

Vantalect

AWS BREACH FORENSICS & RECOVERY · SAMPLE DELIVERABLE

Eradication and Root-Cause Closure

DISTRIBUTION: OPERATIONAL

Week 3 of 4: Eradicate and close · prepared for Wrenfield Bancorp, Inc.

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

July 31, 2026 · AWS Breach Forensics & Recovery: The Investigation and the Recovery (four weeks)

SAMPLE DELIVERABLE

This is a sample deliverable. Wrenfield is fictional. Its people, customers, accounts, figures, and attacker are invented for this sample, and any resemblance to a real bank, company, person, or threat group is coincidental. The attacker's addresses come from ranges reserved for documentation.

Contents

What this report records 2

Closure at a glance 3

The root-cause fixes, as code 3

- Pull requests and reviewers 5
- Verification 6
- Code excerpts 6

The guardrails 8

- Policies attached 9
- What the guardrail SCP denies 10
- The staging tests 10

What was accepted in writing 11

Closure of each inventory item 12

Other weaknesses closed in week three 17

Residual risk 17

Notice 19

What this report records

This report records the closure of the Investigation's findings as code, as of Friday, July 31, 2026, the end of week three of the Recovery. It is for Mireille Danvers, Imani Castell, and the bank's platform and incident teams. Its distribution line is Operational: This report is for the bank's incident and platform teams. It is not part of the counsel track and holds no legal analysis.

What it says. 31 items from the compromise inventory are each closed, held, or accepted, with the evidence sealed first and the closure checked. Four of the six root causes are closed in code, with a pull request, a reviewer, a date, and a verification. RC-4 is closed for new versions; open for existing objects: the existing objects have no retention, and the gap is carried as a residual risk with an owner and a date. RC-6 is accepted in writing, with an owner and a date. The guardrails sit at the organization. The residual risk is listed at the end.

What it does not say. It does not repeat the Response's actions of July 4 to July 9, which the Response's reports hold; the Wednesday, July 8 eradication (the attacker's user, keys, and roles deleted after preservation, `svc-artifact-sync` replaced by an OIDC role, and `wf-deploy-`

pipeline's trust narrowed) is recorded here as code, not as an event. It does not say whether any law or rule applies. It reports no hours beyond the Response's 56. The repository names wf-platform-iac (the platform's infrastructure as code, AWS CDK) and wf-ci (the Jenkins shared library) and every pull request number in this report are the sample's. They do not name a real repository.

Closure at a glance

All 31 inventory items and all six root causes have a status on July 31: 16 items removed, 4 restored, 7 isolated for counsel, 4 accepted, and four root causes closed as code, RC-4 closed for new versions only, and RC-6 accepted in writing.

The week-three closure in ten numbers.

Measure	Value
Inventory items	31
Removed (the attacker's objects, deleted after sealing)	16
Restored (the bank's own objects, put back)	4
Isolated (kept for counsel, not deleted)	7
Accepted (cannot be removed or known, including the application tier, where no host access was observed but host compromise is not ruled out)	4
Root causes closed as code	4 of 6
RC-4, Object Lock	Closed for new versions; open for existing objects (R-2)
Critical root causes closed	3 of 3
Accepted in writing	1 (RC-6)

The root-cause fixes, as code

Each of the five root causes with a code change has a merged pull request, a reviewer who is not the author, and a verification we ran. The pull requests are in wf-platform-iac (the platform's AWS CDK code) and wf-ci (the Jenkins shared library). The closed dates are Tuesday, July 28 (RC-1 and RC-2), Wednesday, July 29 (RC-3), Thursday, July 30 (RC-4, new versions only), and Friday, July

31 (RC-5). The 286 million existing objects have no retention. No Object Lock retention job over them appears in the Recovery's record, so RC-4 is open for the existing objects and planned (R-2, F-11 in the root-cause report), not accepted in writing. The July 8 interim controls (RC-1 and RC-2) were made by hand. They are now code.

Pull requests and reviewers

Pull requests for RC-1 to RC-5. Repository names and numbers are the sample's.

