NORTHSTAR CONTROLS

Risk management and compliance audit

Customer-data platform

Internal assurance report
Audit period: Q1 2026

Scope:	Access, change, continuity, and vendor controls
Control owners:	Operations, engineering, security
Overall opinion:	Needs improvement

Fictional example data. Replace findings and control owners with evidence from the live control environment.

Chapter 1

Executive summary

The platform has a workable control framework, but evidence is inconsistent across privileged access and supplier monitoring. No critical breach was identified in the sample. The overall opinion is *needs improvement*: management should close the two high-priority actions before the next customer assurance cycle.

1.1 Opinion and priorities

Severity	Open	Overdue	Priority
Critical	0	0	Immediate
High	2	1	30 days
Moderate	5	2	60 days
Low	4	0	90 days

1. Enforce quarterly recertification for privileged production access.
2. Complete vendor-security reviews for the three subprocessors handling customer data.
3. Add evidence retention and reviewer sign-off to the change-management workflow.

Chapter 2

Risk register

Risk	Exposure	Existing response	Residual view
Privileged access	Excess access could expose customer records.	SSO, MFA, manager approval.	High until recertification is complete.
Change failure	An untested release could interrupt service.	Peer review, staging, rollback plan.	Moderate; evidence sample incomplete.
Supplier breach	A subprocessor could mishandle data.	Contract clauses and annual review.	High for overdue reviews.
Continuity gap	A regional outage could exceed recovery target.	Backups and alternate region.	Moderate; test is scheduled.

2.1 Scoring method

Likelihood and impact are each scored from 1 to 5. Inherent risk is their product; residual risk reflects the control design and operating-effectiveness result. Scores are directional and should be calibrated to the organisation's approved risk appetite.

Chapter 3

Control testing

Control	Sample	Pass	Exceptions	Test note
Identity lifecycle	25	23	2	Leaver access removed late in two cases.
Production access	18	14	4	Recertification evidence missing.
Change approvals	30	28	2	Emergency changes lacked retrospective sign-off.
Backup restoration	4	4	0	Latest restore test met target.
Vendor review	6	3	3	Subprocessor files incomplete.

3.1 Remediation roadmap

0–30 days Security owner closes privileged-access exceptions and records evidence in the control repository.

31–60 days
Procurement completes vendor reviews and attaches current attestations to each supplier record.

61–90 days
Engineering automates change evidence capture and repeats the sample-based test.

Management response

Management accepts the findings. Action owners will report status biweekly to the risk committee; internal assurance will retest the high-priority controls on 30 April 2026.