



Harbour IT

IASME CYBER ASSURANCE EVIDENCE

Northwind Traders

PREPARED BY

Harbour IT

DATE

11 October 2026

EVIDENCE DATE

11 Oct 2026

SCHEME

IASME

MICROSOFT 365 TENANT

northwindtraders.onmicrosoft.com

● Not ready

Northwind Traders has 6 controls to fix before applying for Cyber Assurance.

IN THIS REPORT

Summary	3
Fix before you apply	3
Organisation and governance	4
Cloud services and the supply chain	5
Information assets	7
Legal compliance and data protection	10
People	12
Physical and environmental protection	14
Preventing intrusion	15
Backup and restore	17
Monitoring	18
Change management	19
Business continuity	20

Incident management

21

What the assessor checks

22

About this evidence

22

Summary

Northwind Traders has 6 controls to fix before applying for Cyber Assurance.

The controls IASME Cyber Assurance asks about, theme by theme: what Microsoft 365 shows judged from the data, and the rest as text to complete. Hold Cyber Essentials first; its pack covers the technical controls.

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

39 controls



■ 3 Pass ■ 6 Fail ■ 29 Your evidence ■ 1 Not collected

Fix before you apply

An assessor won't accept a gap in these. Each one names the accounts or settings behind it and the fix.

1 Third-party apps controlled

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 Data encrypted in the cloud, in transit and on laptops

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

3 Access limited to what each job needs

Anyone, including guests, can invite guests. Fix: Restrict guest invitations to admins and the Guest Inviter role, or at least to members, under External collaboration settings.

4 Access removed when people leave

4 accounts inactive for 90+ days or never used. Fix: Disable accounts that haven't signed in for 90 days, or were created over 30 days ago and never used.

5 MFA on every cloud account

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.

6 Few, separate, named administrators

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

Organisation and governance

● Your evidence

A named director is accountable for information security and data protection, it's on the board's agenda, and someone is given the time and skills to run it.

A named person accountable for security

● Your evidence

A board member, director or partner has overall responsibility for information security and data protection, and it is a standing item at management meetings.

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.

Security policies written, approved and reviewed

● Your evidence

Information security policies cover the scope, set clear responsibilities, are shared with everyone they apply to, and have been reviewed and approved in the last 12 months.

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.

A current risk assessment with owners and actions

● Your evidence

A risk assessment covering the scope, reviewed in the last 12 months, names an owner and a treatment for each risk and has an action plan approved at board level.

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.

Cloud services and the supply chain

● Fail

The cloud services that hold the organisation's data are known, where they keep it is known, and suppliers are held to security requirements.

Cloud services in use listed

● Pass

The cloud services used to store and share information are listed.

WHAT WE FOUND

- Microsoft 365 (Microsoft 365 Business Basic, Microsoft 365 Business Premium). Cloud services connected to Microsoft 365 sign-in: Mail Sync Pro, Survey Tool, Zoom.

What Microsoft 365 can't show: Microsoft 365 lists the apps connected to its sign-in; add services people sign in to separately.

Where cloud data is stored

● Pass

The organisation knows where its cloud providers store its data.

WHAT WE FOUND

- Email, files and Teams data are held in Microsoft 365, in Microsoft's datacentres.

What Microsoft 365 can't show: Judged from the tenant's country in Microsoft 365. Add every other cloud service.

Third-party apps controlled

● Fail

Users can't connect third-party apps to company data on their own, and apps with broad access are known.

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)
- Any user can register an app.
 - Users can register apps that nobody reviews

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: Third-party application access to Microsoft 365 data is not controlled. Users can consent to any app. 1 app with access to mail, files or the directory.

What Microsoft 365 can't show: Judged from Entra ID consent settings and app permissions.

Security requirements for suppliers

● Your evidence

Suppliers and contractors who handle the organisation's information must meet defined security requirements, checked before they start and reviewed.

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: All of this. Answer from the organisation's own records.

Information assets

● Fail

Equipment and information are listed with owners, sensitive and personal data is identified and encrypted, and data is wiped before equipment goes.

An asset register with named owners

● Your evidence

Physical and information assets, including every laptop, tablet and phone, are recorded with a named owner, a category and their location.

