

Make one critical workload ready for production.

A decision-ready assessment of the architecture, delivery path, security posture, observability, and operating model behind a fictional commerce workload.

ORGANISATION	Northstar Commerce (fictional)
WORKLOAD	Checkout and fulfilment path
ENGAGEMENT	10 business days
REPORT STATUS	Representative sample - not client data

WHAT THIS SAMPLE IS

The structure and level of specificity are representative. Every organisation, score, metric, and finding in this document is fictional.

The system works. Recovery still depends on people knowing where to look.

READINESS

2.4 / 5

CONDITIONAL

Decision

Proceed with the planned regional launch only after closing the duplicate-order failure mode and demonstrating a rollback against the current database migration path. Both changes fit inside the existing release window; neither requires a platform rewrite.

What is working

The team owns its service, deploys from a consistent pipeline, and has strong infrastructure telemetry. The delivery foundation is sound enough to improve iteratively.

What changes first

Instrument the checkout journey, set a service-level objective, make requests idempotent at the payment boundary, and turn rollback from documentation into a rehearsed operation.

DIMENSION	SCORE	WHAT THE EVIDENCE SHOWED
Reliability and SLOs	2.4 / 5	Availability is monitored, but no service-level objective or error-budget policy drives release decisions.
Delivery flow	3.1 / 5	Automated deployment exists. Production promotion still requires two manual handoffs and cannot be reproduced locally.
Platform self-service	2.0 / 5	A new service takes three to five days and depends on a platform engineer copying an existing repository.
Security and supply chain	2.7 / 5	Images are scanned. Provenance is unsigned, admission policy is advisory, and exceptions are not time-bound.
Observability and response	1.9 / 5	Infrastructure telemetry is strong. User-journey traces, dependency ownership, and a tested rollback path are missing.
Operating model and cost	2.3 / 5	Ownership is understood socially rather than recorded. Cost is visible by subscription, not workload or product.

Four findings. One release decision.

Priority combines user impact, likelihood, detectability, and the effort required to recover. It is not a generic severity score.

01 / CRITICAL	The checkout path can create duplicate orders when the downstream payment call times out.	Add idempotency at the domain boundary and exercise it in a failure-injection test before the next release.
02 / HIGH	Rollback is documented but has not been run against the current database migration strategy.	Make expand-contract migrations the paved road and rehearse rollback in the production-like environment.
03 / HIGH	Deployment identity can change production networking outside the application release boundary.	Split identities by concern, apply least privilege, and fail non-compliant plans in pull requests.
04 / MEDIUM	The platform team is the human interface for every new service and exception.	Ship one self-service service template with clear validation feedback before expanding the catalogue.

Release condition

Items 01 and 02 are release conditions. Items 03 and 04 belong in the first 60 and 90 days respectively. This keeps the launch decision separate from the transformation backlog.

Evidence reviewed

REPOSITORIES	Application, infrastructure, pipeline templates
OPERATIONS	Dashboards, alerts, runbooks, two recent incident reviews
PEOPLE	Product lead, service owner, platform lead, security lead
OBSERVATION	One deployment and one service-creation journey

Reduce risk, rehearse recovery, then remove the queue.

Each window ends in observable proof. A completed ticket is not evidence that the operating condition changed.

WINDOW	OUTCOME	WORK	PROOF
0-30 days	Bound the failure	Set the checkout SLO; add idempotency; narrow deployment identity; instrument the critical journey.	Failure-injection test passes and the SLO is visible to the product team.
31-60 days	Make recovery routine	Adopt expand-contract migrations; automate rollback; write and run the first game day.	A failed release is recovered inside the agreed objective without privileged improvisation.
61-90 days	Remove the queue	Publish one service golden path; embed policy checks; expose actionable pipeline feedback.	A product engineer creates and deploys a compliant service without a platform ticket.

Measures agreed before implementation

Failed deployment recovery time	47 minutes	Under 15 minutes in two rehearsals
New service lead time	3-5 business days	Under 60 minutes without a platform ticket
Critical-journey trace coverage	0%	95% of checkout requests
Policy exceptions without expiry	11	0

THE HANDOVER

The client receives the evidence index, scorecard, architecture and delivery-flow maps, risk register, decision log, implementation backlog, and executive readout. The roadmap remains useful whether Five9s implements it or the client does.