Northbridge Components Ltd.

NIST 800-53 Audit Report

ASSESSMENT SCOPE

Corporate IT, cloud and software delivery

ASSESSMENT CRITERIA

NIST SP 800-53 Rev. 5 / Release 5.2.0

ASSESSMENT PERIOD

21-25 September 2026

REPORT ISSUED

7 October 2026

REPORT REFERENCE

AS-NC-2026-01

VERSION

2.0

PREPARED BY

Atlant Security

PREPARED FOR

Board and IT management

DOCUMENT CLASSIFICATION

Illustrative sample

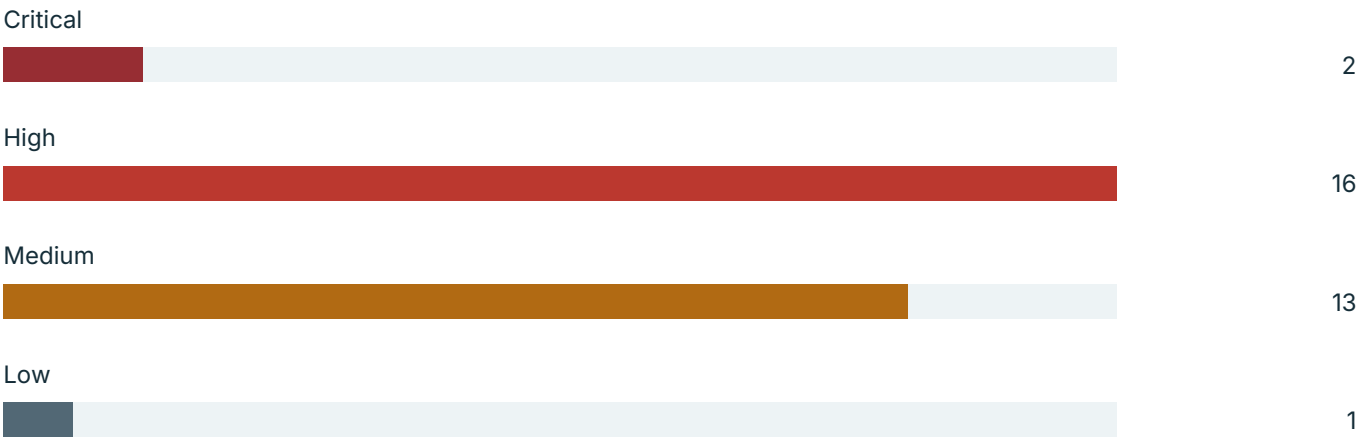
FICTIONAL SAMPLE. No client assessment took place. The organisation, evidence and observations are invented to demonstrate assessment and reporting methods.

MANAGEMENT ASSESSMENT

Executive summary

The assessed environment has functioning identity, network and operational safeguards, but production deployment trust and exposed CI credentials create the most urgent paths to business impact. Weaknesses in review, telemetry and recovery compound these paths. Security work is taking place without consistent evidence that the intended outcome is enforced across environments.

Findings by severity



Number of findings in each severity band. Total: 32. One finding can involve several systems or control objectives.

Management priority	Required decision
Immediate / N53-09, 20	Restrict production federation trust; rotate the exposed CI credential after preserving the record and inspect its use.
First 30 days	Approve owners and safe changes for identity, cloud logging, administration paths, mail exceptions and release approvals.
Months 2-3	Demonstrate recovery, complete supplier and data decisions, and verify the software delivery safeguards.
Months 4-12	Embed measurement, reassess residual exceptions and repeat independent checks after significant changes.

The assessment identifies plausible exposure paths; it does not assert an observed breach. Management remains responsible for change approval, availability and residual-risk decisions. Each detailed finding records the condition and the evidence needed for closure.

