

SECURITY ASSESSMENT

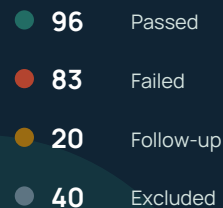
Executive summary

northwind.example | 29 September 2026 | Internal assessment

OVERALL POSTURE

Control gaps require attention

Prioritize the observed weaknesses, validate coverage and confirm closure with fresh evidence.



52

Failed control types

96

Passing results

20

Follow-up results

7

Distinct hosts returned

The leading areas for review are privileged identity, certificate services & trust, protocols & transport security. The scan recorded 83 failed and 96 passing results. Repeated host checks are counted separately; these totals are not unique vulnerabilities. The report does not establish active compromise, business impact or an organization-wide security score.

WHERE TO FOCUS

01

Privileged identity

4 failed control types · CRITICAL

02

Certificate services & trust

2 failed control types · HIGH

03

Protocols & transport security

8 failed control types · HIGH

FAILED RESULTS BY SEVERITY



ASSESSMENT SNAPSHOT

REMOTE COLLECTION

6 of 6 targets returned; 7 of 63 discovered hosts selected

DC 1/2 · server 5/9 · workstation 1/52

HUMAN REVIEW

1 review required

Collected evidence to assess

EXPLICIT CONFIGURATION

11 not configured

Validate effective defaults

COVERAGE LIMITS

1 unavailable / 7 inconclusive

Collect or validate evidence

ERRORS / EXCLUSIONS

0 errors / 40 not applicable

Errors never count as passes

THE MANAGEMENT DECISION

Assign owners, agree a staged rollout and resolve each evidence limitation before accepting closure. Manual reviews and absent explicit settings are separate from failed collection.

PRIORITIZED FINDINGS & RECOMMENDATIONS

Priority workstreams

Ordered by highest recorded baseline severity. Business impact and deadlines require owner review.

01 Privileged identity

**CRITICAL**

4 failed control types; 1 distinct scope. AD-007: privileged SPN accounts: svc-backup. AD-001: krbtgt password age 1127.0 days.

Action Review privileged SPNs and password exceptions. Where flagged, plan controlled krbtgt rotation after checking replication and effective ticket lifetimes.

02 Certificate services & trust

**HIGH**

2 failed control types; 2 distinct scopes. ADCS-001: unmet requirement - Published certificate templates: ESC1 candidates. ADCS-005: enrollment protection candidates require IIS validation.

Action Validate enrollment candidates and effective permissions; renew expired endpoint certificates and confirm IIS protections before closing findings.

03 Protocols & transport security

**HIGH**

8 failed control types; 6 distinct scopes. NET-003: legacy TLS/cipher exposure candidates. HOST-003: SMBv1 enabled.

Action Retire observed legacy protocols and stage signing, channel binding and TLS changes after checking application compatibility.

04 Platform maintenance

**HIGH**

1 failed control type; 1 distinct scope. HOST-002: server builds exceed the dated update-age baseline.

Action Verify servicing and lifecycle status; complete the supported update path, reboot where needed and rescan the same systems.

05 Directory hygiene & policy

**HIGH**

5 failed control types; 1 distinct scope. AD-006: unmet requirement - Administrative group membership exceeds lab threshold. AD-004: unmet requirement - Enabled users with stale replicated logon timestamps.

Action Validate account ownership and activity, review effective password policy and document exceptions before disabling accounts or changing policy.

06 Host access & configuration

**HIGH**

8 failed control types; 6 distinct scopes. HOST-005: unmet requirement - LM/NTLM compatibility policy. HOST-013: unmet requirement - Print Spooler on domain controllers.

Action Apply an agreed role-specific baseline in a pilot group, document compatibility exceptions and verify effective settings after rollout.

PRIORITIZED FINDINGS & RECOMMENDATIONS

Supporting workstreams

Ordered by highest recorded baseline severity. Business impact and deadlines require owner review.

07 Microsoft 365 identity



HIGH

9 failed control types; 1 distinct scope. ENT-003: unmet requirement - Legacy authentication blocked. ENT-015: unmet requirement - Application credentials not expired and not longer-lived....

Action Enforce MFA, block legacy authentication, reduce Global Administrators and restrict guest, application and consent settings before reassessing the tenant.

08 Mail, data & threat protection



HIGH

8 failed control types; 1 distinct scope. DEF-003: unmet requirement - Alerts unresolved for more than 7 days. EXO-003: unmet requirement - SMTP AUTH disabled organization-wide.

Action Enable anti-phishing protections, block external forwarding, disable SMTP AUTH and basic auth, keep audit logging on and triage stale Defender alerts.

09 Collaboration & sharing



HIGH

3 failed control types; 1 distinct scope. SPO-001: unmet requirement - External sharing level does not allow anonymous links. TEAMS-001: unmet requirement - External access restricted to allowed domains.

Action Remove anonymous sharing links, restrict external sharing and Teams federation to allowed domains and keep anonymous meeting attendees in the lobby.

10 Endpoint prevention



MEDIUM

1 failed control type; 1 distinct scope. HOST-009: unmet requirement - Windows Firewall profiles enabled.

Action Verify the active protection product; enforce supported prevention controls in stages and confirm runtime state after deployment.

11 Detection & audit readiness



MEDIUM

3 failed control types; 7 distinct scopes. HOST-085: process-creation auditing gap. HOST-055: Security log capacity below 200 MiB.

Action Apply the agreed audit policy; validate event generation, central receipt, retention and alert routing with a controlled test.

DELIVERY PLAN & ASSESSMENT CONFIDENCE

From findings to action

Proposed timing starts when the plan is accepted. Owners and exceptions remain to be agreed.

01

First 30 days

Validate priority evidence and failed connections. Assign owners; schedule the highest-severity identity, certificate and protection work.

02

Days 31-60

Pilot the agreed Windows and authentication baseline. Check application dependencies, update plans and effective logging.

03

Days 61-90

Complete approved rollout, rescan equivalent scope and close findings only with evidence. Record residual risks and review dates.

COVERAGE & DECISIONS**COLLECTION**

No whole-target remote collection failure was reported. Individual controls can still have missing or unavailable evidence.

CONFIDENCE

Executive figures cover the 71 Essentials controls; the technical report covers all 194. 7 distinct hosts returned evidence; the same host can appear locally and remotely. No trend or improvement is inferred without a comparable earlier scan.

BOUNDARIES

Microsoft 365 coverage is limited to the listed Entra ID, Exchange Online and Purview, SharePoint, Defender and Teams controls, all read with read-only access. Backup resilience, external perimeter testing and effective share permissions are outside scope. AD CS findings are candidates, not proven attack paths.

ACCEPTANCE

No compensating controls or accepted risks have been recorded. Require an owner, supporting evidence and a review date for each exception. Full observations and check IDs remain in the technical report.

Sample report: fictional organization

This report describes the configuration collected from the hosts and workloads listed in it, at the time shown, within the limits in its coverage section. It is a point-in-time review, not a penetration test, an audit opinion, a certification or a guarantee of security or compliance. Findings and guidance are informational; test any change first. Settings that could not be read are reported as missing, not passing. Microsoft and Windows behavior can change after the collection date. Prepared by GlacierPoint Technologies LLC under the GlacierPoint Scan Terms of Service.