

**Beacon Technology Partners**

MANAGED IT & SECURITY SERVICES

CONSOLIDATED ASSESSMENT

Security Assessment Report

Microsoft 365 security posture, Cloud infrastructure posture, Connected app risk, Business email compromise, SOC 2 compliance drift.

PREPARED FOR

Northwind Logistics Pvt Ltd

REPORT DATE 2026-10-21

TENANT SIZE 120 users

5 sections in one reportPowered by **Zybil Technologies** · Verified Microsoft Partner · Read-only, agentless assessment

What is in this report

This report brings the selected assessments for Northwind Logistics Pvt Ltd into one document, so you read one report instead of several. Each section stands on its own and states what was checked and how.

1	Microsoft 365 security posture Secure Score 36.2%, 44 open gaps (17 high priority)	p. 4
2	Cloud infrastructure posture Azure + AWS, 67 unhealthy findings (14 high)	p. 13
3	Connected app risk 23 third-party apps, 2 high risk	p. 16
4	Business email compromise 1 critical finding: hidden forwarding rule	p. 18
5	SOC 2 compliance drift 2 controls drifted since baseline	p. 20

ABOUT THIS SAMPLE

This is the exact format Beacon Technology Partners delivers to its clients, generated on the Zybim platform and carrying the partner's own name and colours. The organisation, people and findings are fictional. Partners can white-label every report; end customers can also run the Microsoft 365 assessment free at zybim.com.

Who this report is for

One assessment, three audiences. Each reader can go straight to the part they need.

Leadership & CISOs

Know where you stand in one page.

- Secure Score benchmarked against peers
- Top risks in plain language, ranked by impact
- A 30 / 60 / 90-day plan with clear owners
- Monthly monitoring shows the trend to the board

Auditors & compliance

Evidence mapped to the clauses you test.

- Every finding tagged to SOC 2, ISO 27001:2022, NIST CSF 2.0
- India DPDP Act s.8(5) and CERT-In Directions views
- Drift alerts with dates: proof controls stayed on between audits
- Read-only method and permissions documented

IT teams & MSPs

Exact fixes, not generic advice.

- Step-by-step remediation with Microsoft Learn links
- Effort and user-impact rating per control
- Licence waste and licence gaps in the same report
- White-label: your logo, colours and domain

What the platform covers

Microsoft 365

Secure Score, 90+ controls, Copilot readiness, licences

Cloud

Azure, AWS and GCP posture via Defender for Cloud

Connected apps

OAuth apps, consent settings, risky permissions

Email threats

Hidden inbox rules and forwarding used in invoice fraud

Compliance drift

SOC 2 / CIS controls watched continuously

HOW IT WORKS

1. Approve a publisher-verified Microsoft app with read-only permissions. 2. The platform reads configuration and Microsoft's own Secure Score data, then benchmarks and maps it. 3. You receive this report, and can switch on monthly monitoring. No agents to install. Revocable in one click. Email and file contents are never read.

SECTION 1 OF 5

Microsoft 365 security posture

Secure Score, gap roadmap, licences and cost

Secure Score 36.2%, 44 open gaps (17 high priority)

This section answers

- How secure is the tenant compared with similar organisations?
- Which fixes recover the most protection for the least effort?
- Which audit clauses and attack techniques are affected?
- Are we paying for licences we don't use, or missing ones we need?

Executive summary

36.2%

Secure Score

AT RISK

Northwind Logistics Pvt Ltd scores 92 of 254 available Microsoft Secure Score points (36.2%). Microsoft's comparison group for organisations of a similar size averages 44.8% (113.8 of 254 points), so the tenant is 8.6 percentage points below that benchmark. The assessment found 44 open improvement opportunities worth 162 points: 17 high priority, 24 medium and 3 lower priority. 31 of them are protections your licences already include but that are not switched on yet, which makes them the fastest wins.

SECURE SCORE

36.2%

92 of 254 points

PEER AVERAGE

44.8%

113.8 of 254 points

OPEN ACTIONS

44

worth 162 points

HIGH PRIORITY

17

24 medium, 3 lower

Benchmark

Your organisation

36.2%

Peer average

44.8%

8.6 percentage points below the peer average.

HOW TO READ THIS REPORT

Microsoft Secure Score measures how fully your tenant uses the security controls already included in your licensing. Each recommended action below shows the points it recovers, its category, expected user impact, and implementation effort, so priorities can be set on impact, not guesswork. Not-started controls are protections you are licensed for but not using at all.

