SOP: First-Time Deployment of a New Application to the Operations Center

Document ID: OPS-SOP-NEWAPP-001
Applies to: All DevNest product teams and Platform Ops
Environment: DevNest Cloud (prod + pre-prod)
Change Type: *Net-New Application Onboarding*
Risk Tier: Defaults to **Tier-1** until assessed; Tier-0 requires CRO sign-off.

1) Purpose

Process for onboarding and deploying a new application into DevNest production environment, ensuring:

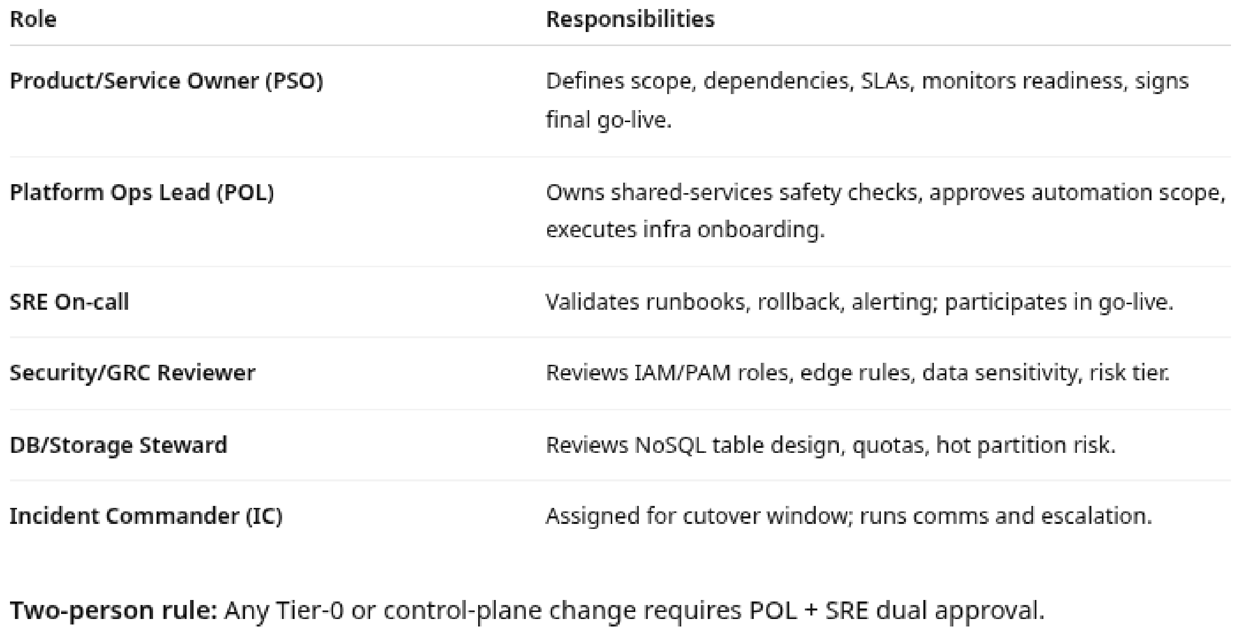
- Safe integration with shared services
- Validated blast radius and dependency accuracy
- Audit-defensible change management
- Operational readiness including monitoring, runbooks, KRIs, and ownership

2) Scope

Cvers the **first ever** deployment of a **new product service or microservice group** into:

- Production
- Pre-production environments that are production-connected
    - e.g., shared NoSQL, shared IAM
- Does **not** apply to routine deployments to an already-onboarded application.
    - Those follow OPS-SOP-DEPLOY-002.

3) Roles & Responsibilities (RACI)



Role	Responsibilities
Product/Service Owner (PSO)	Defines scope, dependencies, SLAs, monitors readiness, signs final go-live.
Platform Ops Lead (POL)	Owns shared-services safety checks, approves automation scope, executes infra onboarding.
SRE On-call	Validates runbooks, rollback, alerting; participates in go-live.
Security/GRC Reviewer	Reviews IAM/PAM roles, edge rules, data sensitivity, risk tier.
DB/Storage Steward	Reviews NoSQL table design, quotas, hot partition risk.
Incident Commander (IC)	Assigned for cutover window; runs comms and escalation.

Two-person rule: Any Tier-0 or control-plane change requires POL + SRE dual approval.

4) Preconditions / Entry Criteria

All items must be complete before scheduling Day-0 deployment.

4.1 Documentation

- Application scope + owner documented in Service Catalog.
- Dependency Map completed and reviewed by Platform Ops.
- Risk Tier assigned (Tier-1 default; Tier-0 if systemic).
- Runbook v1 drafted (startup/shutdown, health checks, rollback, common errors).
- Support boundaries defined (what Ops vs Product handles).
- SLA/SLO targets proposed.

4.2 Technical Readiness

- Code in main branch with CI passing.
- Container images built and scanned.
- IaC (Terraform/CloudFormation) reviewed and merged.
- Service tags validated (see §6).
- IAM roles created, least-privilege verified.
- NoSQL tables/streams provisioned with quotas reviewed.
- Edge/WAF baseline ruleset approved.
- Observability instrumentation (logs/metrics/traces) integrated.

