



PRODUCT DEVELOPMENT

Software launch readiness checklist

Verify the release and its operating conditions

Review a release across functionality, access, data, recovery, monitoring and support. Use explicit acceptance conditions and an accountable launch decision to control the transition into production.

THE WORK

Review an identifiable release candidate with the product, delivery, operational and relevant specialist owners.

THE RESULT

A recorded release decision, ordered rollout and explicit pause, recovery and acceptance conditions.

INSIDE THIS GUIDE

02 Release scope

04 Security, data and capacity

08–09 Readiness checks

03 Product behaviour

05–07 Recovery and operation

10 Release decision

Release identity and scope

Purpose and owners

A release is ready when the team can identify what will change, demonstrate the important behaviour, operate the resulting service and respond if the change fails. Passing a test suite is one part of that decision. Access, data, monitoring, support and recovery also need to be ready for the same release.

Use this checklist for a named release candidate and production environment. Bring the product owner, delivery lead and operational owner together around a single readiness record. Involve security, data or business specialists where the change affects their responsibilities.

The output is a recorded release decision, an ordered rollout plan and a clear set of conditions for pausing or recovering. Reopen the relevant checks if the release candidate, configuration or deployment scope changes after review.

Identify the deployed change

Record the release identifier, source revision or build, target environment and deployment window. Include configuration, infrastructure, database, integration and feature-flag changes in the scope. A release description should make it possible for somebody outside the development team to understand which service behaviour will change.

Confirm that the tested artifact is the artifact being deployed. Preserve the build and configuration information required to reproduce it. Identify dependencies that must be released before or alongside the change, and confirm the owners of those activities.

Document the affected users and business processes. Check whether the change alters permissions, notifications, pricing, transaction processing, reports or data retention. Include any required customer or staff communication in the release plan.

Establish the acceptance owner and the person authorised to pause the rollout or initiate recovery. Keep their contact route available during the release window. If a required approver or technical owner is unavailable, resolve coverage before the release begins.

02 / REVIEW

Verify product behaviour

Critical tasks and recovery

Start with the customer and operator tasks that the release affects. Check the successful path, relevant exception paths and recovery from interruption. Preserve the test conditions and results so the acceptance decision can be traced to a specific version and environment.

Verify validation and error messages with the underlying failure conditions. Confirm that a person can understand what happened, what remains saved and what they can do next. Examine duplicate submissions, retries, expired sessions and partial completion where they can affect the service.

Permissions, access and defects

Check permissions from the perspective of each relevant role. A control being hidden in the interface does not establish that access is restricted in the underlying service. Confirm that a user cannot retrieve or change another user's protected information through a direct request or changed identifier.

Inspect the experience on the devices and accessibility arrangements relevant to the audience. Include keyboard access, focus behaviour, labels, readable errors and completion of the essential task with the required assistive tools. Record unresolved barriers with their actual consequence and release decision.

Connect every release-blocking issue to its resolution or explicit authorised decision. Do not let the absence of a ticket label substitute for a review of the defect's consequence.

03 / REVIEW

Security, data and capacity

Access, secrets and information

Confirm the production access model, administrative roles and ownership of service accounts. Remove development access and diagnostic settings that are inappropriate for the operating environment. Verify that secrets are managed through the approved mechanism and are not exposed in client code, build output, logs or shared release notes.

Review changes to collected information, retention, consent and access. Confirm that integrations receive only the information required for their function. Check the operational route for correcting, deleting or restricting records where the service requires it.

Demand and external constraints

Review the expected demand and the evidence supporting it. Check the service under the important operating conditions, including background work, integration delays and recovery from dependency failure. Use workload and acceptance thresholds appropriate to the service; retain their definitions in the readiness record.

Confirm production quotas, connection limits, storage capacity, certificates, network routes and access to required external services. Identify the owner and response route for dependencies the team does not control. Check scheduled jobs and time-sensitive activity around the proposed release window.

Exposure and transaction boundaries

Assess relevant dependency and application security findings. Assign the decision on any unresolved exposure to the authorised owner. Record the consequence, temporary control, review point and condition for closure. A scanner result is an input to this review; the team still needs to understand the affected path and deployed configuration.

For changes involving payment, identity or sensitive records, inspect the entire transaction boundary. Verify the relationship between a customer-visible result, the authoritative system state and the notification or downstream action triggered by it.

Failure handling and configuration

Inspect timeouts, retries and queue behaviour. A retry policy can increase load during an outage, and a successful request may still lead to duplicate downstream work if the transaction boundary is unclear. Confirm how the service detects duplication, preserves state and recovers from partial processing.

Verify that the production configuration matches the assumptions used during testing. A difference in permissions, scale, routing, feature flags or data shape can materially change the behaviour of an otherwise identical build.

Recovery and observability

Order and rehearse the data work

Identify every schema change, migration, backfill and data transformation. Establish the source of truth during the rollout and the compatibility required while old and new application versions may coexist. Confirm the order in which application and data changes must occur.

Rehearse consequential data operations using representative structure and an approved data-handling arrangement. Record elapsed time, validation results and the recovery route. Verify backups through restoration where the release depends on them, including configuration and access required to use the restored service.