Root cause	Severity	Repository	PR	What changed	Author	Reviewer	Approver	Merged
RC-1	Critical	`wf-ci`	#87	Build authenticates with an OIDC web identity token; remove the static key from the pipeline	Imani Castell	Owen Tribble	None	Tuesday, July 28
RC-1	Critical	`wf-platform-iac`	#231	OIDC provider and role wf-artifact-sync-oidc in wf-tools; svc-artifact-sync removed from the stacks	Owen Tribble	Imani Castell	None	Tuesday, July 28
RC-2	Critical	`wf-platform-iac`	#233	wf-deploy-pipeline trust: the Jenkins role only, source identity required, ten accounts, one stack set	Imani Castell	Owen Tribble	Mireille Danvers	Tuesday, July 28
RC-3	Critical	`wf-platform-iac`	#236	Guardrail SCP wf-org-guardrails and the resource control policy, as code	Imani Castell	Mireille Danvers	None	Monday, July 27
RC-3	Critical	`wf-platform-iac`	#237	Attach staging copies of both policies to the staging OU, with the 14 policy tests	Imani Castell	Owen Tribble	None	Monday, July 27
RC-3	Critical	`wf-platform-iac`	#240	Attach both policies at the organization root	Imani Castell	Mireille Danvers	None	Wednesday, July 29
RC-4	High	`wf-platform-iac`	#238	Object Lock, governance mode, 30 days, on new versions of wf-imaging-archive-prod	Owen Tribble	Imani Castell	Rafael Quintero	Thursday, July 30
RC-5	High	`wf-platform-iac`	#241	EventBridge rules: all management events to Interceptor's watch and the provider; page rule for high-severity findings	Owen Tribble	Imani Castell	None	Thursday, July 30
RC-5	High	`wf-platform-iac`	#242	Read data events on wf-imaging-archive-prod and wf-lending-docs-prod; write events on the lending bucket	Owen Tribble	Imani Castell	None	Friday, July 31

Verification

We ran each verification with the bank's engineers. Verification for each root cause, with the date it closed:

How each root cause was verified. RC-4 is verified for new versions only. RC-6 has no code change; its record is the written acceptance.

Root cause	Closed	Verification
RC-1	July 28	A test build on a throwaway branch took its credentials through `AssumeRoleWithWebIdentity`, and the trail shows the call from the build host. The credential report for wf-tools lists no IAM user with an access key. `GetUser` on svc-artifact-sync returns NoSuchEntity (deleted July 8, RE-181).
RC-2	July 28	The stack set shows 10 of 10 instances in sync, with drift detection on. A call to assume the role from any principal in wf-tools other than the Jenkins role, or without the source identity, was denied in all 10 accounts. The Jenkins role with the source identity succeeded in wf-nonprod-lending.
RC-3	July 29	The staging OU (holding wf-sandbox-2) ran the 14 policy tests on July 27 and 28: 10 attacker moves denied and 4 legitimate moves allowed. Attached at the organization root on July 29 at 11:05 (RE-195). No legitimate pipeline call was denied in the next 24 hours.
RC-4	July 30 (new versions only)	`GetObjectLockConfiguration` returns governance mode, 30 days. A test delete of a new version was denied. `s3:BypassGovernanceRetention` is held by the break-glass role only. Scope of the check: new versions only. A version written before July 30 shows no retention, because default retention applies to versions written after it is set. This is the residual risk R-2, and the root cause is not reported as fully closed.
RC-5	July 31	A test `ListRoles` call from a test key appears in the organization trail, and the EventBridge rule shows one delivery to the provider's queue. A test high-severity finding paged two people on the staged holiday schedule in 4 minutes. Read data events for both buckets are in the trail.
RC-6	July 31	Not a code change. The written acceptance ACC-1 is signed, dated, and owned (next section).

Code excerpts

The narrowed trust for `wf-deploy-pipeline` (RC-2), deployed to the ten workload accounts as one stack set (`wf-platform-iac` #233):

```yaml
WfDeployPipelineRole:
  Type: AWS::IAM::Role
  Properties:
    RoleName: wf-deploy-pipeline
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: Allow
          Principal:
            AWS: arn:aws:iam::584729103358:role/wf-jenkins-agent
          Action: [sts:AssumeRole, sts:SetSourceIdentity]
          Condition:
            StringLike:
              sts:SourceIdentity: "wf-ci-*"
```

The role that replaces `svc-artifact-sync` (RC-1), in `wf-tools` (`wf-platform-iac` #231). The build holds no secret: it exchanges the pipeline's identity token for short-lived credentials.

```yaml
ArtifactSyncRole:
  Type: AWS::IAM::Role
  Properties:
    RoleName: wf-artifact-sync-oidc
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: Allow
          Principal:
            Federated: arn:aws:iam::584729103358:oidc-provider/ci.wrenfield.example
          Action: sts:AssumeRoleWithWebIdentity
          Condition:
            StringEquals:
              ci.wrenfield.example:aud: sts.amazonaws.com
              ci.wrenfield.example:sub: job:wf-ci/artifact-sync
```

