

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

Landing zone design and handover

ILLUSTRATIVE SAMPLE • FICTIONAL SCENARIO

PREPARED FOR
PREPARED

Orivane Industrial Group
2026-07-24

Design mandate

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.

Orivane's Nacre platform will support 24 business applications across six divisions. It provides common access, network and recovery controls so each team does not have to build its own. The design uses 48 AWS accounts in three approved regions. Each production application has a separate account; shared services have their own administrators.

This document sets out the design, key decisions and tests required before the operations team takes responsibility. A successful deployment is only one step. Each control needs an owner, a way to detect failure and a recovery procedure.

Design priorities

PRIORITY	DESIGN CONSEQUENCE
Limited administrative access	Workload teams deploy their own services; they cannot administer organization policy, audit archives or recovery copies.
Consistent account approval	A new account follows the same request, baseline, verification and ownership workflow as an existing account.
Recoverable change	A failed platform rollout can be stopped by wave; recovery does not depend on the identity being repaired.
Clear operating costs	Each workload has a cost owner and a budget signal; allocation is distinct from authorization to spend.

Workload application design, commercial licensing and continuous managed operations require their own scope. The platform provides interfaces and runbooks for these responsibilities; it does not silently absorb them.

Nacre project baseline

Nadia Bellerose sponsors programme NCRE-26. Elias Moreno owns the platform and Maya Dufresne approves its security boundary. This 24 July design follows ORV-SEC-2607 and specifies baseline nacre-1.4.0. The design is accepted for implementation; production admission remains subject to the gates in this report.

INTERFACE	AGREED BASELINE
Account authority	orv-mgmt owns organization policy. orv-secops receives detections; orv-log retains audit evidence. orv-recovery is one of six shared-service accounts.
Delivery system	Repository platform.orivane.example/nacre; module release 1.4.0; account manifest accounts-0724.yaml; change series CHG-2620-2625.
Regional placement	ca-central-1: Canadian manufacturing and distribution; us-east-1: US distribution and recovery; eu-west-1: European operations.
Identity and naming	Orivane ID federation; Nacre-Platform privileged group; prod.orivane.example and lab.orivane.example zones owned by Jonah Patel.
Service objectives	LedgerFlow and Dockline: RTO 60 min, RPO 15 min. ForgeTrack and MarginLedger: RTO 4 h, RPO 1 h, subject to rehearsal.
Operating allocation	CAD 185,000 monthly planning envelope; six cost centres owned by Celia Hart. Alerts at 70%, 90% and 100% do not grant spend authority.

RTO is the maximum time allowed to restore service. RPO is the maximum acceptable loss of recent data, measured in time. Both must be verified through recovery exercises.

Ownership and working records

Tessa Lin owns LedgerFlow, Marc Bellamy owns ForgeTrack and Léa Mercier owns recovery. Amira Chen independently verifies account admission. DEC-024 records the account-per-workload decision; EX-019 permits the MillWatch legacy endpoint until 30 September. The exception expires rather than becoming a second permanent baseline.

Account topology and decision record

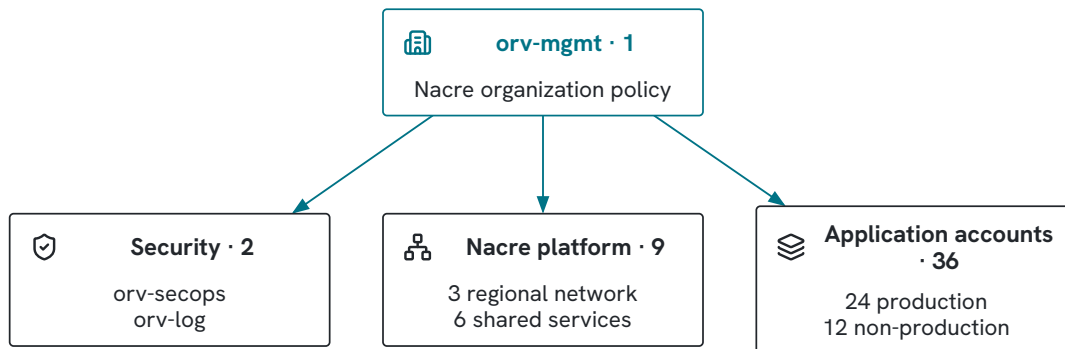


Figure 1 Account groups and policy scope. Arrows indicate governance, not network access.

The total is 48 accounts. Production gets one account per workload in this model; non-production is pooled by team and sensitivity. Regions are deployment locations, not additional accounts. The management account hosts no business workload.

ADR-01 / Separate production by ownership

Account-per-workload production boundaries make permissions, budgets and incident containment attributable. The alternative, one production account per business unit, reduces account administration but couples unrelated release roles and recovery authority. The design accepts the account-management overhead and automates baseline changes centrally. Shared non-production accounts may not hold production data without an explicit exception.