Where the gaps are

Open improvement opportunities grouped by security domain, ranked by recoverable points.

SECURITY DOMAIN	OPEN ACTIONS	NOT STARTED	POINTS AVAILABLE
Apps	31	29	+118
Identity	7	5	+24
Data	4	4	+12
Device	2	2	+8

Priority remediation roadmap

All 44 improvements, ranked by Secure Score points recovered, each with the steps to fix it. Impact and effort ratings come from Microsoft's control profiles for your tenant.

1 Ensure multifactor authentication is enabled for all users

ZB-ID-003 · FAIL

HIGH PRIORITY

Identity

+10 pts

User impact: Moderate

Effort: Low

27 of 120 users can sign in with a password alone. Require MFA for every user; with Business Standard this means turning on security defaults, or Conditional Access once Entra ID P1 is licensed. Exclude two monitored break-glass accounts.

[Full steps: Multifactor authentication](#)

Mitigates: Account breach, Password Cracking

SOC 2 CC6.1 | ISO 27001 A.8.5 | MITRE T1078.004, T1110

2 Create Safe Links policies for email messages

ZB-AP-001 · FAIL

HIGH PRIORITY

Apps

+9 pts

User impact: High

Effort: Medium

Ensure that all users have an assigned Safe Links policy, by either updating your existing policies or creating new ones, with URLs rewritten and checked against a list of known malicious links when a user clicks the link.

[Full steps: Safe Links](#)

SOC 2 CC6.8, CC6.6 | ISO 27001 A.8.7 | MITRE T1566.002

3 Block legacy authentication protocols

ZB-ID-004 · FAIL

HIGH PRIORITY

Identity

+8 pts

User impact: Low

Effort: Low

Legacy protocols such as POP, IMAP and SMTP AUTH do not support MFA and are the main route for password-spray attacks. 4 accounts signed in with legacy clients in the last 30 days; move them to modern clients, then block.

[Full steps: Block legacy authentication](#)

Mitigates: Password Cracking, Account breach

SOC 2 CC6.1, CC6.6 | ISO 27001 A.8.5 | MITRE T1110.003, T1078.004

4 Turn on Safe Attachments in block mode

ZB-AP-054 · FAIL

HIGH PRIORITY

Apps

+8 pts

User impact: High

Effort: Medium

Ensure that all users have an assigned Safe Attachments policy in Block mode by either updating your existing policies or creating new ones.

[Full steps: Safe Attachments](#)

SOC 2 CC6.8, CC6.6 | ISO 27001 A.8.7 | MITRE T1566.001, T1204

5

Ensure that intelligence for impersonation protection is enabled

ZB-AP-002 · FAIL

HIGH PRIORITY

Apps

+8 pts

User impact: Unknown

Effort: Medium

Ensure that all users have an assigned anti-phishing policy with 'Enable mailbox intelligence' and 'Enable intelligence for impersonation protection' turned on.

Full steps: Microsoft Secure Score

SOC 2 CC6.8, CC6.6 | ISO 27001 A.8.7 | MITRE T1566

6

Ensure all forms of mail forwarding are blocked and/or disabled

ZB-AP-031 · FAIL

HIGH PRIORITY

Apps

+5 pts

User impact: Unknown

Effort: Unknown

Automatic forwarding to external domains is allowed. Set the outbound spam policy's automatic forwarding to 'Off' or 'Automatic – System-controlled', and remove transport rules that forward to external domains. See also Section 4.

Full steps: Microsoft Secure Score

Mitigates: Data Exfiltration, Account breach

SOC 2 CC6.7, CC7.2 | ISO 27001 A.5.14, A.8.16 | MITRE T1114.003

7

Ensure DLP policies are enabled

ZB-DA-001 · FAIL

HIGH PRIORITY

Data

+5 pts

User impact: High

Effort: Medium

Ensure that at least one Microsoft 365 DLP policy exists in the Microsoft Purview compliance portal. Start with the built-in templates for financial data and Indian personal data in test mode.

[Full steps: Data loss prevention](#)

SOC 2 CC6.7 | ISO 27001 A.8.12, A.5.14 | MITRE T1567

8

Ensure user consent to apps accessing company data on their behalf is not allowed

ZB-ID-001 · FAIL

HIGH PRIORITY

Identity

+4 pts

User impact: Moderate

Effort: Low

Go to Microsoft Entra ID > Enterprise applications > Consent and permissions, and select 'Allow user consent for apps from verified publishers, for selected permissions'. See Section 3 for the apps already connected.