An excerpt of the guardrail SCP `wf-org-guardrails` (RC-3, `wf-platform-iac` #236), the two statements that refuse keys with the attacker's own material:

```json
[
  {
    "Sid": "DenyNonAwsKeyOrigin",
    "Effect": "Deny",
    "Action": "kms:CreateKey",
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {"kms:KeyOrigin": "AWS_KMS"},
      "ArnNotLike": {"aws:PrincipalArn": "arn:aws:iam::*:role/wf-break-glass"}
    }
  },
  {
    "Sid": "DenyImportedKeyMaterial",
    "Effect": "Deny",
    "Action": ["kms:ImportKeyMaterial", "kms:DeleteImportedKeyMaterial"],
    "Resource": "*",
    "Condition": {
      "ArnNotLike": {"aws:PrincipalArn": "arn:aws:iam::*:role/wf-break-glass"}
    }
  }
]
```

The first statement refuses a key only when its origin is not `AWS_KMS`, so ordinary key creation stays allowed. The second refuses importing or deleting imported key material for everyone except the break-glass role.

The guardrails

The guardrail SCP and RCP were proven in a staging OU on July 27 and 28, then set at the organization root on Wednesday, July 29. The staging OU held one sandbox account, `wf-sandbox-2`, and a staging copy of each policy (attached July 27, removed after the production policies were attached on July 29). Fourteen tests ran there: ten attacker moves that must be denied, and four legitimate moves that must be allowed. Every test came out as expected.

Policies attached

The service control policies (SCP) and resource control policies (RCP) that stand on July 31: six policies, four SCPs and two RCPs. The `deny-attacker-principals` row is a statement inside `wf-incident-containment`, not a policy.

Policy	Type	Target	Attached	Reference	Status on July 31
`wf-incident-containment`	SCP	Workloads OU	July 4, 01:22 EDT	RE-003	Stays attached through the watch; its exceptions are the incident role and the break-glass role
`deny-attacker-principals (statement in the same policy)`	SCP	Workloads OU	July 4, 02:58 EDT	RE-064	Stays; the three attacker principals no longer exist, so the statement matches nothing
`wf-deny-outside-access`	RCP	Workloads OU	July 4, 03:20 EDT	RE-072	Stays attached to Workloads (policy type enabled at the root 03:15:10, outside trusts listed 03:16:40); the code-defined RCP at the root carries the same rules
`wf-evidence-deny-all`	SCP	Incident OU	July 4, 03:52 EDT	Evidence register (p-wrnfevid00001)	Stays; the evidence account's deny-all, with two exempt roles
`wf-vault-deny-all`	SCP	Recovery OU	July 4, 04:34 EDT	RE-078	Stays; updated at 16:45 on July 8 (EV-01092) to exempt the two copy roles only, each with MFA and two-person approval, so the setup role is denied by name; and a second statement that denies snapshot deletion, sharing, and unlocking and key deletion, disabling, policy, and grant changes to everyone
`wf-org-guardrails`	SCP	Organization root	July 29, 11:05 EDT	RE-195	In force; defined in wf-platform-iac #236
`wf-org-data-perimeter`	RCP	Organization root	July 29, 11:12 EDT	PR #237 and #240	In force; denies outside principals on STS, KMS, and S3

What the guardrail SCP denies

- `kms:CreateKey` where `kms:KeyOrigin` is not `AWS_KMS`; `kms:ImportKeyMaterial`; `kms:DeleteImportedKeyMaterial`; `kms:ScheduleKeyDeletion`
- `kms:PutKeyPolicy` and `kms:CreateGrant` except by the key administrator role
- `ec2:ModifySnapshotAttribute`, `rds:ModifyDBSnapshotAttribute`, and snapshot deletion, except by the backup roles
- `s3:PutLifecycleConfiguration`, `s3:PutBucketVersioning`, and `s3:CreateJob` (S3 Batch) except by the named pipeline roles
- `cloudtrail:DeleteTrail`, `cloudtrail:StopLogging`, `iam:CreateUser`, and `iam:CreateAccessKey`
- Recycle Bin rule changes; `rds:ModifyDBInstance` where it turns deletion protection off
- Exceptions: the break-glass role and, until August 7, the incident role
- Not covered: a person with Organizations rights in the management account can change the vault OU's SCP (the setup role `OrganizationAccountAccessRole` has been denied by name since 16:45 on July 8, `EV-01092`); see R-3

The staging tests

The 14 staging tests, run July 27 and 28. A guardrail is attached at the root only after all 14 pass.

