

PC-SAMPLE-SEC-01 / EN / V1.1

Landing zone security assessment

ILLUSTRATIVE SAMPLE • FICTIONAL SCENARIO

PREPARED FOR
PREPARED

Orivane Industrial Group
2026-07-10

Decision brief

This report presents an original fictional scenario. Orivane, its people, suppliers, systems, records and results are invented; established technology names identify the example stack only. No client material was used. Example hostnames use the reserved .example domain.

Nacre, Orivane Industrial Group's AWS landing zone, provides the shared accounts, access rules and network services for its applications. It separates business applications from shared services, but two weaknesses must be fixed before expansion. The build server nacre-build-03 is accessible from the internet and can use LedgerFlow's ReleaseDeploy role. Application administrators can also change where their own audit logs are sent. An attacker could use these permissions to change production software and hide the evidence.

The review covers all 48 AWS accounts: organization policies, access, deployment, network connections, data protection and recovery. We recommend keeping current services running, removing unnecessary access between accounts, and checking that prohibited actions are blocked before adding new applications.

Decisions requested

DECISION	REASON
Hold expansion	Keep services running; add production accounts only after the required controls pass their tests.
Limit deployment access	Separate build and release identities before widening audit permissions or rotating credentials.
Schedule recovery testing	Reserve application-owner time for isolated restoration and dependency validation.

Orivane: scope and review records

Nadia Bellerose, Chief Information Officer, commissioned review ORV-SEC-2607 before the Nacre expansion. Orivane manufactures industrial components and operates distribution and field-service businesses. Its 2,400 employees work across 18 sites in Canada, the United States and Europe. The six units are Motion, Packaging, Materials, Distribution, Field Service and Corporate.

RECORD	ASSESSMENT BASELINE
Review window	29 June–10 July 2026; evidence cut off at 16:00 UTC on 10 July. Read-only collection and isolated authorization probes.
Account inventory	INV-0710.csv: 48 active accounts; orv-mgmt, orv-secops, orv-log and 45 platform/workload accounts. No suspended accounts.
Approved regions	ca-central-1 (Montréal), us-east-1 (Northern Virginia), eu-west-1 (Ireland). Other enabled regions checked for resources.
Identity evidence	IAM-0709: 312 role-trust documents; 94 cross-account edges reviewed, including 24 production release roles.
Network evidence	NET-0708: 57 VPC attachments, nine transit route tables and 126 approved service flows.
Recovery evidence	BKP-0709: 24 production backup plans. LedgerFlow recovery rehearsal REC-0709 stops before business validation.

Accountable reviewers

Elias Moreno owns Nacre; Maya Dufresne owns security operations; Jonah Patel owns routing; Léa Mercier owns recovery. Tessa Lin accepts LedgerFlow order-processing behavior. Records are indexed in the Orivane evidence library under ORV-SEC-2607. The conclusion applies to baseline nacre-1.3.2, not later changes.

Estate and assessment coverage

Orivane operates 48 AWS accounts supporting six business units in three approved regions. All accounts are represented in the inventory and policy review. Application source-code review, physical security and supplier assurance are outside this assessment. No claim of certification or exhaustive vulnerability discovery follows from the coverage below.

ACCOUNT BOUNDARY	ACCOUNTS
Management	1
Security and log archive	2
Regional networking	3
Shared services	6
Production workloads	24
Non-production	12

Coverage is explicit

DOMAIN	REVIEW METHOD
Organization	Effective policies and account placement for the complete inventory; management-account exceptions kept separate.
Identity and delivery	Role trust, effective deployment permissions, federation claims and approved emergency paths.
Network and data	Route and firewall reachability, private endpoints, bucket and key policies, backup ownership.
Operations	Audit delivery, alert routing, account admission and a representative application recovery sequence.

A missing record remains an evidence gap. It is never counted as a healthy control. The model separates configuration evidence from a successful operational exercise; one cannot substitute for the other.

System boundaries and risk method

Workforce sign-in enters Orivane ID; the Nacre-Platform group receives 60-minute administrative sessions. Approved groups receive short-lived roles in workload accounts. The orv-ci account runs nacre-build-03; the ledgerflow-release workflow deploys into orv-ledgerflow-prod. Regional transit provides access to shared DNS and management services. Audit records leave workload accounts for a separate archive, and recovery copies sit in a distinct administrative boundary.

The account layout is only the starting point. Separation works only when access rules, routing and recovery permissions enforce it. A production account behind a private network can still be exposed through a trusted release role.