5) Change Management Requirements

1. **Change ticket required** in ChangeHub:
   - Type: Net-New Application
   - Risk tier, blast radius, rollback plan mandatory
2. **Peer review mandatory**
   - If emergency override is used → deployment is **blocked** pending CRO approval
3. **Change window**
   - New apps deploy **only during standard window** unless Tier-0 incident case

6) Tagging & Automation Safety (Critical)

Because DevNest automation scopes by tags, incorrect tagging can create systemic blast radius.

6.1 Required tags for new apps

Every new service must have:

- `product.<line-of-business>` (e.g., `product.commerce`)
- `tier.<0|1|2>` (temporary Tier-1 until assessment)
- `platform.shared=false`
- `automation.scope=app-only` (blocks controlplane rollouts)
- `owner.<team>`

6.2 Forbidden tags for new apps

Do not apply any of these:

- `controlplane.*`
- `platform.shared`
- `critical.tier0` (unless approved)

6.3 Tag validation step

Platform Ops must run:

- `scope-lint inventory.yaml --service <newapp>`
- `automation-dryrun --tags <newapp tags>`

Exit criterion: Dry run must show **only the new app** in scope.

7) Step-By-Step Procedure

Phase 1: Intake & Scoping (T-10 to T-5 business days)

1. **Submit Net-New Application Onboarding Form**
    - app name + owner
    - intended LOB
    - risk tier proposal
    - dependency list
    - data classification
2. **Platform Ops review meeting**
    - validate shared-service dependencies
    - confirm tag set
    - identify systemic collision risks
3. **Security/GRC review**
    - IAM roles, PAM needs, edge exposure, data sensitivity
4. **Storage review**
    - NoSQL design, indexes, quota, expected R/W patterns
5. **Approve move to pre-prod onboarding**

Output: Approved onboarding plan + change ticket opened.

Phase 2: Pre-Production Onboarding (T-5 to T-2)

1. **Provision infrastructure via IaC**
    - VPC/net permissions
    - compute (K8s namespace/ECS service)
    - NoSQL tables/streams
    - secrets in vault
2. **Register service in DNS/Discovery**
    - create **app-scoped** discovery records
    - validate records resolve to test endpoints
3. **Configure Edge/WAF (pre-prod)**
    - baseline ruleset

    - rate limiting thresholds
    - bot score/challenge parameters
4. **Integrate IAM**
    - workforce/admin roles
    - service-to-service token policies
5. **Instrument Observability**
    - service dashboards created
    - SLO alerts configured
    - logs searchable in central stack
6. **Run pre-prod deployment**

    -
      ```
      cicd deploy --env preprod --scope app-only
      ```

Exit criteria

- pre-prod health checks green
- edge/WAF rules stable
- NoSQL throughput within bounds
- dashboards show correct signals
- rollback tested once in pre-prod

Phase 3: Go-Live Readiness Review (T-2 to T-1)

1. **Operational Readiness Review (ORR)**
    - PSO + POL + SRE + Security in 45-min gate
2. Confirm:
    - runbook v1 complete and accessible
    - on-call rotation defined
    - escalation paths confirmed
    - KRIs/KPIs defined (see §9)
    - rollback plan real and time-boxed
3. **Approve production window**

Output: ORR approval recorded in change ticket.

Phase 4: Production First Deployment (Day 0)

Participants on bridge: Primary Service Owner, Primary Operations Lead, SRE on-call, IC, Security on standby

1. **Start change bridge**
    - IC opens incident channel (even if not an incident)
    - POL confirms scope lint passed
2. **Freeze unrelated deploys** in same LOB for window
3. **Deploy to production**
    - `cicd deploy --env prod --scope app-only`
4. **Validate service discovery**
    - check internal DNS resolution
    - verify no cross-service record edits
5. **Validate edge/WAF**
    - confirm ruleset version matches approved SHA
    - run synthetic traffic tests
6. **Health checks**
    - app liveness/readiness
    - dependency calls to IAM, NoSQL
7. **Enable traffic gradually**
    - 5% → 25% → 50% → 100%
    - observe retries, latency, throttling
8. **Declare stable**
    - 30 minutes at 100% traffic without SLO breach

Exit criterion: PSO + POL sign go-live complete.