No.	Test in the staging OU	Expected	Result
1	Create a KMS key with Origin EXTERNAL, and one with Origin AWS_KMS	EXTERNAL denied; AWS_KMS allowed	EXTERNAL denied; AWS_KMS allowed
2	Import key material into a key	Denied	Denied
3	Share an RDS snapshot with an account outside the organization	Denied	Denied
4	Share an EBS snapshot with an outside account	Denied	Denied
5	Put a lifecycle rule on a versioned bucket	Denied	Denied
6	Create an S3 Batch job as a non-pipeline principal	Denied	Denied
7	Stop logging on a trail	Denied	Denied
8	Create an IAM user or an access key	Denied	Denied
9	Assume a role from a principal outside the organization (the RCP)	Denied	Denied

No.	Test in the staging OU	Expected	Result
10	Delete a snapshot in the Recycle Bin rule's scope as an administrator	Denied	Denied
11	AWS Backup copies a snapshot to the vault with the backup role	Allowed	Allowed
12	The Jenkins role deploys a stack with the source identity	Allowed	Allowed
13	The break-glass role lifts a test control	Allowed	Allowed
14	The incident role reads configuration	Allowed	Allowed

What was accepted in writing

One item is accepted, not fixed: RC-6, the placement of the month-end snapshots. Mireille Danvers signed the acceptance on Friday, July 31, 2026. An acceptance is not a closure: the risk stays on the register until the date below.

The written acceptance of RC-6.

Field	Entry
Acceptance	ACC-1, for RC-6: Month-end snapshots in the workload account itself, the central copy in governance mode
What is accepted	Month-end RDS snapshots stay in the workload account wf-prod-lending (nine of them), with their copies in wf-backup under Vault Lock in governance mode. The Recovery's copies in wf-recovery-vault are protected as the compensating controls below describe: the 46 EBS copies were locked from July 6 through July 20 and no extension is evidenced, so they now rely on the vault's access policy and key availability, and the ten RDS copies were never locked.
Why	Moving the central vault to compliance mode is irreversible once its grace period ends, and the bank wants one quarter to confirm its retention periods first.
Accepted until	Friday, December 18, 2026, when the backup vault moves to compliance mode (next quarter)
Owner of the change	Imani Castell, wf-platform-iac issue #245
Signed by	Mireille Danvers, Chief Information Security Officer, Friday, July 31, 2026
Review due	Friday, October 30, 2026, at the scheduled guardrail review

What stands in the way of the risk while it is accepted.

- The guardrail SCP now denies deleting or sharing snapshots in the workload accounts, except by the backup roles.
- In wf-recovery-vault, the 46 EBS snapshot copies were under LockSnapshot in compliance mode from July 6 through July 20 (14 days, cool-off 72 hours). No extension is evidenced, so they now rely on the vault OU's SCP and the keys the bank holds, as the ten RDS copies do. The ten RDS snapshot copies (the nine month-end snapshots and one of the live database) are plain snapshots and were never under a lock. The vault OU's SCP, which also denies deletion, sharing, and key changes to everyone, and keys the bank holds are what protect all of them.
- The weakest link in that protection is a person with Organizations rights in the management account who could change the SCP (see R-3). AWS Backup Vault Lock covers one recovery point of the live database; it does not cover the RDS copies.
- Read-only and write events reach Interceptor's watch, so a delete attempt would alert.

Closure of each inventory item

All 31 rows of the compromise inventory are below, once each, with how each was closed and how we checked. The evidence column gives the sealed evidence item captured before any removal. Status is the inventory's.

The 31 inventory items and their closure. Evidence items (EVD) are in the custody log.

