Brandvold; 27 hours in all.

Window	Date	Time	What it did	Approved	Pre-flight checks
W1	Jan 21	09:00 to 15:00 CST	Landing zone	Jan 16	3
W2	Jan 23	09:00 to 12:00 CST	IAM Identity Center and the identity provider	Jan 21	3
W3	Jan 28	09:00 to 15:00 CST	The join and enrollment	Jan 26	9
W4	Feb 3	09:00 to 12:00 CST	Policies to Sandbox and NonProd	Jan 30	4
W5	Feb 5	09:00 to 13:00 CST	Policies to Prod, and the vended account	Feb 3	4
W6	Feb 10	09:00 to 14:00 CST	Backup and tag policies; the backup account	Feb 6	4

Every call lands in the organization trail with his source identity; an EventBridge rule posts each AssumeRole to the platform channel. Vantalect holds no write access to any member account; everything inside members goes through tidepost-foundation and tidepost-cdk pull requests.

Hours against the cap



Consultant hours by week against a cap of 70.

Hours used per week. The cap is 70 hours; the fee is fixed.

Week	Starts	Theme	Hours
1	Jan 19	Landing zone and core accounts	16
2	Jan 26	The founders' account joined and enrolled	19
3	Feb 2	Guardrails, vending, and shared services	18
4	Feb 9	Backup, tags, re-scan, and handover	15
Total			68

The fee is fixed, so the hours are a measure and not a meter. 68 of 70 means the add-on fit its cap with 2 to spare, and the write access to the management account was 6 windows totaling 27 hours.

Handoffs to the other engagements

Three engagements follow the add-on, or run beside it, and each takes something from it. The handoffs below are the specific items, with the day each was done, so nobody has to re-derive the state.

Security Audit and Hardening

Handed to the Security Audit and Hardening engagement.

Item	What is handed over	Done
C-1	Root credentials removed under centralized root access, after the join	January 29, 2026
C-7	Identity Center connected January 23; people provisioned January 26 and assigned to tp-prod at the join, January 28; the remaining IAM users retired February 10	February 10, 2026
C-9	The organization trail into tp-log-archive replaces the account trail at the join	January 28, 2026
detection	Delegated GuardDuty and Security Hub, so the detection report runs from tp-audit	January 29, 2026

Well-Architected Review and Remediation

Handed to the Well-Architected Review and Remediation engagement.

Item	What is handed over	Done
tp-backup and the backup policy	Reliability REL09 turns the policy on by tagging resources	February 10, 2026
tp-staging	The vended staging account, empty until the June rebuild (EC2-1a)	January 29, 2026

Cost Analysis and Optimization

Handed to the Cost Analysis and Optimization engagement.

Item	What is handed over	Done
CUR 2.0 data export	Starts in tp-management at the join	January 28, 2026
pre-join Cost Explorer extract	Twelve months by service and usage type	January 27, 2026
tag policy	Attached to Prod, NonProd, and Sandbox	February 10, 2026

What remains for Tidepost

The add-on vends the accounts and sets the guardrails. It does not move Tidepost into them, and it does not run the organization afterward. This is the list, with owners.

- **Move the staging and data workloads into their own accounts.** Moving the staging and data workloads out of tp-prod is workload migration, a change order or another statement of work. The add-on vends the accounts; Tidepost moves into them on its own calendar (the data accounts wait for the third quarter). tp-staging is empty until the June rebuild, and tp-dev already holds the developer instances that Tidepost's engineers moved on February 4. Owner: Kofi Brandvold, following RB-1 and RB-2.
- **Tag the resources that should be backed up.** The backup policy selects nothing until a resource carries backup=required; the Well-Architected Remediation does that. Until then the policy selects nothing.
- **Activate cost allocation tags.** Waits until the keys appear on resources and belongs to the Well-Architected Remediation (COST01). Owner: Gwen Tallis.
- **Rotate the waived vendor key** on May 12, 2026, and every 90 days after, through TidepostVendorKeyRotation. Owner: Kofi Brandvold.

- **Review the waiver at each quarterly access review.** Owner: Sasha Ilyin.
- **Decide on a support plan for each new account.** Support plans are per account: tp-prod keeps Business Support+, and each new account starts on Basic Support. Owner: Gwen Tallis.
- **Take up VPC Block Public Access when the load balancers can take it.** It is not attached, because it would block the public load balancers without exclusions. RB-3 is where that decision is made.
- **Score MAF-11 when a shared network exists.** There is one VPC and no Transit Gateway, so the check is unscored until separate accounts need to share one.

The SOC 2 observation window opens April 1, 2026. Every control this foundation provides has a start date before it, but Vantalect is not Tidepost's auditor and predicts nothing about the report.

The risk register at close

The register was kept from the readout. Each risk is shown with its owner and how it ended.

The 10 risks in the register and how each ended.

ID	Risk	Size	Owner	Result
FR-1	Billing transfer	Medium	Gwen Tallis	No gap in cost history: twelve months of extract plus the export from January 28
FR-2	Reserved Instances and Savings Plans	Low	Gwen Tallis	Nothing to lose at the join
FR-3	Marketplace subscriptions	Low	Gwen Tallis	No vendor to re-issue an offer
FR-4	Support plans	Medium	Gwen Tallis	Cleared the day before the window
FR-5	Service quotas	Low	Kofi Brandvold	Template applied on the vended account
FR-6	Account-level dependencies	Low	Kofi Brandvold	Nothing to break
FR-7	Root email and MFA custody	Medium	Sasha Ilyin	Custody proven on both sides; recovery tested
FR-8	SCP and RCP blast radius	High	Kofi Brandvold	Zero policy-caused denials after any attachment; one policy corrected in staging
FR-9	Control Tower enrollment	Low	Kofi Brandvold	Enrolled in the January 28 window
FR-10	SOC 2 timing	Medium	Sasha Ilyin	Trail from January 21; guardrails by February 10

© 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.