WHAT WE FOUND

- But: 1 of 39 device records unused for 90+ days.
- But: 1 of 37 joined computers not in Intune.
- Computers managed by Intune: 36
- Of which encrypted: 32
- Windows computers out of support: 5
- Reaching end of support within 90 days: 20
- Not compliant: 6

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 register covers everything else.

Data encrypted in the cloud, in transit and on laptops

● Fail

Data is encrypted on its way to and while stored in cloud services, and on mobile devices that hold it.

WHAT WE FOUND

- But: 1 of 1 mail domain doesn't fully enforce MTA-STS.

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

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 for company computers; Microsoft encrypts Microsoft 365 data itself.

Removable media tracked and encrypted

● Your evidence

USB drives and other removable media are controlled, recorded and encrypted.

Text to paste: Removable media is [blocked by Intune policy or allowed only on encrypted, company-issued drives], and drives that hold the organisation's data are recorded in the asset register.

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

Data reviewed and deleted when no longer needed

● Your evidence

The data held is reviewed regularly and deleted when it's no longer relevant.

Text to paste: A retention schedule sets how long each kind of data is kept. Data past its retention period is deleted [by Microsoft 365 retention policies or at a review every (period)], and the data held is reviewed [every 12 months] to check it's still needed.

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

Data wiped before equipment is disposed of

● Your evidence

When assets are no longer needed, data is securely wiped or the storage destroyed.

Text to paste: Before devices and storage are reused or disposed of, data is securely wiped [with an Intune wipe or a certified erasure tool] or the storage is destroyed by [certified disposal company], and the certificate is kept.

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

Legal compliance and data protection

● Your evidence

UK GDPR is met: the ICO fee is paid, someone manages data protection, personal data is recorded with its lawful basis, the privacy notice is current, rights requests are handled and processors are under contract.

ICO data protection fee paid

● Your evidence

The organisation is registered with the ICO, or has recorded why it's exempt.

Text to paste: The organisation is registered with the Information Commissioner's Office, registration number [ZA number], renewed on [date].

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

Data protection managed by a named person

● Your evidence

A Data Protection Officer is appointed where one is required; otherwise the decision is recorded and a named person manages data protection.

Text to paste: [The organisation has appointed (name) as its Data Protection Officer, contactable at (email address).] or [The organisation assessed on (date) that it doesn't need a Data Protection Officer; (name, role) is responsible for data protection.]

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

Personal data recorded with its lawful basis

● Your evidence

For each kind of personal and special category data held, the purpose and lawful basis are recorded.

Text to paste: A record of processing activities lists each kind of personal data held, its purpose and lawful basis, who it's shared with, where it's stored and how long it's kept. [Role] maintains it, and it was last reviewed on [date].

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

A current privacy notice

● Your evidence

A privacy notice says what data is collected and why, how it's used and people's rights, and is reviewed.

Text to paste: A privacy notice at [web address] explains what personal data is collected, why and on what lawful basis, who it's shared with, how long it's kept, people's rights and how to complain. It was last reviewed on [date].

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

People's rights requests handled

● Your evidence

There is a process for requests to see, correct or delete personal data, and for withdrawing consent.

Text to paste: Requests to see, correct or delete personal data, and complaints about how it's used, go to [contact] and are logged in [system]. They're answered within one month, and [role] checks each response before it's sent.

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

Data processing agreements with suppliers

● Your evidence

Every supplier that processes personal data has a contract with the data protection terms UK GDPR requires, including for data held outside the UK.

Text to paste: Every supplier that processes personal data for the organisation has a written contract with the terms UK GDPR Article 28 requires: acting only on instructions, confidentiality, security, approval of sub-processors, help with people's rights, and deleting or returning the data at the end. They're recorded in [register].

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

People ● Fail

Staff are vetted, given only the access their job needs, briefed and trained, and their access goes when they leave or change role.

Staff checked before they get access

● Your evidence

Everyone with access to the organisation's data is checked as suitable first.

Text to paste: New staff go through [right-to-work, reference and DBS] checks before they get access, and sign [confidentiality agreements].