SCOPE

Assessment scope and populations

Environment	Declared population / scope
Corporate IT	480 enabled member identities (460 workforce, 20 dedicated admin); 26 privileged identities; 460 discovered assets (412 endpoints, 48 servers); 2 offices.
AWS	6 accounts; 18 federation/deployment roles; 38 security groups; 9 public subnets; 24 S3 buckets; 8 customer-managed keys; 12 backup workloads.
Microsoft 365	1 tenant; the same 480 enabled members; 96 guests; 360 mailboxes; 218 inbox rules; 14 transport rules; 3 connectors; 28 SharePoint sites; 38 service principals with grants.
Software and DevSecOps	3 products (customer portal, integration API, order service); 18 repositories; 12 pipelines; 6 runner pools; 24 pull requests; 10 releases and 10 IaC changes sampled.
People and providers	22 specialist security roles; 8 critical suppliers; 12 supplier personnel changes; 16 remote maintenance sessions; 9 personal-data processing activities.

Sampling and boundaries

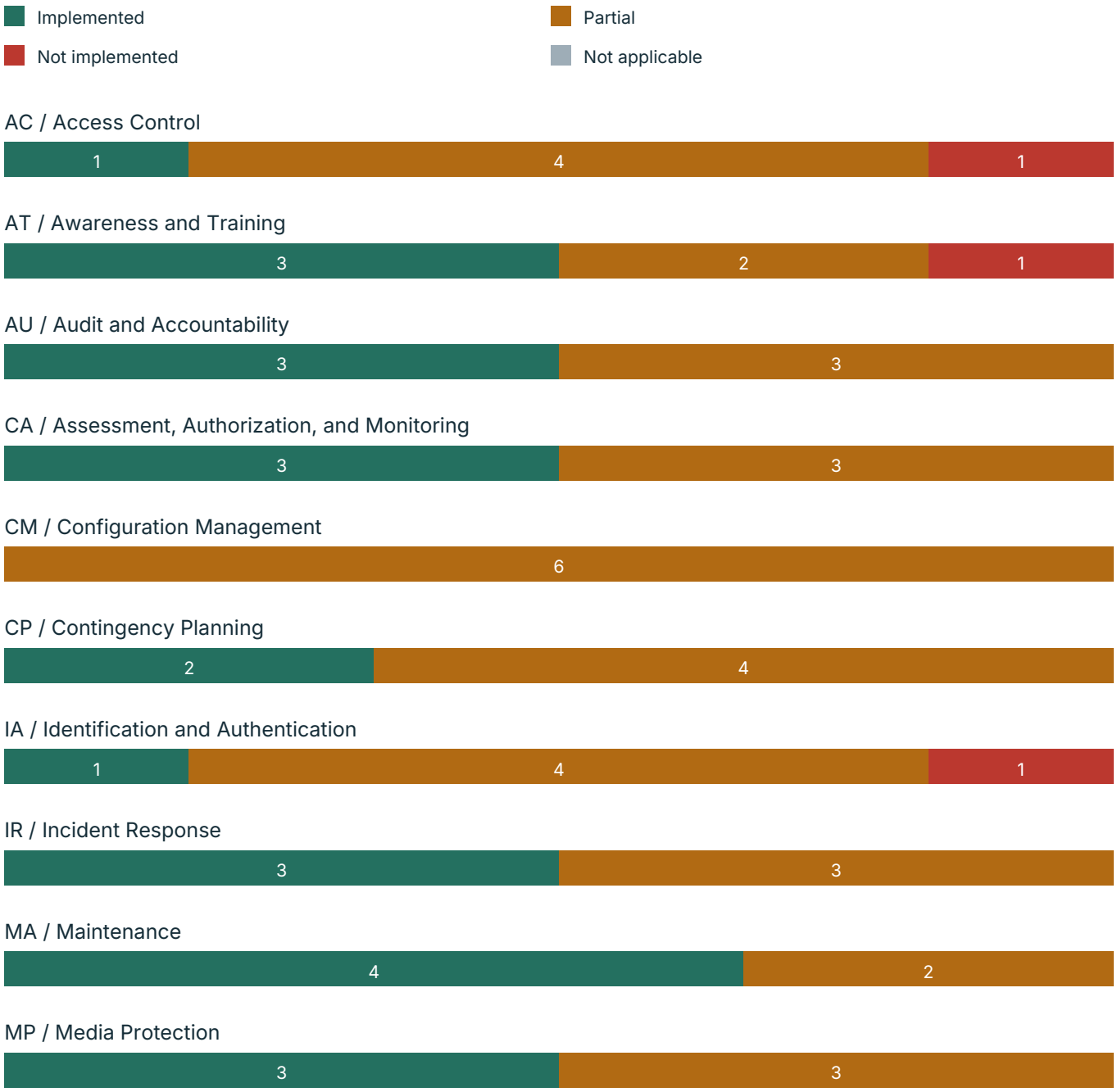
Corporate samples include 14 departures, 80 endpoints, 24 servers for patch evidence, 6 priority recovery workloads, 17 existing actions and 20 configuration changes. Cloud resources are assessed at configuration level; representative event and access checks have the coverage stated in each workpaper.