Signals, baseline and response

Confirm which signals will show that the important tasks are working. Include service errors, latency, transaction outcomes and dependency health where relevant. Establish a baseline before changing the service so the team can interpret the new observations.

Check that alerts reach a named, available responder. Test the route and confirm access to the information needed for investigation. Use logs and traces that connect an incident across components without unnecessarily exposing sensitive information.

Preserve work created after release

A previous application build may be unable to read data written by the new release. Check that limitation before describing a deployment rollback as the recovery plan. Decide how transactions created after the change will be preserved or reconciled, and who can authorise the required business decision.

State the last safe point for returning to the earlier state. If the release passes that point, document the available recovery options, their consequences and the owner of the decision. Keep the relevant tools, credentials and operating instructions available throughout the release.

Analytics and operating support

Verify essential analytics events against the actual action they represent. Check the release does not duplicate events, omit important states or change the definition of a business measure without notice. Keep product reporting distinct from operational health signals when they serve different decisions.

Provide the support team with the change summary, known limitations, affected customer journey and escalation route. Update the operating guidance at the same time as the product. Confirm ownership for the first operating period after release and for the eventual handover to normal support.

Run an ordered rollout

Sequence and staged exposure

Write a sequence that another authorised operator can follow. Each consequential step should identify the owner, the required action, the expected evidence and the condition for continuing. Include preparation, release verification, traffic or feature enablement, validation and final acceptance.

Use staged exposure where it suits the architecture and risk. Define what the first stage covers, what will be observed and what permits expansion. A small initial audience reduces exposure only when the relevant failures can be detected and the team can act on them.

Intervention and actual state

Set pause and recovery conditions before the rollout begins. Choose thresholds and decision rules appropriate to the affected service, including serious correctness or access failures that may require action even at low volume. Avoid changing the acceptance rule during the release simply to continue the rollout.

Maintain one release record as work proceeds. Record actual completion times, material deviations, decisions and the people making them. Confirm the final production state rather than relying only on a successful deployment job.

Accept the service into operation

Production verification and observation

Verify the important customer and staff tasks in the deployed environment using approved accounts and transactions. Confirm that required jobs, notifications, reporting and support routes work with the new state. Reconcile consequential records where the rollout moved or transformed data.

Keep observation ownership explicit until the release is accepted. The period should reflect the service's operating cycle and the changes made. A task that runs overnight or at a particular business event may need observation after the deployment team would otherwise finish.

Decision and ongoing ownership

Record the decision as approved, held or approved with defined conditions. For a conditional decision, state the owner, temporary control, expiry or review point, and the condition that would trigger intervention. Confirm who accepts the service into normal operation.

Carry unresolved work into the team's normal tracking process with its original consequence and owner. Retain the release record, build identity and recovery information so a later incident can be investigated against the actual change.

07 / VERIFICATION

Launch readiness checks

Mark a condition verified only after reviewing its evidence. Keep unresolved conditions and accepted exceptions in the decision record.

01	Release identity and scope Match the candidate, configuration and dependent changes to the target environment and deployment window.	Evidence to retain Build or revision identity, configuration record, affected-service scope and named release owner.	Verified	☐
02	Product behaviour and exceptions Complete the affected customer and operator tasks, including meaningful failure, retry and access paths.	Evidence to retain Versioned test results, accessibility checks and a decision on each release-blocking defect.	Verified	☐
03	Access and data handling Verify production permissions, secret handling, changed data use and the authoritative transaction state.	Evidence to retain Access review and security/data decisions with owners for unresolved conditions.	Verified	☐
04	Capacity and dependencies Check demand assumptions, limits, certificates, connectivity and behaviour when a dependency is delayed or unavailable.	Evidence to retain Load conditions and results, quota checks and dependency support contacts.	Verified	☐
05	Data migration and recovery Rehearse the data sequence and verify recovery, including the treatment of writes made after the change.	Evidence to retain Migration and restore results, reconciliation method and last safe reversal point.	Verified	☐

08 / VERIFICATION

Launch readiness checks — continued

Mark a condition verified only after reviewing its evidence. Keep unresolved conditions and accepted exceptions in the decision record.

06	Monitoring, alerts and analytics Trigger the relevant signals and confirm a responder receives them; validate the meaning of business events.	Verified ☐ Evidence to retain Alert acknowledgement, diagnostic access and event verification.
07	Support and operating guidance Give support the changed task, known limitations, escalation route and ownership for the first operating period.	Verified ☐ Evidence to retain Current operating instructions and acceptance by the support owner.
08	Rollout and intervention Confirm the sequence, stage-expansion conditions and authority to pause or recover.	Verified ☐ Evidence to retain Ordered rollout plan, decision thresholds and available authorised contacts.
09	Operational acceptance Name who verifies the live service, observes the relevant operating cycle and accepts normal ownership.	Verified ☐ Evidence to retain Acceptance conditions, observation responsibility and an explicit service handover.

09 / DECISION RECORD

Release decision record

Complete the decision against the reviewed configuration. Record unresolved conditions, the authorised owner and the evidence required for acceptance.

Readiness and approval

Release identifier, target environment and deployment window

Readiness evidence and unresolved conditions

Decision and authorised owner

Rollout and acceptance

Pause or recovery condition

Rollout lead and support owner

Production acceptance result and observation owner