Representative attack paths

PATH	PRECONDITION AND CONSEQUENCE
P1 / release	Compromise a build runner → use its trusted role → assume a production release role → alter an application artifact. No user sign-in is required after runner compromise.
P2 / evidence	Obtain workload administration → change audit delivery or its key access → create a monitoring gap. Existing retained records are a separate control to verify.
P3 / recovery	Compromise a workload role → reach backup administration → remove recoverable copies. Backup-job success does not prove isolation.

Evidence required before closure

- ✓ Trace effective caller permissions and target trust together.
- ✓ Exercise the denied path and the approved business path.
- ✓ Retain the policy version, observation and accountable reviewer.

Deployment access: current and proposed

These diagrams isolate the deployment path behind SEC-01. Arrows show authority or an action, not network connectivity. They do not imply that deployment permission automatically includes audit or backup administration.

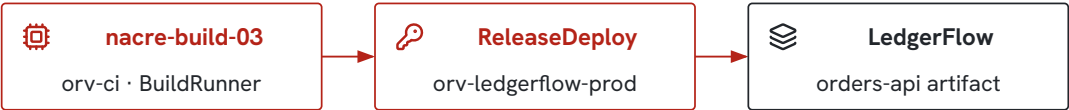


Figure 1 Modeled weakness: build authority reaches production.

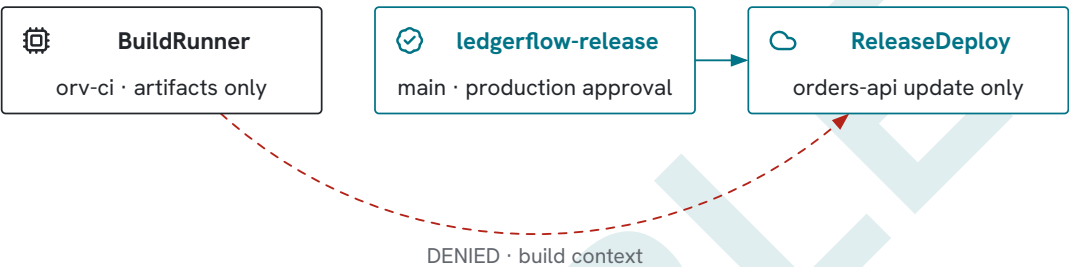


Figure 2 Proposed control: production trusts the approved release context.

Severity key

LEVEL	MEANING IN THIS ASSESSMENT
⚠ HIGH	Access that can affect production or recovery outside its intended scope. Three findings.
⚠ MEDIUM	A control gap depends on another failure or unverified dependency. Three modeled findings.
ℹ LOW	A bounded weakness with limited immediate reach. None assigned in this sample.

Rank considers reachability, required privilege, potential impact and how easily an attack could be detected. Configuration paths remain hypotheses until safely exercised; a diagram does not prove exploitation.

Findings: platform administration

 SEC-01

 HIGH

Build server can deploy to production

IAM-0709 identifies nine of 24 production roles trusting orv-ci/BuildRunner. In probe ID-17, nacre-build-03 assumes LedgerFlow's ReleaseDeploy role and is authorized to update orders-api; no production artifact is changed. A protected repository branch therefore does not prevent a compromised runner from using the already-available role. The decisive evidence is the combination of trust policy, caller permission and an allowed release action, not the existence of a public runner alone.

Separate build and release credentials, constrain the federation subject to an approved release context, and minimize the target role. Confirm that a build-context token fails even when it references a valid artifact. Residual risk remains in the approved release workflow and its maintainers.

 SEC-02

 HIGH

Application administrators can stop audit logs

Logs arrive in orv-log, but WorkloadAdmin can stop the local delivery trail in six production accounts. AUD-12 records an allowed StopLogging decision for orv-dockline-prod; retained archive objects remain protected. Central storage protects neither future collection nor the key path by itself. An attacker could interrupt records before acting; this finding does not claim that already-retained objects can be altered.

Move collection authority into the security boundary and monitor delivery independently of the emitting account. Test attempted disablement, key-access loss and delivery failure. Preserve an independently authorized recovery path so a policy mistake does not make collection irreparable.

 SEC-03

 MEDIUM

Exceptions survive account moves

Seven of eleven exceptions have expired. EX-014 still permits a public endpoint after orv-partsdesk-test moved from Sandbox to NonProduction on 2 July; its 30 June expiry did not trigger a policy review. A temporary permission can outlive its business owner or escape the intended boundary. Require an owner, expiry and effective-policy test at every account move; a stale inventory tag is insufficient evidence.