[Full steps: Configure how users consent to applications](#)

Mitigates: Data Exfiltration, Data Spillage

SOC 2 CC6.1, CC9.2 | ISO 27001 A.5.19 | MITRE T1528, T1550.001

9

Ensure mailbox auditing for all users is Enabled

ZB-AP-038 · WARN

MEDIUM PRIORITY

Apps

+3 pts

User impact: Unknown

Effort: Low

Connect to Exchange Online and run: Set-OrganizationConfig -AuditDisabled \$false. Then confirm auditing is on for every mailbox.

[Full steps: Mailbox auditing](#)

Mitigates: Data Exfiltration, Account breach

SOC 2 CC7.2, CC7.3 | ISO 27001 A.8.15, A.8.16 | MITRE T1562.008

Improvements 10–44 continue in the full report in the same format.

Copilot readiness: early signals

Microsoft 365 Copilot shows people anything they can already open, so loose sharing becomes visible overnight. This is a tenant-level preview from settings and directory data only. File contents are never read.

3 oversharing signals to address before rollout

18 guest accounts · 0 of 0 Copilot seats assigned

2 Public Microsoft 365 groups readable by everyone in the organisation

2 groups (both with a Team) are Public: anyone in the organisation can join and read their content, and so can Copilot on their behalf. Examples: Finance Team, HR Policies. Switch any that hold sensitive material to Private.

SharePoint default sharing link is "Anyone with the link"

New sharing links work for anyone, without sign-in. Change the default to "People in your organisation".

No sensitivity labels are published

Copilot cannot tell confidential files apart. Publish a basic label set (Public, Internal, Confidential).

License & cost optimization

What your Microsoft 365 licensing costs, and where paid seats might be going to waste.

EST. MONTHLY WASTE

\$150

\$1,800 a year

LICENSED USERS

122

110 Business Standard · 12 Premium

TO REVIEW

14

seats

Finding	Seats	Est. per month
Business Standard licences on disabled accounts	6	\$84
Business Premium licences not assigned to anyone	3	\$66
Licensed users with no sign-in for 90+ days (review)	5	not counted

LICENSING NOTE

14 controls in this report cannot be fully enforced on Business Standard, because they need Microsoft Entra ID P1 (Conditional Access), Intune or Defender for Business. These are included in Microsoft 365 Business Premium. Reclaiming the seats above offsets part of an upgrade. Prices are US list prices; your partner can quote local pricing.

Additional configuration checks

The platform's own read-only checks of your Microsoft 365 and Entra ID settings, beyond Microsoft Secure Score. 27 checks assessed: 12 need attention, 15 pass. 9 could not be assessed (see below). Five examples are shown.

No guest accounts hold administrator roles

ZB-ID-038 HIGH

Administrator roles are held by 1 guest account.

HOW TO FIX

1. Open Entra admin center > Roles & admins and review each role.
2. Remove guest accounts from administrator roles.
3. Create a dedicated member account if the person needs the role.

SOC 2 CC6.3 | ISO 27001 A.8.2, A.5.18, A.5.15

Administrators use separate accounts without licences

ZB-ID-040 MEDIUM

3 administrator accounts hold Microsoft 365 licences, which suggests daily-use accounts hold admin rights.

HOW TO FIX

1. Give each administrator a separate admin account with no mailbox or licence.
2. Use the daily account for email and the admin account only for administration.

SOC 2 CC6.3 | ISO 27001 A.8.2, A.5.18

An admin consent workflow is enabled

ZB-AP-056 MEDIUM

There is no admin consent workflow, so blocked users have no safe route to request an app.

HOW TO FIX

1. Open Entra admin center > Enterprise applications > Consent and permissions > Admin consent settings.
2. Turn on 'Users can request admin consent'.
3. Name the reviewers.

SOC 2 CC6.1, CC9.2 | ISO 27001 A.5.19

A phishing-resistant method (passkey/FIDO2) is available

ZB-ID-035 LOW

No phishing-resistant method is enabled.

HOW TO FIX

1. Open Entra admin center > Protection > Authentication methods > Policies.
2. Enable Passkey (FIDO2), starting with administrators.

SOC 2 CC6.1 | ISO 27001 A.8.5

Only admins and designated inviters can invite guests

ZB-ID-027 MEDIUM

Anyone in the tenant, including guests, can invite guests.