ID	Item	Account	Status	Closure	Sealed first	Verified
CI-001	KMS key, wf-prod-lending	wf-prod-lending	Isolated	Outside statement dropped from the key policy July 4, 02:09:05 EDT (`EV-00633`). Key material expired July 7 at 18:00 (`EV-01037`), so the key is in PendingImport. On July 8 at 10:03 the bank's DisableKey was rejected with KMSInvalidStateException (`EV-01052`), and DescribeKey returned PendingImport (`EV-01053`). Kept as it is for counsel; deletion is not scheduled.	EVD-007	July 31: key state is PendingImport; no material; policy names no outside account
CI-002	Alias wf-backup-2026, wf-prod-lending	wf-prod-lending	Isolated	Left in place on the key in PendingImport. Counsel's hold; renaming would alter the record.	EVD-007	July 31: alias resolves to the key in PendingImport
CI-003	KMS key, wf-prod-imaging	wf-prod-imaging	Isolated	Outside statement dropped from the key policy July 4, 02:09:25 EDT (`EV-00634`). Material expired July 7 (`EV-01038`); key in PendingImport. DisableKey was rejected with KMSInvalidStateException on July 8 at 10:03 (`EV-01054`), and DescribeKey returned PendingImport (`EV-01055`). Kept for counsel.	EVD-008	July 31: key state is PendingImport; no material; policy names no outside account
CI-004	Alias wf-backup-2026, wf-prod-imaging	wf-prod-imaging	Isolated	Left in place on the key in PendingImport, for counsel.	EVD-008	July 31: alias resolves to the key in PendingImport
CI-005	KMS key, wf-prod-data	wf-prod-data	Isolated	Outside statement dropped from the key policy July 4, 02:09:45 EDT (`EV-00635`). Material expired July 7 (`EV-01039`); key in PendingImport. DisableKey was rejected with KMSInvalidStateException on July 8 at 10:04 (`EV-01056`), and DescribeKey returned PendingImport (`EV-01057`). Kept for counsel.	EVD-009	July 31: key state is PendingImport; no material; policy names no outside account
CI-006	Alias wf-backup-2026, wf-prod-data	wf-prod-data	Isolated	Left in place on the key in PendingImport, for counsel.	EVD-009	July 31: alias resolves to the key in PendingImport

ID	Item	Account	Status	Closure	Sealed first	Verified
CI-007	Lifecycle rule on the imaging archive	wf-prod-imaging	Removed	Removed July 4 at 01:35 (RE-017), after the rule was captured. The guardrail now denies lifecycle changes on the archive.	EVD-001	July 4 and July 29: no attacker rule; change denied in test 5
CI-008	Database snapshot made by the attacker	wf-prod-lending	Removed	Deleted July 28 by Imani Castell after the inventory was sealed. The data was never collected; the vault holds the bank's own copy.	EVD-019	July 28: snapshot list has no such name
CI-009	31 EBS snapshots made by the attacker, wf-prod-lending	wf-prod-lending	Removed	Deleted July 28 by Imani Castell after the inventory was sealed.	EVD-016	July 28: 31 of 31 not found
CI-010	15 EBS snapshots made by the attacker, wf-prod-data	wf-prod-data	Removed	Deleted July 28 by Imani Castell after the inventory was sealed.	EVD-016	July 28: 15 of 15 not found
CI-011	Role s3-batch-replication, wf-prod-imaging	wf-prod-imaging	Removed	Policy and role deleted July 8 at 10:02 and 10:03 (RE-162, RE-163), after capture.	EVD-021	July 8: GetRole returns NoSuchEntity
CI-012	S3 Batch job, wf-prod-imaging	wf-prod-imaging	Removed	Canceled July 4 at 01:28 (RE-015) after 3 hours 47 minutes. The job record is sealed. The guardrail denies new jobs from other principals.	EVD-017	July 4: the job record shows it canceled; July 29: test 6
CI-013	31 snapshot copies under attacker keys, wf-prod-lending	wf-prod-lending	Removed	Deleted July 28 by Imani Castell. The copies could not be read after July 7.	EVD-016	July 28: 31 of 31 not found
CI-014	15 snapshot copies under attacker keys, wf-prod-data	wf-prod-data	Removed	Deleted July 28 by Imani Castell.	EVD-016	July 28: 15 of 15 not found
CI-015	Database snapshot copy under the attacker key	wf-prod-lending	Isolated	Held for counsel with its sharing removed on July 4 (CI-026). Metadata only is sealed; its data was never collected. It cannot be read once the key material has expired.	EVD-015	July 31: snapshot not shared; key in PendingImport
CI-016	Nine month-end database snapshots, deleted by the attacker	wf-prod-lending	Restored	Restored from wf-backup July 5, 05:10 to 07:50 (RE-083 to RE-091). Their copies in wf-recovery-vault are plain snapshots, not under a lock; the vault SCP and the bank's keys protect them. See ACC-1 and R-3.	EVD-019	July 6: 9 of 9 present; copies shared to the vault and present

