



NIST CYBERSECURITY FRAMEWORK 2.0 EVIDENCE

Northwind Traders

PREPARED BY

Harbour IT

DATE

14 October 2026

EVIDENCE DATE

13 Oct 2026

SCHEME

NIST

MICROSOFT 365 TENANT

northwindtraders.onmicrosoft.com

● Gaps to close

Northwind Traders has 4 controls not in place.

IN THIS REPORT

Summary	2
Gaps to close	3
Govern (GV)	4
Identify (ID)	6
Protect (PR)	8
Detect (DE)	12
Respond (RS)	13
Recover (RC)	14
About this evidence	14

Summary

Northwind Traders has 4 controls not in place.

The CSF 2.0 categories Microsoft 365 data speaks to, judged from the checks, and text for the rest. Use it when a client or a parent company asks for a CSF mapping or profile.

10 controls need evidence Microsoft 365 can't show (firewalls, patch timing, anti-malware settings and processes): each has a text to complete.

18 controls



■ **0** Pass ■ **4** Fail ■ **4** Partly ■ **10** Your evidence

Gaps to close

The controls most likely to be queried, with the fix for each.

1 GV.SC Supply chain risk management

Users can consent to any app. Fix: Set user consent to "Allow user consent for apps from verified publishers, for selected permissions" or turn it off and use the admin consent workflow.

2 ID.RA Risk assessment

25 of 36 Windows computers past end of support. Fix: Upgrade computers on Windows 10 or an old Windows 11 release to the current Windows 11 release.

3 PR.AA Identity, authentication and access: MFA

Enforced by Require MFA for all users, with 1 exclusion to review. Fix: Create a Conditional Access policy requiring MFA for all users and all cloud apps, or turn on Security Defaults if the tenant has no Entra ID P1.

4 DE.CM Continuous monitoring

1 suspicious inbox rule. Fix: Check each rule with the mailbox owner.

5 ID.AM Asset management

1 of 39 device records unused for 90+ days. Fix: Disable, then after 30 days delete, device records that haven't signed in for 90 days.

6 PR.AA Identity, authentication and access: least privilege

1 guest with admin roles. Fix: Remove admin roles from guest accounts.

7 PR.DS Data security

4 of 36 computers not encrypted. Fix: Turn on BitLocker.

8 PR.PS Platform security

1 of 37 joined computers not in Intune. Fix: Enrol Entra-joined and hybrid-joined computers in Intune.

Govern (GV)

● Fail

Roles, policy, risk management and supply chain risk are set and overseen by leadership.

GV.RR Roles, responsibilities and authorities

● Your evidence

Leadership is accountable for cybersecurity, and roles are set and resourced.

Text to paste: [Name], [role], has overall responsibility for information security and data protection and reports to [the board or partners], where security is a standing agenda item. Day-to-day IT security is managed by [IT provider].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

GV.PO Policy

● Your evidence

Cybersecurity policy is set, communicated, enforced and reviewed.

Text to paste: Information security policies covering [acceptable use, access control, passwords, data protection and incident response] are approved by [role], reviewed every [12 months] and acknowledged by staff.

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

GV.RM Risk management strategy

● Your evidence

Risk appetite and priorities are set and used to make decisions.

Text to paste: An information security risk assessment covering [scope] names an owner for each risk, the agreed treatment and an action plan. It was last reviewed on [date] by [name and role] and approved by [director or partner].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

GV.SC Supply chain risk management

● Fail

Suppliers are known, assessed and bound by security requirements, and the cloud apps that reach company data are controlled.

GAPS

- Users can consent to any app.
 - Any user can grant any app access to their mail and files
- 1 app with access to mail, files or the directory.
 - Mail Sync Pro: Mail.Read (application permission; unverified publisher)

Fix: Set user consent to "Allow user consent for apps from verified publishers, for selected permissions" or turn it off and use the admin consent workflow. Consent phishing relies on this setting.

Text to paste: Suppliers and contractors that handle the organisation's data are checked before they're used, must meet [Cyber Essentials or equivalent security requirements], and are reviewed [every 12 months]. They're listed in [supplier register].

What Microsoft 365 can't show: Microsoft 365 shows which apps can reach its data; the supplier reviews are the organisation's own.

Identify (ID)

● Fail

Assets are known and risks to them are understood and improved on.