Manufacturing control systems, destructive testing, provider data-centre visits and full application penetration testing are excluded. Azure infrastructure and GCP are not used in this fictional estate; Entra ID and Microsoft 365 are included. The corporate and AWS recovery populations are reported separately and are not summed as unique services.

CONTROL-FAMILY RESULTS

Control-family assessment results

Selected objective outcomes / families 1-10



Each row contains 6 selected tests; segment labels are counts. Total: 43 implemented, 70 partial, 4 not implemented and 3 not applicable. 43 of 117 applicable objectives (36.8%) have supporting implementation evidence. This is not a NIST compliance or enterprise-security percentage.

DETAILED FINDING

N53-01 / Account lifecycle and privileged access

HIGH | AC-2 / AC-6

Owner: Head of IT / Identity lead | Evidence: EV-01-IAM / EV-02-HR

Criterion and population

NB-IAM-01 sets a 24-hour leaver-disable target and requires a recorded business need for standing administrative access. The values were defined by the organisation and approved as assessment criteria.

All 14 recorded departures in the previous 60 days; all 26 identities with privileged role assignments.

Assessment procedure

We reconciled the HR termination register with identity status and sign-in timestamps. We compared every privileged role assignment with the approved access register and interviewed its owner.

Observed condition

Five departed-user identities remained enabled more than 24 hours after the recorded leaving time. Seven of 26 privileged identities lacked a current recorded need for standing access. The populations overlap; counts are reported separately.

Record	Observed attribute	Result
usr-ex-014	Departure + 72 hours	Identity still enabled
usr-ex-027	Departure + 51 hours	Identity still enabled
adm-ex-006	Standing role	No current justification

> ASSESSMENT BOUNDARY
>
> An enabled account establishes an access-management exception, not that the account was used after departure. No password attempts or production privilege changes were performed.

CORRECTIVE ACTION

N53-01 / Risk and corrective actions

HIGH | Head of IT / Identity lead

Risk and cause

An obsolete or unjustified identity could provide an unnecessary route to business data or administrative functions if its credentials were obtained. The risk is elevated by standing privilege and by delays in removing access.

HR and IT worked from separate trackers. The access register had no enforced expiry or reconciliation owner.

Required corrective action

1. Within 7 days: reconcile the five departure exceptions; disable access through the approved change process after confirming legitimate dependencies.

2. Within 14 days: record the business need for each privileged assignment; remove or time-bound access where the owner cannot justify it.

3. Within 30 days: automate HR-to-IT handoff and produce a weekly exception report with named owners and escalation.

Closure evidence and retest

Reconcile all 14 departure records again and inspect the seven privileged exceptions. Obtain change tickets and new exports; verify a new departure follows the agreed 24-hour target. A policy update alone does not close this finding.

Planning allowance: 3-5 person-days | Target: Month 1. Estimates exclude approvals, procurement and observation time. Changes require owner approval; no remediation was performed during assessment.