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

Access limited to what each job needs

● Fail

People only have access to the systems and data their role needs.

WHAT WE FOUND

- Guests have limited access to directory objects (the default).

GAPS

- Anyone, including guests, can invite guests.
 - Guests can invite other guests

Fix: Restrict guest invitations to admins and the Guest Inviter role, or at least to members, under External collaboration settings.

Text to paste: Access to files and systems is given through role-based groups, approved by [role], and changed when people move roles. [Access is reviewed every 12 months.]

What Microsoft 365 can't show: Microsoft 365 shows what guests can see and who can invite them; describe how staff access is set.

Security and data protection training

● Your evidence

Staff and contractors are briefed on their responsibilities when they start and trained regularly.

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.

Access removed when people leave

● Fail

When people leave or change role, their access is removed or changed promptly.

WHAT WE FOUND

- No stale guest invitations.

GAPS

- 4 accounts inactive for 90+ days or never used.
 - hannah.robinson@northwindtraders.example: Licensed member, last signed in 7 Apr 2026
 - sophie.smith@northwindtraders.example: Licensed member, last signed in 21 Jan 2026
 - thomas.clarke@northwindtraders.example: Licensed member, last signed in 2 Jun 2026
 - g#EXT#@northwindtraders.example: Guest, never signed in, created ?
- 1 disabled account still licensed.
 - robert.hughes@northwindtraders.example: Disabled, holding 1 licence

Fix: Disable accounts that haven't signed in for 90 days, or were created over 30 days ago and never used (after checking with the client), then remove their licences. Inactive accounts are a common foothold for attackers.

Text to paste: Some inactive accounts in Microsoft Entra ID have not been disabled. 4 accounts inactive for 90+ days or never used. 1 disabled account still licensed.

What Microsoft 365 can't show: Judged from sign-in activity in Microsoft Entra ID. Describe the leavers process in the answer.

Physical and environmental protection

● Your evidence

Premises are secured, only authorised people get in, and networks are restricted to authorised devices.

Premises secured

● Your evidence

Business premises in scope are physically protected, with access limited to authorised people.

Text to paste: Offices are protected by [locked doors, access control and alarms]. [Servers and network equipment are kept in a locked room or cabinet.]

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

Preventing intrusion

● Fail

Accounts are protected by MFA, sessions and devices lock, vulnerabilities are found by scanning and fixed, and malicious sites are blocked.

MFA on every cloud account

● Fail

Multi-factor authentication protects every account that can reach the organisation's cloud services.

WHAT WE FOUND

- But: 14 users without MFA.
- 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 36

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 every other cloud service.

Few, separate, named administrators

● Fail

Administrator access is limited to the people who need it, through separate accounts.

WHAT WE FOUND

- 2 Global Administrators.
- Cloud-only tenant: no accounts are synced from on-premises AD.
- But: 2 admins without a phishing-resistant method.
- 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

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: Microsoft 365 shows who holds admin roles today; add administrators of other systems.

Devices and sessions don't stay signed in

● Your evidence

Accounts and devices lock or sign out after a period of inactivity.

Text to paste: Computers lock after [5 to 15] minutes of inactivity and need a password, PIN or Windows Hello to unlock. Phones and tablets need a PIN of at least 6 digits or biometrics [enforced by Intune].

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

Vulnerability scans at least every six months

● Your evidence

All systems are scanned for vulnerabilities at least every six months and after major changes, with penetration tests where the risk assessment calls for them, and the findings are fixed.

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: All of this. Answer from the organisation's own records.

Malicious websites blocked

● Your evidence

Access to malicious internet sites and domains is blocked at the boundary or on the device.

Text to paste: Malicious websites are blocked by [Microsoft Defender SmartScreen and network protection, a filtering DNS service such as Quad9, or the firewall's web filter].

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

Backup and restore

● Your evidence

Information is backed up at least weekly, kept apart and protected, with a copy somewhere else, and restores are tested.

Regular, separate, tested backups

● Your evidence

All information is backed up regularly, backups are protected and kept in a different location, and restores are tested.

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.

Monitoring

● Not collected

Access attempts are watched, logs are kept safe for a set time, and warnings are reviewed.