ID.AM Asset management

● Partly

Hardware, software, services and data are inventoried, and stale entries are removed.

WHAT WE FOUND

- Computers managed by Intune: 36
- Of which encrypted: 32
- Windows computers out of support: 25
- Not compliant: 6

GAPS

- 1 of 39 device records unused for 90+ days.
 - OLD-PC: Windows, last seen 200 days ago

Fix: Disable, then after 30 days delete, device records that haven't signed in for 90 days (Entra admin center > Devices > All devices, filter by activity). Old records can still hold BitLocker keys and count toward device limits.

Text to paste: An asset register in [tool or spreadsheet] lists [hardware, software, cloud services and the information held], each with a named owner, a category and where it is. Devices are added when they're set up and removed when they're disposed of, and the register was last reviewed on [date].

What Microsoft 365 can't show: Microsoft 365 lists the devices Intune and Entra ID know; the inventory covers everything else.

ID.RA Risk assessment

● Fail

Vulnerabilities are identified, including systems out of vendor support, and risks are assessed.

GAPS

- 25 of 36 Windows computers past end of support.
 - LAPTOP-HUGHES (robert.hughes@northwindtraders.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-MARTIN22 (maya.martin@northwindtraders.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-PATEL13 (hannah.patel@northwindtraders.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-ROBERTS31 (george.roberts@northwindtraders.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-TAYLOR04 (grace.taylor@northwindtraders.example): Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - and 20 more

Fix: Upgrade computers on Windows 10 or an old Windows 11 release to the current Windows 11 release (Intune: Windows feature updates policy). Replace hardware that can't run Windows 11, or buy Extended Security Updates as a stopgap.

Text to paste: External vulnerability scans run [monthly] using [tool or provider]. [A penetration test was last carried out on (date) by (provider).]

What Microsoft 365 can't show: Judged from the Windows versions Intune reports. Describe scanning of everything else.

Protect (PR)

● Fail

Identities are verified and least privilege enforced, people trained, data protected, platforms hardened and backed up.

PR.AA Identity, authentication and access: MFA

● Fail

Users are authenticated in proportion to risk: multi-factor authentication for everyone, and legacy protocols blocked.

WHAT WE FOUND

- But: 2 admins without a phishing-resistant method.
- But: 3 people can only use a text or call as a second factor.
- Users with an MFA method registered: 62.2% of 37
- Accounts covered by an enforced MFA policy: 36 of 37
- Not covered: breakglass@northwindtraders.example

GAPS

- Enforced by Require MFA for all users, with 1 exclusion to review.
 - breakglass@northwindtraders.example: Excluded from "Require MFA for all users"
- 1 admin not covered by MFA.
 - breakglass@northwindtraders.example: Global Administrator: excluded from Require MFA for all users
- Legacy authentication is allowed.
 - No enabled policy blocks legacy authentication for all users

Fix: Create a Conditional Access policy requiring MFA for all users and all cloud apps, or turn on Security Defaults if the tenant has no Entra ID P1. Keep exclusions to break-glass accounts.

Text to paste: Multi-factor authentication (MFA) is enforced for Microsoft 365 email (including Outlook on the web and mobile) and cloud applications, through Microsoft Entra ID. Enforced by Conditional Access ("Require MFA for all users") for everyone except 1 named exclusion: breakglass@northwindtraders.example (break-glass).

What Microsoft 365 can't show: Judged for Microsoft 365 sign-ins. Add other systems.

PR.AA Identity, authentication and access: least privilege

● Partly

Access rights are managed with least privilege, admin rights are few, and leavers lose access.

WHAT WE FOUND

- 2 Global Administrators.
- Accounts holding privileged roles: 4
- Admins with no MFA policy: 1
- Admins with no MFA method registered: 2

GAPS

- 1 guest with admin roles.
 - g#EXT#@northwindtraders.example: Guest holding Exchange Administrator
- 1 app with privileged roles.
 - Some app: App holding Exchange Administrator
- 4 accounts inactive for 90+ days or never used.
 - hannah.robinson@northwindtraders.example: Licensed member, last signed in 8 Apr 2026
 - sophie.smith@northwindtraders.example: Licensed member, last signed in 23 Jan 2026
 - thomas.clarke@northwindtraders.example: Licensed member, last signed in 3 Jun 2026
 - g#EXT#@northwindtraders.example: Guest, never signed in, created ?