HOW TO FIX

1. Open Entra admin center > External Identities > External collaboration settings.
2. Set guest invite settings to admin roles or the Guest Inviter role only.

SOC 2 CC6.1, CC9.2 | ISO 27001 A.5.15, A.5.18

Passing checks

Administrators are required to use MFA; SMS and voice-call sign-in methods are disabled; Administrator accounts are cloud-only; Disabled accounts hold no administrator roles; App registrations have no expired credentials; A security notification contact is set; All domains added to the tenant are verified; and 8 more.

Not assessed

Not counted as passes or failures; the reason is a licence, not a finding. Needs Microsoft Entra ID P1 (Conditional Access), which this tenant does not appear to have. Affects: Access requires a compliant device; Sign-in frequency for sensitive access; Trusted locations; and 6 more.

Audit view: framework clauses

Which of your Microsoft 365 controls provide evidence toward each clause. 101 of the 102 controls assessed in this report are mapped.

Indicative mapping, pending independent review. A clause with no open finding means no gap was found in the controls assessed; it is not a statement of compliance. Formal audits and certification are performed by independent auditors.

SOC 2 (Trust Services Criteria)

CC6.1 Logical access security

24 OPEN OF 44

Open: Ensure multifactor authentication is enabled for all users; Block legacy authentication protocols; Ensure user consent to apps ... and 21 more

CC6.3 Role-based access and least privilege

2 OPEN OF 8

Open: No guest accounts hold administrator roles; Administrators use separate accounts without licences

CC6.6 Protection against external threats

18 OPEN OF 40

Open: Create Safe Links policies for email messages; Turn on Safe Attachments in block mode and 16 more

CC6.7 Restricting data transmission and movement

7 OPEN OF 8

Open: Ensure DLP policies are enabled; Ensure all forms of mail forwarding are blocked and 5 more

CC6.8 Preventing and detecting malicious software

21 OPEN OF 34

Open: Turn on Safe Attachments in block mode; Ensure intelligence for impersonation protection is enabled and 19 more

CC7.2 Monitoring for anomalies

5 OPEN OF 13

Open: Ensure mailbox auditing for all users is Enabled; Ensure all forms of mail forwarding are blocked and 3 more

CC9.2 Vendor and business-partner risk

6 OPEN OF 8

Open: Ensure user consent to apps ...; An admin consent workflow is enabled and 4 more

ISO/IEC 27001:2022 (Annex A)

A.5.15 Access control

10 OPEN OF 17

Open: Only admins and designated inviters can invite guests; No guest accounts hold administrator roles and 8 more

A.5.17 Authentication information

NO GAP FOUND (9 ASSESSED)

A.5.19 Information security in supplier relationships

3 OPEN OF 3

Open: Ensure user consent to apps ...; An admin consent workflow is enabled and 1 more

A.8.2 Privileged access rights

2 OPEN OF 7

Open: No guest accounts hold administrator roles; Administrators use separate accounts without licences

A.8.5 Secure authentication

6 OPEN OF 15

Open: Ensure multifactor authentication is enabled for all users; Block legacy authentication protocols and 4 more

A.8.7 Protection against malware

20 OPEN OF 33

Open: Turn on Safe Attachments in block mode; Create Safe Links policies for email messages and 18 more

A.8.12 Data leakage prevention

2 OPEN OF 2

Open: Ensure DLP policies are enabled; Ensure additional storage providers are restricted in Outlook on the web

A.8.15 Logging

1 OPEN OF 2

Open: Ensure mailbox auditing for all users is Enabled

NIST Cybersecurity Framework 2.0 (categories)

PR.AA Identity management, authentication and access control

23 OPEN OF 45

Open: Ensure multifactor authentication is enabled for all users; Block legacy authentication protocols and 21 more

PR.DS Data security

6 OPEN OF 6

Open: Ensure DLP policies are enabled; Ensure all forms of mail forwarding are blocked and 4 more

DE.CM Continuous monitoring

20 OPEN OF 41

Open: Ensure mailbox auditing for all users is Enabled; Turn on Safe Attachments in block mode and 18 more

RS.MA Incident management

NO GAP FOUND (1 ASSESSED)

India DPDP Act 2023

s.8(5) Reasonable security safeguards to prevent personal data breach

19 OPEN OF 32

Open: Ensure multifactor authentication is enabled for all users; Ensure DLP policies are enabled and 17 more

India CERT-In Directions (28 Apr 2022)

Logs Maintain ICT system logs for 180 days

1 OPEN OF 2

Open: Ensure mailbox auditing for all users is Enabled

Incident Report cyber incidents within 6 hours

2 OPEN OF 3

Open: Ensure all forms of mail forwarding are blocked and/or disabled; Set automatic email forwarding rules to be system controlled

Threat view: MITRE ATT&CK

The same findings grouped by how an attacker would use them, in kill-chain order. Counts show open findings out of the controls assessed.