ADR-02 / Centralize policy, distribute delivery

Platform owners maintain guardrails and account interfaces. Application teams own workload configuration and release approval. Organizational policy establishes permission ceilings; it does not grant access or replace workload-level permissions. The management boundary needs its own tighter operating procedure because it is managed differently from the application accounts.

Identity and control ownership

Workforce access uses federation and short-lived sessions. Human administration, automated deployment and emergency access are separate paths. The account baseline exposes documented role interfaces rather than a shared administrator credential. Every privileged assignment has an owner and a review point.

CONTROL	OWNER	EVIDENCE BEFORE HANDOVER
Organization policy	Maya Dufresne approves; automation applies reviewed versions.	Forbidden changes denied in a canary member account; effective policy retained.
Deployment identity	Tessa Lin approves LedgerFlow target permissions.	Approved release succeeds; build context and unrelated repository fail.
Audit and detection	Maya Dufresne owns orv-log and the SecOps queue.	Test event received and triaged; delivery failure generates a separate alert.
Recovery authority	Léa Mercier owns orv-recovery and destructive-change approval.	Isolated restoration works without workload-administrator credentials.
Emergency access	Elias Moreno authorizes; Maya Dufresne reviews afterward.	Independent sign-in exercised; notification and credential renewal recorded.

Permission boundaries in practice

A platform administrator does not automatically become an application data reader. A release identity may update approved infrastructure without permission to weaken its own trust policy. Exceptions identify the permission being widened, the business owner and an expiry. Renewal requires evidence that the underlying constraint still exists; an exception is not a permanent second baseline.

Connectivity and data interfaces

Each region has an explicit transit boundary. Separate routing rules govern production, test environments and shared services. Shared DNS (name resolution) and traffic inspection are available only to approved applications. Access to them does not open every shared subnet. Region-to-region paths exist only for documented application or recovery dependencies.

SOURCE	DESTINATION	CONTRACT
LedgerFlow	nacre-dns-ca	Only approved resolver endpoints and zones; queries and forwarding failures observable.
LedgerFlow API	ledgerflow-db	TCP 5432 from the API subnet only, with symmetric return; owner approves changes to either side.
orv-partsdesk-test	LedgerFlow prod	Denied by default; synthetic test verifies the boundary after every routing change.
ledgerflow-release	AWS API	Scoped identity, regional endpoint policy and audited change context.
orv-recovery	Vault LedgerSafe	Independent authority; restore traffic does not inherit normal production connectivity.

ADR-03 / Central inspection where it has an owner

Central inspection gives policy consistency but introduces shared throughput and failure dependencies. Size it against modeled concurrent traffic and test degradation before adopting it as a mandatory path. Traffic that cannot tolerate the dependency needs an approved local control, not an undocumented bypass. Data classification and key ownership remain application responsibilities even when traffic crosses a central appliance.

Account approval and failed checks

The workflow keeps provisioned accounts outside production until the deployed baseline is independently verified. A failed check produces a recoverable quarantine state. Corrections reenter the same versioned workflow; changing an inventory label cannot admit an account.

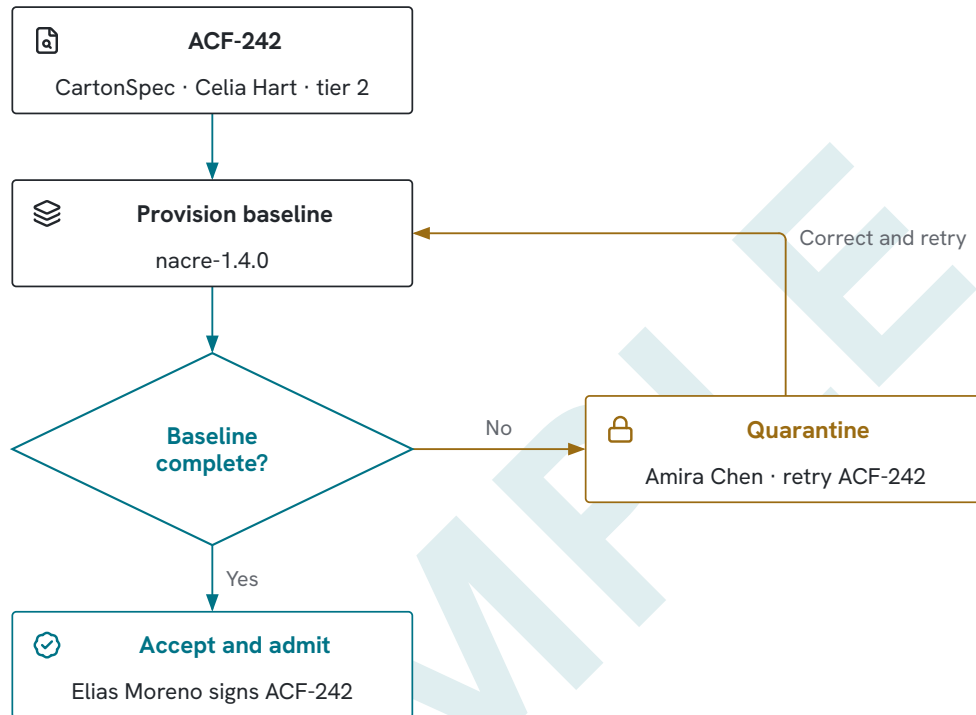


Figure 2 Account admission is an explicit decision with a correction loop.