Fix: Remove admin roles from guest accounts. If an external partner needs access, use GDAP or a member account in this tenant protected by MFA.

Text to paste: Administrator role assignments in Microsoft 365 are tracked, with gaps. 4 accounts hold privileged admin roles, 2 of them Global Administrator (ann.patel@northwindtraders.example, breakglass@northwindtraders.example). 2 Global Administrators. 1 guest with admin roles. 1 app with privileged roles.

What Microsoft 365 can't show: Judged from Entra ID roles and sign-in activity.

PR.AT Awareness and training

● Your evidence

People are trained to do their work with security in mind.

Text to paste: All staff complete security awareness training [when they join and every year], through [training provider or platform]. Simulated phishing exercises run [monthly or quarterly] and the results are reviewed by [role].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

PR.DS Data security

● Partly

Data is protected at rest and in transit, and isn't shared or forwarded outside unnoticed.

WHAT WE FOUND

- The default outbound policy blocks automatic external forwarding.
- But: 1 of 1 mail domain doesn't fully enforce MTA-STS.
- But: 2 domains without DMARC enforcement.

GAPS

- 4 of 36 computers not encrypted.
 - DESK-WRIGHT18
(leo.wright@northwindtraders.example):
Windows disk isn't encrypted
 - LAPTOP-HUGHES
(robert.hughes@northwindtraders.example):
Windows disk isn't encrypted
 - LAPTOP-SCOTT29
(olivia.scott@northwindtraders.example):
Windows disk isn't encrypted
 - LAPTOP-SMITH07
(olivia.smith@northwindtraders.example):
Windows disk isn't encrypted
- 3 files and folders shared with anyone.
 - Campaign video.mp4 (Marketing / Documents):
Anyone can edit
 - Brand assets (Marketing / Documents): Anyone
can view, link never expires
 - holiday.jpg (OneDrive of
ann.patel@northwindtraders.example): Anyone
can view
- 4 external forwards.
 - ann.patel@northwindtraders.example: Mailbox
forwarding to ann.patel@homemail.example
(keeps a copy)
 - ann.patel@northwindtraders.example: Inbox rule
"Copy to home" forwards to
ann.patel.home@homemail.example
 - grace.taylor@northwindtraders.example: Mailbox
forwarding to grace.taylor@homemail.example
(doesn't keep a copy)
 - olivia.smith@northwindtraders.example: Inbox
rule "Invoices to bookkeeper" forwards to
bookkeeping@ledgerline.example

Fix: Turn on BitLocker (Windows) and FileVault (macOS) with an Intune disk encryption policy, with recovery keys escrowed to Entra ID, so a lost or stolen laptop doesn't expose the client's data.

Text to paste: Data in Microsoft 365 is encrypted at rest by Microsoft (BitLocker and per-file service encryption) and in transit using TLS. Not every company computer is encrypted: 4 of 36 computers not encrypted.

What Microsoft 365 can't show: Judged from Intune encryption, SharePoint sharing and Exchange forwarding.

PR.PS Platform security

● Partly

Hardware and software are managed, configured securely and kept updated, and logs are generated.

WHAT WE FOUND

- Mailbox auditing is on for the organisation.
- Not checked: users can't create new tenants (Microsoft didn't return this setting).
- Computers managed by Intune: 36
- Of which encrypted: 32
- Windows computers out of support: 25
- Not compliant: 6

GAPS

- 1 of 37 joined computers not in Intune.
 - DESK-RECEPTION: Hybrid joined, not managed by Intune
- 6 of 37 managed devices not compliant.
 - DESK-ROBINSON12 (george.robinson@northwindtraders.example): Not compliant
 - DESK-WRIGHT18 (leo.wright@northwindtraders.example): Not compliant
 - LAPTOP-HUGHES (robert.hughes@northwindtraders.example): Not compliant
 - LAPTOP-SCOTT25 (alfie.scott@northwindtraders.example): Not compliant
 - LAPTOP-SCOTT29 (olivia.scott@northwindtraders.example): Not compliant
 - and 1 more
- Any user can register an app.
 - Users can register apps that nobody reviews

Fix: Enrol Entra-joined and hybrid-joined computers in Intune (automatic enrolment under Devices > Enrollment > Windows) so compliance, encryption and updates can be enforced on them.