ID	Item	Account	Status	Closure	Sealed first	Verified
CI-017	31 EBS snapshots deleted by the attacker, wf-prod-lending	wf-prod-lending	Restored	Restored from the Recycle Bin July 4 at 07:40 (RE-080).	EVD-016	July 4: 31 of 31 listed
CI-018	15 EBS snapshots deleted by the attacker, wf-prod-data	wf-prod-data	Restored	Restored from the Recycle Bin July 4 at 07:41 (RE-081).	EVD-016	July 4: 15 of 15 listed
CI-019	Legacy trail wf-lending-legacy-trail, deleted	wf-prod-lending	Accepted	The legacy trail configuration was deleted. Previously delivered log files remain unless separately deleted; no such deletion is shown. The configuration was not recreated, and the bank accepted that on July 28, because the organization trail supplies the required coverage. The guardrail now denies trail deletion.	EVD-013	July 29: organization trail digests validate for the window; test 7
CI-020	IAM user aws-support-sync, wf-prod-data	wf-prod-data	Removed	Policy detached and user deleted July 8 at 10:00 and 10:01 (RE-157, RE-159), after capture.	EVD-021	July 8: GetUser returns NoSuchEntity; July 31 credential report has no such user
CI-021	Access key AKIAWRFNEXAMPLE00002	wf-prod-data	Removed	Deactivated July 4 at 03:01 (RE-065). Deleted July 8 at 10:00 (RE-158).	EVD-021	July 8: ListAccessKeys returns none
CI-022	Role OrgAccessBackup, wf-prod-lending	wf-prod-lending	Removed	Policy detached and role deleted July 8 at 10:01 and 10:02 (RE-160, RE-161), after capture.	EVD-021	July 8: GetRole returns NoSuchEntity; no role in the organization trusts the attacker's account
CI-023	Ransom note, imaging archive	wf-prod-imaging	Removed	Version deleted July 28 after the object and its metadata were sealed, and before Object Lock reached the bucket on July 30.	EVD-002	July 28: listing has no such object
CI-024	Ransom note, data lake bucket	wf-prod-data	Removed	Deleted July 28 after sealing.	EVD-003	July 28: listing has no such object
CI-025	Ransom note, lending documents bucket	wf-prod-lending	Removed	Deleted July 28 after sealing. The bucket's write events are on since July 31.	EVD-004	July 28: listing has no such object

ID	Item	Account	Status	Closure	Sealed first	Verified
CI-026	Share of the database snapshot copy	wf-prod-lending	Removed	Attribute state captured first (02:03:10), then sharing removed July 4, 02:08:20 EDT (`EV-00632`) by Imani Castell through the break-glass role, after 137 minutes open. The guardrail now denies sharing.	EVD-015	July 4: the attribute lists no account; test 3 on July 27
CI-027	KMS grant, prod-lending key	wf-prod-lending	Removed	Grant state captured first (02:04:30), then the attacker's grant revoked July 4, 02:10:30 EDT (`EV-00636`) by Imani Castell. The RDS service grant was already retired at 00:51:06.	EVD-007	July 4: the attacker's grant is not listed; July 28: the key has no grants
CI-028	Deletion protection on wf-los-prod	wf-prod-lending	Restored	Turned back on Tuesday, July 28. Until then the containment policy was the compensating control. The guardrail denies turning it off.	EVD-014	July 28: the instance shows deletion protection on
CI-029	Applicants' records in the shared snapshot	wf-prod-lending	Accepted	If the copy was made, it cannot be recalled. Probable, with high confidence; not confirmed. Counsel decides what follows.	EVD-013	Nothing in the bank's logs can confirm or rule it out
CI-030	Host access to the application tier	wf-prod-lending	Accepted	No host access observed in the reviewed records; host compromise cannot be ruled out with the collected evidence. No change needed.	EVD-018	July 5: the application and load-balancer logs show no known attacker traffic
CI-031	Reads from the imaging archive	wf-prod-imaging	Accepted	Cannot be closed for the past. Read data events have been on since July 31 so the question can be answered from then on.	EVD-027	July 31: read events appear for the two buckets

Other weaknesses closed in week three

Four weaknesses from the root-cause report closed in week three alongside the root causes. The rest are open with dates, in the residual risk below.