Initial Access

T1566 Phishing

16 OPEN OF 26

Open: Turn on Safe Attachments in block mode; Ensure intelligence for impersonation protection is enabled and 14 more

T1078.004 Valid Accounts: Cloud Accounts

8 OPEN OF 23

Open: Ensure multifactor authentication is enabled for all users; Block legacy authentication protocols and 6 more

Credential Access

T1110.003 Brute Force: Password Spraying

2 OPEN OF 3

Open: Block legacy authentication protocols; Ensure multifactor authentication is enabled for all users

T1528 Steal Application Access Token

2 OPEN OF 2

Open: Ensure user consent to apps ...; An admin consent workflow is enabled

Collection and Exfiltration

T1114.003 Email Collection: Email Forwarding Rule

2 OPEN OF 2

Open: Ensure all forms of mail forwarding are blocked; Set automatic email forwarding rules to be system controlled

T1567 Exfiltration Over Web Service

3 OPEN OF 3

Open: Ensure DLP policies are enabled; Ensure additional storage providers are restricted in Outlook on the web and 1 more

The full report lists all 9 tactics and 21 techniques.

Recommended next steps

FIRST 30 DAYS

Turn on MFA for all users and block legacy authentication, then create Safe Links and Safe Attachments policies. Remove the hidden forwarding rule found in Section 4 immediately. Together these recover about 35 Secure Score points.

DAYS 30–60

Work through impersonation protection, external forwarding and DLP (about 26 points). Restrict app consent and review the two high-risk apps in Section 3. Close the high-severity cloud findings in Section 2, starting with public storage and open management ports.

DAYS 60–90

Decide on Business Premium for Conditional Access and device compliance. Re-assess to measure improvement, then move to monthly posture monitoring so regressions are caught as they happen, and the evidence trail is ready for auditors and insurers.

Methodology & scope

Data is read through Microsoft Graph using the following application permissions granted in your tenant: AuditLog.Read.All (sign-in activity timestamps); Directory.Read.All (users, groups, licences and connected apps); MailboxSettings.Read (mailbox rule and forwarding settings, not message content); Policy.Read.All (Conditional Access and tenant policies); RoleManagementPolicy.Read.Directory (privileged-role policy settings); SecurityEvents.Read.All (Secure Score and control profiles). All are read-only and revocable at any time from the Microsoft Entra admin center. None of these permissions allows the platform to read email content or file contents. Scores and recommendations originate from Microsoft's own assessment of your tenant; the platform adds prioritisation, benchmarking, framework mapping and remediation planning. The peer average is Microsoft's own comparison value, shown as a percentage of the maximum score. This report reflects posture at the assessment timestamp and should be refreshed after remediation.

Ready to act on this roadmap?

Your free 30-minute walkthrough with Beacon Technology Partners sequences these findings into a remediation plan. Beacon Technology Partners can implement it end to end: security hardening, licensing, and monthly monitoring under one partner.

SECTION 2 OF 5

Cloud infrastructure posture

Azure, AWS and GCP through Microsoft Defender for Cloud

2 Azure subscriptions + 1 AWS account · 67 unhealthy findings (14 high)

This section answers

- How exposed are our cloud workloads, across every subscription and account?
- Which misconfigurations would an attacker scan for first?
- Which Defender protections are switched off?
- What should we fix first, and how?

Executive summary



NEEDS ATTENTION

Across 2 Azure subscriptions and 1 connected AWS account, Microsoft Defender for Cloud reports a combined secure score of 52%. The assessment found 67 unhealthy findings on 41 resources: 14 high, 31 medium and 22 low severity. Two storage locations are reachable from the internet, and virtual machine management ports are open to any address. Only the free foundational posture checks are active; no Defender workload protection plans are switched on.