Text to paste: Company devices are not all managed centrally. 1 of 37 joined computers not in Intune. 6 of 37 managed devices not compliant.

What Microsoft 365 can't show: Judged from Intune, Exchange Online auditing and Entra ID tenant settings.

PR.IR Technology infrastructure resilience

● Your evidence

Networks are protected and capacity and backups keep services running.

WHAT WE FOUND

- Supporting: 41% of about 1.31 TB used (1 TB + 10 GB × 32 licences).

Text to paste: Microsoft 365 data (Exchange Online mail, OneDrive, SharePoint and Teams) is backed up [daily] by [backup product or provider] to storage separate from Microsoft 365. Backups are kept for [retention period], are [immutable or offline], and use credentials separate from the Microsoft 365 administrator accounts. Restores were last tested on [date].

What Microsoft 365 can't show: Microsoft 365 doesn't back itself up for this purpose; describe the backup of Microsoft 365 too.

Detect (DE)

● Fail

Activity is monitored and adverse events are analysed.

DE.CM Continuous monitoring

● Fail

Sign-ins, accounts and mailboxes are monitored for anomalies.

WHAT WE FOUND

- Not checked: no accounts are at risk in Entra ID Protection (Risky users need Entra ID P2).
- Not checked: no risky sign-ins succeeded (Sign-in risk needs Entra ID P2).
- But: 1 domain had sign-in settings changed in the last 30 days.

GAPS

- 1 suspicious inbox rule.
 - ann.patel@northwindtraders.example: ".": Moves to RSS Feeds mail mentioning invoice, payment; Rule name '!' looks deliberately blank

Fix: Check each rule with the mailbox owner. Rules that delete or bury messages about payments or security alerts are a sign of a compromised account: reset the password, revoke sessions and review sign-ins.

Text to paste: Sign-ins are monitored for suspicious activity by [tool or service], and alerts are reviewed by [team or provider] [within one working day].

What Microsoft 365 can't show: Judged from Entra ID Protection and inbox rules (Entra ID P2 for the full detections).

DE.AE Adverse event analysis

● Your evidence

Alerts are analysed to understand what happened and its impact.

Text to paste: Security alerts and sign-in logs are reviewed [daily or weekly] by [team or provider]. Logs are kept for [period] where users can't change them.

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

Respond (RS)

● Your evidence

Incidents are managed, analysed, reported and contained.

RS.MA Incident management

● Your evidence

An incident response plan is run when an incident is declared.

Text to paste: A documented incident response plan sets out roles, contacts and the steps to contain and recover from a cyber incident, including notifying [the insurer and IT provider]. It was last reviewed on [date] and tested on [date].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

RS.MI Incident mitigation

● Your evidence

Incidents are contained, for example by securing a compromised account.

Text to paste: If an account may be compromised, [IT provider] resets the password, signs the account out of every session, checks its MFA methods and inbox rules, and reviews its sign-ins. Staff report concerns to [contact].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

RS.CO Incident reporting and communication

● Your evidence

Incidents are reported to the people and authorities who must be told.

Text to paste: Every personal data breach is recorded in a breach log with what happened, its effects and what was done. [Role] decides whether it must be reported; reportable breaches go to the ICO within 72 hours of the organisation becoming aware, and to the people affected when the risk to them is high. Lessons learned are reviewed by [role].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

Recover (RC)

● Your evidence

Recovery plans are run and restored data is checked.

RC.RP Incident recovery plan execution

● Your evidence

Systems and data are restored from backups by a tested plan.

Text to paste: A business continuity and disaster recovery plan covers [key systems and services]. Recovery targets are [time to restore] to restore service and no more than [data loss window] of data loss. It was last tested on [date].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

About this evidence

The CSF has no pass mark. Use Pass as evidence a category's outcome is achieved for Microsoft 365, and Fail and Partly as the gaps for the target profile.

Requirements: NIST Cybersecurity Framework (CSF) 2.0, February 2024. Category identifiers are NIST's; outcomes are paraphrased. A CSF profile is the organisation's own: this pack is the Microsoft 365 evidence for it.

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Pass and Fail are judged from Microsoft 365 settings and accounts read with read-only access; nothing was changed. The oldest data used was collected 13 Oct 2026, 04:00 UTC. Accepted risks are exceptions the organisation has reviewed and documented. Complete the [parts in brackets] before using a text.