Decide whether the release can be operated.

Production readiness covers deployment, observation, recovery and the people responsible for the system.

Production readiness review

Gate	Evidence before release
Deployment	A repeatable path using the tested artifact
Configuration	Required settings and secrets available in the target environment
Observation	Useful health checks, traces and alert ownership
Recovery	A rehearsed rollback or restoration path
Support	Runbooks, access and escalation responsibilities agreed

Verify the complete business workflow

A successful process start or health endpoint is not enough. Exercise authentication, data access and important external dependencies in the target environment.

Resolve ownership before approving the release

A documented recovery procedure is not usable if nobody can access the system or authorise the action when it is needed.

Define readiness for the intended release

Production readiness depends on what the system will do, who will use it and the consequence of failure. An internal pilot with reviewed outputs has a different risk profile from an unattended workflow that updates financial records. State the intended audience, data and operating scope before deciding which evidence is needed.

Identify critical user journeys and the external systems they rely on. Confirm that acceptance examples cover ordinary work and important exceptions. Record known limitations and decide how they will be communicated. A release should not be described as ready simply because its feature list is complete. The operating team must also be able to identify problems and take an appropriate recovery action.

Rehearse the boundaries that matter

Test identity and permissions using representative roles. Confirm that configuration, secrets and environment access are available through approved processes. Exercise an unavailable dependency and a repeated request, and inspect the resulting business state. For AI, include unsupported answers, restricted sources and tools that require approval.

Review deployment and recovery together. Establish which version can be restored, whether data changes remain compatible and what must be reconciled after interruption. A backup should be tested with the application and its supporting configuration, not merely checked for the presence of a file. Record the observed result and any remaining steps that depend on another team or provider.

Make the launch decision explicit

Bring the evidence to the people responsible for the business workflow and the running service. Separate release-blocking failures from limitations that can be accepted within a narrower scope. Record the owner and review condition for each accepted issue. Agree the initial monitoring period and the route for user feedback.

The final record should identify the version released, the scope approved, the evidence reviewed and the person authorised to proceed. Keep it linked to the deployment. Revisit readiness when the system gains a new user group, source collection or consequential action. This guide supports an engineering release decision and does not substitute for the organisation's own legal, security or procurement approvals.

Does completing this checklist guarantee a safe release?

No. It structures the review. Acceptance depends on the workload, the evidence and the risks the accountable owner agrees to retain.

Read the current resource online

https://cobnex-review.rgcsekaraa.workers.dev/resource/app-innovation-report/