Required gate evidence

- ✓ An independent observer receives audit events and a delivery-failure alert.
- ✓ Approved actions succeed; forbidden identities and network paths remain denied.
- ✓ Owner, cost allocation, exception expiry and the deployed version are recorded.

Account lifecycle and baseline delivery

An account request is a controlled change. The requester supplies workload owner, environment, data classification, approved regions, cost allocation and recovery tier. Missing ownership stops admission before resources become somebody else's operational problem.

STAGE	ACTION	EXIT CONDITION
1 / approve	Review ownership, placement and exceptions.	Named approver accepts the account contract.
2 / provision	Create account and attach reviewed baseline.	Automation is repeatable; a retry resumes safely rather than duplicating resources.
3 / connect	Configure identity, audit, DNS and permitted network flows.	Expected events and service probes are visible from independent observers.
4 / verify	Exercise allowed and denied operations.	Test record matches the deployed policy version; failures leave account quarantined.
5 / admit	Transfer workload responsibility and cost ownership.	Owner accepts runbooks and alert routes before first production deployment.
6 / retire	Remove access and dependencies; preserve required records.	Data disposition and retained evidence approved; routes, budgets and inventory reconciled.

Shared configuration updates

Version the baseline and roll it out through canary, non-production and production cohorts. Keep workload-specific values outside shared modules. A drift report distinguishes authorized exceptions from unreviewed changes and records which desired version each account should run. Reconciliation must not silently remove a necessary incident containment rule.

Migration waves and stop conditions

The 24 workloads move under NCRE-26 on 11 August, 25 August and 8 September. The inventory below fixes wave membership; placement changes when dependency discovery shows a shared stateful service. A workload is not ready merely because its infrastructure plan is clean. Data movement, user access, certificates, DNS and recovery must fit the same window.

WAVE	WORKLOADS	ADMISSION EVIDENCE
11 Aug · Alder	4	PolicyShelf, ShiftBoard, FieldNotes, CartonSpec. Amira Chen verifies rebuild and rollback without production writes.
25 Aug · Birch	8	ToolVault, LabelWorks, GradeBook, MillWatch, RouteDesk, FreightLens, PartsDesk, PeopleDeck. Prove identity, routes and alerts.
8 Sep · Cedar	12	ForgeTrack, AlloyPlan, PackFlow, LinePulse, StockBridge, BatchTrace, LedgerFlow, Dockline, ServiceAtlas, WarrantyDesk, MarginLedger, Partspan. Rehearse stateful recovery.

Stop the wave when evidence changes

Stop if audit receipt fails, an unexpected privilege appears, a forbidden network path opens, or recovery cannot meet the workload's approved objective. Keep unaffected workloads on their accepted baseline. The incident lead decides whether to roll back, contain or fix forward; the deployment tool must not make that business decision by timeout alone.

Before moving a stateful service, record the last recoverable point and the consequence of post-cutover writes. Reverting infrastructure does not reverse database writes or messages already delivered. If rollback would lose accepted transactions, stop new writes and use the approved reconciliation procedure before moving traffic.

- **Approval responsibilities**

Elias Moreno approves baseline readiness. Tessa Lin approves LedgerFlow behavior and data integrity. Neither can sign for the other.

Handover and operating acceptance

DELIVERABLE	ACCEPTANCE TEST
Platform repository	A second engineer creates a canary account from the documented workflow without author assistance.
Architecture decisions	Owners can explain account boundaries, approved exceptions and the consequences of changing them.
Control evidence	Allowed and denied identity, network and policy tests reference the deployed baseline version.
Operating runbooks	Duty staff receive an alert, identify the affected owner and perform a safe diagnostic action.
Recovery package	A service is restored in isolation with keys, dependencies and application validation.
Inventory and cost map	Every active account has a workload owner, cost owner, lifecycle state and exception review date.

Open decisions at the handover checkpoint

At the 24 July checkpoint, Cedar admission remains conditional on REC-2619 proving ForgeTrack's four-hour recovery objective and CHG-2625 validating Jonah Patel's DNS alert escalation. Léa Mercier and Jonah Patel present evidence on 31 July. These are explicit hold points, not implied acceptance. The handover record lists the evidence still missing, the accountable role and the next review. A warranty for delivered work is separate from an ongoing monitoring or on-call service.

Reference and assumptions

The [AWS Well-Architected Reliability Pillar](#) provides a general review lens for change and recovery. The topology, workload distribution, migration plan and acceptance contract are original design examples. Sizing, legal retention and service objectives must be established for a real estate before implementation.