RESPONSIBLE CLOUD™ · SAMPLE DELIVERABLE

Executive Risk Dashboard

Illustrative organization: Northstar Services · Reporting date: August 2026

Demonstration only: All organizations, findings, values, owners, and dates in this sample are fictional. No client information is used.

Status model: A finding identifies a condition; a recommendation proposes treatment; a client decision records acceptance, rejection, modification, or deferral; implementation records reported completion; verification evaluates agreed evidence; and residual risk records what remains. This sample does not treat those states as interchangeable.

42	6	5	3	$184K
Technology services	AI use cases	Priority risks	Proposed decisions due	Annual technology spend

Executive summary

Northstar has strong leadership engagement but incomplete SaaS ownership, inconsistent privileged-access review, informal AI adoption, and limited evidence that critical-vendor recovery assumptions have been tested. The recommended 90-day plan begins with ownership and visibility improvements before larger technology purchases.

Priority risk register

Priority	Risk and business impact	Proposed owner	Recommended decision / action	Target
High	Shared administrator accounts could prevent attribution and increase the impact of credential compromise.	COO	Approve named administrator model and emergency-access process.	15 days
High	Unreviewed AI tools may receive customer or employee information without approved safeguards.	CEO	Approve interim AI use rules and use-case register.	15 days
High	Critical SaaS recovery depends on vendor assumptions that have not been documented or exercised.	COO	Assign recovery requirements and conduct tabletop exercise.	45 days
Medium	Duplicate and ownerless subscriptions create waste and unmanaged renewal risk.	CFO	Validate inventory and consolidate renewals.	60 days
Medium	Departing-user access review is inconsistent across SaaS providers.	HR Director	Adopt one offboarding checklist with evidence retention.	30 days

Proposed decisions for leadership

DECISION 1

AI guardrails

Recommendation: Approve an interim list of allowed uses, prohibited data, and human-review requirements.

Estimated effort: 12 internal hours plus legal review.

Proposed owner: CEO

DECISION 2

Identity ownership

Recommendation: Fund named administrative accounts and quarterly privileged-access review.

Estimated cost: $3,600 annual licensing plus implementation.

Proposed owner: COO

DECISION 3

Vendor resilience

Recommendation: Establish minimum recovery evidence for critical SaaS providers.

Estimated effort: 20 internal hours plus provider support.

Proposed owner: COO

DECISION 4

Subscription consolidation

Recommendation: Retire unused tools at renewal and require a business owner for new purchases.

Potential reduction: $11,400 annual spend, subject to validation.

Proposed owner: CFO

Recommended 90-day improvement roadmap

Window	Recommended actions	Evidence required for verification
Days 1-30	Confirm inventory owners; approve AI interim rules; replace shared administrator access; adopt offboarding checklist.	Approved policy; named accounts; signed ownership register; access-review record.
Days 31-60	Review critical vendors; consolidate subscriptions; define recovery requirements; document exceptions.	Vendor records; renewal decisions; recovery objectives; exception register.
Days 61-90	Run executive incident exercise; test selected recovery evidence; report progress and residual risk.	Exercise report; recovery test record; updated dashboard; executive decisions log.

Cost and accountability snapshot

Workstream	Estimated external cost	Internal effort	Proposed budget owner
Identity and access improvement	$3,600-$8,000	24-40 hours	COO
AI governance baseline	Legal review to be quoted	18-30 hours	CEO
Vendor and recovery readiness	$2,500-$6,000	30-50 hours	COO
SaaS consolidation	Potential net savings	16-24 hours	CFO