Weaknesses from the root-cause report closed by July 31.

ID	Weakness	What changed	Pull request	Reviewer	Merged	Verified
W-1	Other IAM users with long-lived keys	9 IAM users with 11 keys: 5 users deleted, 4 moved to roles	`wf-platform-iac #243`	Imani Castell	July 31	July 31: credential report shows no IAM user with an active key
W-2	Other roles that trust a whole account with no condition	5 role trusts narrowed to a named role with a source identity	`wf-platform-iac #244`	Mireille Danvers	July 31	July 31: Access Analyzer finds no unconditioned account trust
W-6	Snapshot and image sharing allowed everywhere	Snapshot sharing denied; block public access on in all 22 accounts	`wf-platform-iac #236`	Mireille Danvers	July 27	July 29: tests 3 and 4
W-7	Per-account trails that an account administrator can delete	Trail deletion and stop-logging denied	`wf-platform-iac #236`	Mireille Danvers	July 27	July 29: test 7; legacy trails retire by August 14

Residual risk

Seven risks remain after week three, and each has an owner and a date. The sweep in week four tests that the closed items stay closed. It does not close any of these.

Residual risk on July 31, with owners and dates.

ID	Risk	Why it remains	Owner	Date
R-1	RC-6 is accepted, not fixed. Nine month-end snapshots sit in the workload account, and the central vault is in governance mode.	ACC-1, signed July 31	Imani Castell	December 18
R-2	RC-4 is open for the existing objects. Object Lock covers new versions only; the 286 million objects that existed on July 30 have no retention.	Retention for the existing versions needs an S3 Batch Operations Object Lock retention job, which the bank has not chosen (F-11, planned). It is not accepted in writing. The replication to the vault (rule at 17:05, `EV-01094`; an S3 Batch Replication job over the 286 million current versions at 18:25 on July 8, `EV-01101`) finished July 12 at 21:40, 99 hours 15 minutes later, with 1,206 tasks failed (SrcVersionNotFound) and the 122.6 million noncurrent versions not in its manifest. It makes a copy of the current objects; it puts no retention on the production objects.	Rafael Quintero	September 30
R-3	The management account is outside the reach of any SCP, and the vault's protection of the ten RDS snapshot copies, and of the 46 EBS copies since their lock ended July 20, rests on the vault OU SCP and key availability.	A person with Organizations rights in the management account could change that SCP. The setup role `OrganizationAccountAccessRole`, which the SCP exempted, has been denied by name since 16:45 on July 8 (`EV-01092`), so only the two copy roles, each with MFA and two-person approval, can act in the vault. The management account holds no workloads; break-glass and MFA protect it. A guardrail cannot. The bank decides who holds Organizations rights.	Mireille Danvers	October 30
R-4	Data probably copied out (probable, with high confidence) cannot be recalled if it was, and any use made of it is unknown.	The key calls on July 4 fit the pattern of a snapshot copy. Counsel decides what follows.	Diane Whitcombe	Standing
R-5	Reads from the imaging archive before July 31 are unknown.	Reads were not logged until RC-5 closed.	Mireille Danvers	Standing

ID	Risk	Why it remains	Owner	Date
R-6	The Jenkins controller is now the trust anchor for the build, and its disk was never imaged.	Only its logs were collected (EVD-012). Hardening the controller is not in the Recovery's scope.	Imani Castell	September 15
R-7	Four weaknesses from the root-cause report are open with dates (W-3, W-4, W-5, and W-8), and the legacy trails in W-7 retire by August 14.	They need change windows or the bank's decisions.	Mireille Danvers	September 30

Notice

Wrenfield is fictional. Its people, customers, accounts, figures, and attacker are invented for this sample, and any resemblance to a real bank, company, person, or threat group is coincidental. The attacker's addresses come from ranges reserved for documentation.

© 2026 Vantalect, LLC. Sample deliverable; Wrenfield Bancorp, Inc. is fictional.

AWS, Amazon Web Services, and the AWS service names are trademarks of Amazon.com, Inc. or its affiliates. MITRE ATT&CK is a registered trademark of The MITRE Corporation. PostgreSQL is a registered trademark of the PostgreSQL Community Association of Canada. Other product names are trademarks of their owners. Vantalect is not affiliated with or endorsed by any of them. Wrenfield Bancorp, Inc. is fictional.