Findings: application isolation and recovery

⚠️ SEC-04

⚠️ HIGH

Backup and workload administration overlap

All 24 production workloads have backup schedules. BKP-0709 finds RecoveryAdmin assumable by WorkloadAdmin for 18 of them, including LedgerFlow and Dockline; this permits destructive copy administration. A successful backup job measures creation, not survival after compromise. The attack path is a privileged workload session followed by backup-policy or copy deletion authority.

Separate recovery administration, validate retention protections and require a second authority for destructive lifecycle changes. Restore a representative application into an isolated account, including its keys and dependencies. A protected copy that the recovery team cannot decrypt is not usable recovery evidence.

⚠️ SEC-05

⚠️ MEDIUM

Shared routes connect environments that should be separate

The ca-central-1 table nacre-tgw-shared imports 12 non-production and eight production attachments. Probe NET-31 reaches LedgerFlow's application subnet from orv-partsdesk-test; the endpoint firewall denies TCP 5432. Endpoint firewalls block some flows, but the intended environment boundary is absent from routing. A later firewall change could expose services outside its author's assumed scope.

Define permitted source, destination and service triples, then derive route association and firewall intent from that matrix. Verify both forward and return paths, including DNS and inspection. Keep explicit shared-service exceptions; a blanket separation that breaks name resolution is not a workable fix.

⚠️ SEC-06

⚠️ MEDIUM

A successful deployment does not prove readiness

Factory run ACF-218 marks orv-cartonspec-prod ready after deployment, although its audit probe is missing and cost owner is blank. The nacre-1.3.2 workflow has no independent admission step. A new account can therefore enter production with an incomplete operating baseline. Introduce an admission record with positive and negative tests, a named approver and a recoverable quarantine state.

Remediation sequence and ownership

The windows below describe a proposed sequence after approval, not a delivery promise. Owners must confirm access, dependencies and change windows before dates become commitments. Containment precedes broad policy changes; acceptance is attached to the same change record as implementation.

WINDOW	OWNER AND ACTION	CLOSURE EVIDENCE
13 July	Elias Moreno: separate build and release trust. SEC-01 .	Build token denied; approved release succeeds; failed attempt reaches security monitoring.
14 July	Maya Dufresne: protect audit collection and alert on delivery gaps. SEC-02 .	Disablement denied; controlled delivery failure alerts through an independent channel.
20 July	Léa Mercier: separate copy administration and prove decryption. SEC-04 .	Workload administrator cannot delete copies; isolated restore includes dependencies and validation.
22 July	Jonah Patel: constrain transit by approved service flow. SEC-05 .	Forbidden cross-environment flows fail in both directions; DNS and allowed traffic work.
24 July	Elias Moreno: expire exceptions and gate account admission. SEC-03 , SEC-06 .	Account move rechecks policy; failed admission leaves account quarantined; ownership is recorded.

Change safety

Test each policy in a pilot account first. Save the effective policy and role assignments before change. Confirm an independent emergency identity and rollback authority before restricting administration. Stop the rollout if an approved release, audit delivery or essential shared service fails. Restore only the last known safe configuration; reopening an exposed path requires an explicit, expiring risk decision.

Validation record and limitations

Maya Dufresne reviewed the ORV-SEC-2607 evidence index on 10 July. Configuration collection is complete; remediation retests remain open under CHG-2613 through CHG-2617. The entries below identify the collected records and the additional evidence required for closure.

EVIDENCE SET	REQUIRED CONTENT
E1 / INV-0710	Account inventory reconciled to organization membership; unreviewed regions and suspended accounts identified separately.
E2 / IAM-0709	Caller permissions, trust policy and session context for each cross-boundary path; allowed and denied attempts.
E3 / AUD-12	Collection configuration, archive and key permissions, received event and independent delivery-failure alert.
E4 / NET-0708	Approved flow matrix, effective routes and firewall decisions, records of allowed and blocked connections.
E5 / REC-0709	Copy ownership, deletion-denial test, isolated restore log, key access and application-owner validation.
E6 / ACF-218	Account request, effective baseline, exception expiry and signed admission or quarantine decision.

What remains outside the conclusion

The assessment does not establish application-level authorization, resilience under full production load, supplier security or the absence of compromise. Sampling must be widened if the inventory shows another deployment pattern. A finding closes only when the proposed control is effective and its evidence has been reviewed; a merged change alone is not closure.

Reference framework

The domain coverage is informed by the [AWS Well-Architected Security Pillar](#). The scenario, findings and priorities above are original illustrative material, not conclusions supplied by that framework.