SECURE SCORE

52%

all environments

HIGH

14

fix first

MEDIUM

31

findings

LOW

22

findings

Score by environment

ENVIRONMENT	RESOURCES	HIGH	SECURE SCORE
Azure · Production subscription	24	8	48%
Azure · Dev/Test subscription	9	2	61%
AWS · Logistics apps account	8	4	50%

Defender protection coverage

Protection plan	Resources in scope	Status
Foundational CSPM (free)	All 41	On
Defender CSPM (attack paths, agentless scanning)	41	Off
Defender for Servers	7 VMs (5 Azure, 2 AWS EC2)	Off
Defender for Storage	6 storage accounts / buckets	Off
Defender for SQL / databases	3 databases	Off

Top cloud findings

Ranked by severity and exposure. The full report lists all 67 findings by resource, with remediation steps.

1 Storage account allows public network access

HIGH

Azure · Production · stnwlogsdocs

The storage account accepts connections from any network, and one container allows anonymous read. Disable public blob access and restrict network access to selected networks or private endpoints.

[Full steps: Microsoft Defender for Cloud recommendation](#)

2 S3 bucket allows public read access

HIGH

AWS · nw-shipment-exports

Block Public Access is off for this bucket and its policy grants read to everyone. Turn on S3 Block Public Access at account and bucket level, then review who needs access.

[Full steps: Microsoft Defender for Cloud recommendation](#)

3 Management ports of virtual machines should be protected with just-in-time network access control

HIGH

Azure · Production · 3 VMs

RDP (3389) is open to any address on 3 VMs. Enable just-in-time VM access, or close the port and use Azure Bastion.

[Full steps: Microsoft Defender for Cloud recommendation](#)

4 MFA should be enabled for accounts with owner permissions on your subscription

HIGH

Azure · Production

2 owner accounts can manage the subscription without MFA. Require MFA for all accounts with owner or contributor rights.

[Full steps: Microsoft Defender for Cloud recommendation](#)

5 Machines should have vulnerability findings resolved

HIGH

Azure + AWS · 4 VMs

4 machines have critical OS vulnerabilities older than 30 days. Enable Defender for Servers for continuous vulnerability assessment and patch the listed packages.

[Full steps: Microsoft Defender for Cloud recommendation](#)

6 Diagnostic logs should be enabled for Key Vault and App Service

MEDIUM

Azure · Production · 5 resources

Without logs, an incident cannot be investigated. Send diagnostic logs to a Log Analytics workspace with 180-day retention (relevant to CERT-In log retention).

[Full steps: Microsoft Defender for Cloud recommendation](#)

SECTION 3 OF 5

Connected app risk

Third-party apps and what they can access

23 third-party apps, 2 high risk

This section answers

- Which outside apps can read our mail, files or directory?
- Which ones come from unverified publishers?
- Who approved them, and are they still used?

Executive summary

We reviewed 23 third-party apps (311 service principals in total, the rest being Microsoft's own services) connected to your tenant. 2 hold high-risk access and 4 more are worth reviewing. Your consent setting also lets users approve new apps without review.

THIRD-PARTY APPS

23

HIGH RISK

2

WORTH REVIEWING

4

App	Access held	Consented by	Risk
PDF Merge Online	Read and write all mail; read all files	1 user	HIGH
QuickSync Contacts	Read directory; read all users' calendars (application)	Admin, tenant-wide	HIGH
Calendar Sync Pro	Read and write calendars	3 users	REVIEW
CRM Connector (legacy)	Read directory	Admin, tenant-wide	REVIEW
Survey Builder	Read user profile, send mail as user	6 users	REVIEW
E-Sign Express	Read and write files the user selects	4 users	REVIEW

Users can consent to third-party apps without admin approval

ZB-ID-001 MEDIUM

This is the most common way a risky app gets connected. 'PDF Merge Online' above was approved this way.

HOW TO FIX

1. Open Entra admin center > Enterprise applications > Consent and permissions > User consent settings.
2. Choose "Allow user consent for apps from verified publishers, for selected permissions".
3. Turn on the admin consent workflow and name the reviewers.

Scope: only applications connected through Microsoft's own sign-in and consent screens are visible. This report never revokes or changes anything; every action is for your Global Administrator to apply.

SECTION 4 OF 5

Business email compromise

Hidden inbox rules and forwarding used in invoice fraud

1 critical finding on a finance mailbox

This section answers

- Is any mailbox silently forwarding or hiding financial email?
- Which accounts show signs of compromise?
- What exactly should we do now?