Phase 5: Post-Deployment Monitoring (Day 0 to Day 7)

1. **Enhanced monitoring mode (72 hrs)**
    - no config changes without POL approval
2. **Daily health check summary to Ops Center**

    - key KRIs / incidents / anomalies

3. **Week-1 retrospective**
    - confirm risk tier finalization
    - tune alerts/thresholds
    - update run-book v1 → v1.1

8) Rollback Procedure (First Deployment)

Rollback must be executable **even if Identity or Edge are degraded.**

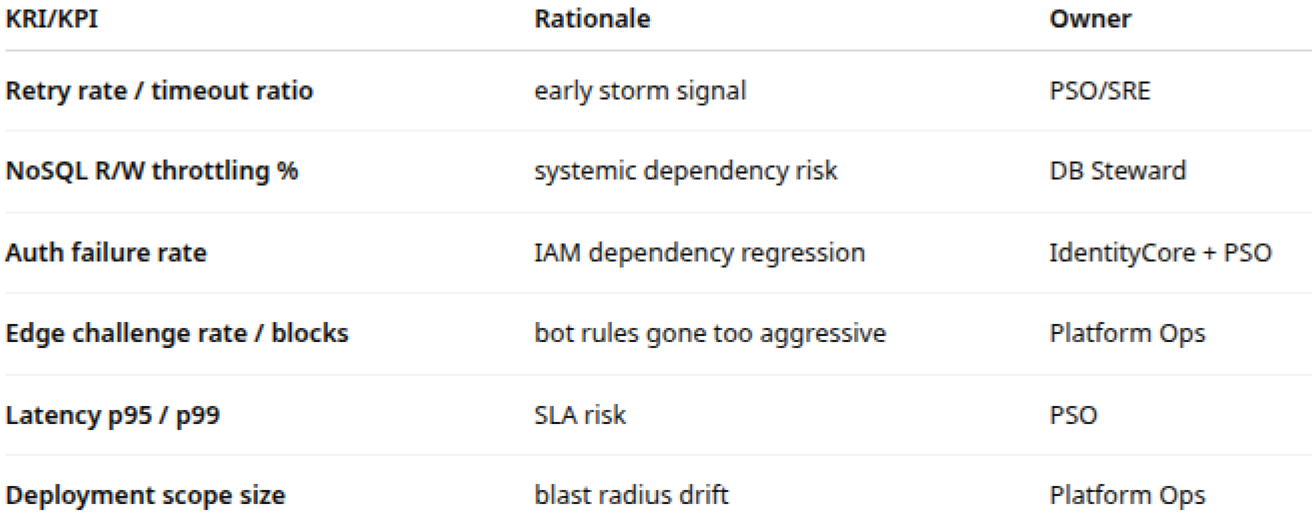
1. **Trigger rollback** if any are true:
   - P1 incident declared
   - sustained 5xx > threshold
   - NoSQL throttling rising continuously
   - auth failures > 2× baseline
2. **Rollback command**

   -
     ```
     cicd rollback --env prod --service <newapp> --scope app-only
     ```
3. **Disable edge routing**
   - revert edge ruleset to previous stable version
4. **Validate dependency stability**
   - confirm no DNS drift
   - confirm NoSQL recovery trend
5. **Post-rollback comms**
   - IC posts summary and time to restore

Rollback must complete in ≤**15 minutes** for Tier-0 services, ≤**30 minutes** Tier-1.

9) Required KRIs/KPIs (First-Week Set)

New apps must publish and alert on minimum KRIs:



KRI/KPI	Rationale	Owner
Retry rate / timeout ratio	early storm signal	PSO/SRE
NoSQL R/W throttling %	systemic dependency risk	DB Steward
Auth failure rate	IAM dependency regression	IdentityCore + PSO
Edge challenge rate / blocks	bot rules gone too aggressive	Platform Ops
Latency p95 / p99	SLA risk	PSO
Deployment scope size	blast radius drift	Platform Ops

Thresholds must be documented in runbook.

10) Evidence & Audit Artifacts

Ops Center retains:

- change ticket + approvals
- ORR checklist
- tag lint report
- CI/CD run logs for deploy + rollback test
- edge ruleset SHA
- NoSQL provisioning plan
- dashboards + alert definitions
- week-1 retrospective action list

11) Common Failure Modes & Mitigations

1. **Mis-tagging Appendix: ORR Checklist (Quick Form)**
2. **Scope**

- Service catalog entry complete
- Dependency map validated
- Risk tier assigned

3. **Safety**

- Tags validated + no forbidden tags
- Automation dry run clean

4. Two-person approval if Tier-0**includes controlplane scope**
    - mitigated by mandatory lint + dry run
5. **NoSQL hot partitions during ramp-up**
    - mitigated by staged traffic + quota review
6. **Edge rules overly strict**
    - mitigated by pre-prod synthetic tests + gradual enablement
7. **Monitoring blind spots**
    - mitigated by ensuring telemetry survives NoSQL degradation
8. **Rollback depends on SSO**
    - mitigated by break-glass + out-of-band tooling

12) Appendix: Operational Readiness Review Checklist

Scope

- Service catalog entry complete
- Dependency map validated
- Risk tier assigned

Safety

- Tags validated + no forbidden tags
- Automation dry run clean
- Two-person approval if Tier-0

Operations

- Runbook v1 complete
- On-call ownership confirmed
- Rollback tested in pre-prod

Monitoring

- Dashboards created
- KRIs/KPIs defined with thresholds
- Alerts route to correct on-call

Sign-offs

- PSO (Product Service Owner)
- POL (Platform Operations Lead)
- SRE (Site Reliability Engineering)
- Security