Logs and audit trails kept

● Pass

Event logs and audit trails are kept securely for a defined period.

WHAT WE FOUND

- Mailbox auditing is on for the organisation.

Text to paste: Mailbox audit logging is enabled in Exchange Online, recording access to and actions on mailboxes. Mailbox auditing is on for the organisation.

What Microsoft 365 can't show: Judged from Exchange Online mailbox auditing and the unified audit log.

Sign-in attempts watched

● Not collected

The organisation watches who is trying to access its information and from where.

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).

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 (needs Entra ID P2 for the full detections).

Warnings and reports reviewed

● Your evidence

Security warnings and reports are reviewed regularly and security settings are rechecked.

WHAT WE FOUND

- But: 1 suspicious inbox rule.
- But: 1 domain had sign-in settings changed in the last 30 days.

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: Microsoft 365 shows what's logged and flagged; describe who reviews it and how often.

Change management

● Your evidence

Changes are planned, tested and approved, only approved software is installed, and new uses of personal data get an impact assessment first.

Changes approved and tested

● Your evidence

Changes to systems, applications and networks are recorded, tested and approved before they're made.

Text to paste: Changes to systems, applications and networks are logged in [ticket system], checked for their security effect, tested where possible and approved by [role] before they're made. Emergency changes are reviewed afterwards.

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

Only approved software installed

● Your evidence

Computers and servers are set up only with approved software, and software nobody needs is removed.

Text to paste: New devices are set up from [a standard build or Windows Autopilot] without unnecessary software, and unused software and services are removed [during regular reviews by the IT provider].

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

Impact assessments before high-risk processing

● Your evidence

A data protection impact assessment is carried out before high-risk processing starts.

Text to paste: A data protection impact assessment is carried out before any new system or process that is likely to be high risk to people, using [the ICO's template]. [Role] signs each one off, and the ICO would be consulted if a high risk remained.

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

Business continuity

● Your evidence

Continuity and disaster recovery plans exist, are reviewed and tested every year, and are signed off.

Continuity and recovery plans tested yearly

● Your evidence

Business impact assessments and continuity and recovery plans are in place, reviewed and tested at least once a year, and approved at board level.

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.

Incident management

● Your evidence

Incidents are reported, recorded and investigated, the right outside bodies are told, and lessons are learned.

Incidents reported, investigated and learned from

● Your evidence

Security incidents and suspected weaknesses are reported and recorded, investigated for their cause, and the lessons fed back, with clear roles for everyone involved.

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.

A compromised account is contained

● Your evidence

There is a process for when an account or password may be compromised.

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.

Breaches reported to the ICO when required

● Your evidence

Incidents are reported to outside bodies as required, including personal data breaches to the ICO.

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.

What the assessor checks

What the assessor or auditor checks, what each needs, and what Microsoft 365 already shows for it.

Level 2: documents and interviews

At Level 2 an auditor asks to see the evidence behind the Level 1 answers (policies, the risk assessment, the asset register, training records, the breach log) and interviews staff.

Microsoft 365 shows: Microsoft 365 can show the technical evidence on the day: the MFA, admin, logging and leavers controls on this page, with the rows behind them.

Today: MFA on every cloud account ● **Fail** Few, separate, named administrators ● **Fail** Logs and audit trails kept ● **Pass** Access removed when people leave ● **Fail**

About this evidence

Cyber Essentials, or IASME Cyber Baseline, must be held before applying; use the Cyber Essentials pack for the technical controls.

The answers must be approved by a director, partner, owner or trustee before they're submitted.

Scope: Cyber Assurance covers the whole organisation or a named business unit, including paper records. A Pass here covers Microsoft 365; the answer should say what covers the rest.

Requirements: IASME Cyber Assurance, Level 1 (verified self-assessment) and Level 2 (audit). Requirements paraphrased by theme from IASME's Cyber Assurance question set. Question numbers change between versions, so match each answer to its question by wording, and check the current question set in the IASME portal before you submit.

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 11 Oct 2026, 20:31 UTC. Accepted risks are exceptions the organisation has reviewed and documented. Complete the [parts in brackets] before using a text.