Executive summary

We checked mailbox rules and forwarding settings on all 120 mailboxes. One mailbox in the finance team has a hidden rule that forwards invoice and payment emails to an outside address, the classic sign of a compromised account. Act on this today.

CRITICAL

1

MAILBOXES CHECKED

120

EXTERNAL FORWARDING

2

1 hidden, 1 approved

!

Hidden rule forwarding invoices outside the company

ZB-BEC-001 · CRITICAL

accounts@northwind.example

Rule name: "." (a single dot, a common attacker trick)

Condition: subject or body contains "invoice", "payment", "bank details"

Action: forward to an external webmail address, then move to "RSS Feeds"

Created: 2026-10-18, shortly after a sign-in from an unfamiliar location

WHAT TO DO NOW

1. Delete the rule and reset the account's password.

2. Revoke all sessions and re-register MFA for this user.

3. Review sent items and recent payment requests; warn finance not to change bank details by email.

4. Block automatic external forwarding (see Section 1, item 6).

SOC 2 CC7.2, CC7.3 | ISO 27001 A.5.25, A.8.16 | MITRE T1114.003, T1564.008

Approved external forwarding

INFO

logistics-ops@ forwards to a carrier partner's domain. Confirm this is still needed and documented.

This check reads mailbox rule and forwarding settings only, never message content. With monitoring on, new rules like this raise an alert within hours, in plain language, with the fix.

Confidential. Prepared by Beacon Technology Partners · Powered by Zybim Technologies. Read-only, advisory assessment. Nothing in your tenant was changed.

Page 19 of 22

SECTION 5 OF 5

SOC 2 compliance drift

Access-control configuration against SOC 2 and CIS

2 controls drifted since the baseline

This section answers

- Have any controls changed since they were last verified?
- Who changed them, and when?
- Which SOC 2 criteria are affected?

Executive summary

Two monitored controls drifted from the baseline recorded on 2026-09-30: an MFA exclusion was added for one user, and a new Global Administrator was assigned. Both affect SOC 2 CC6 logical-access criteria. Legacy authentication remains blocked.

CRITICAL

0

HIGH

2

DRIFTED CONTROLS

2

Date	Change detected	Criteria	Severity
2026-10-12	MFA exclusion added for 1 user (sales team)	SOC 2 CC6.1 · CIS identity	HIGH
2026-10-15	New Global Administrator assigned (external contractor)	SOC 2 CC6.2, CC6.3 · CIS privileged access	HIGH

CONTROLS PASSING

PASS

CC6.1

Legacy authentication is blocked

PASS

CC6.1

Administrators are required to use MFA

WHAT TO DO

- Confirm both changes were approved through your change process.
- Remove the MFA exclusion, or replace it with a time-limited exception.
- Move the contractor to the least-privileged role needed, with an end date.
- Keep this report as evidence that access controls were monitored during the audit period.

Scope: this report supports a SOC 2 programme by monitoring relevant Microsoft 365 configuration. It is not a SOC 2 audit, examination or attestation; those are performed by an independent licensed CPA firm.

About the platform

This report was produced on **Zybir**, a Microsoft-native security assessment and monitoring platform from Zybir Technologies, a verified Microsoft partner. Read-only access through a publisher-verified Entra app; nothing is installed and nothing in your tenant is changed.

Microsoft 365 assessment Secure Score, 90+ controls, framework and MITRE mapping, licence savings, Copilot readiness. Free	Cloud posture assessment Azure, AWS and GCP posture through Defender for Cloud, ranked findings and fixes. Paid
Posture Monitoring Monthly re-assessment, score trend and regression alerts. Audit- and insurance-ready history. From \$99/mo	Threat Detection Agent (BEC) Always-on detection of hidden inbox rules and forwarding on financial mail. \$39/mo
Compliance Drift Monitor Continuous SOC 2 / CIS drift detection with dated evidence. \$79/mo	AI Security Bundle Threat Detection, Compliance Drift and Connected App Risk agents together. \$99/mo

Prices are list prices in USD on Microsoft Marketplace, billed through your Microsoft invoice, and may differ through partners.

FOR MSPs, RESELLERS AND AUDIT FIRMS

Deliver this report under your own brand. Your logo, colours and domain on every report, "Powered by Zybir" disclosed. Earn margin on assessments, monitoring, licensing and remediation, without building a security team.

zybir.com/partners.html