Cyber Insurance Readiness on Microsoft 365

The five controls insurers ask about, where each one already lives in your Microsoft licensing, and how to prove it at renewal.

Centered Networks · Managed Intelligence for organizations running on Microsoft

Your renewal questionnaire is a security audit

Cyber insurance applications now ask direct questions: *Is MFA enforced for all users? Do you run EDR on every endpoint? Who watches alerts after hours? Are backups protected from ransomware?*

Two things make those questions harder than they look:

1. **Your answers are a legal statement.** If a claim is filed and the control wasn't actually in place, the insurer can dispute the claim. In 2022, after a ransomware claim, Travelers asked a federal court to rescind a policy, saying the insured's application overstated its use of MFA (*Travelers v. International Control Services*). 2. **"We have the license" is not the same as "it's turned on."** Most mission-driven organizations on Microsoft 365 Business Premium already pay for three of the five controls, and a fourth is one add-on away. Many have not configured them, enforced them for every user, or kept a record that proves it.

This guide maps each control to the Microsoft tools you likely already own, shows what "done" looks like, and lists the evidence to keep on file before you sign the questionnaire.

Centered Networks is a Microsoft Solutions Partner, not an insurance broker. We don't sell coverage or set premiums, and no control guarantees coverage or a lower rate. We help you put the controls in place, keep them in place, and document them.

The five controls at a glance

#	What insurers ask about	Where it lives in Microsoft	Included in Business Premium?
1	**Multi-factor authentication (MFA)** for every user, admin, and remote access	Microsoft Entra ID P1 — Conditional Access	**Yes**
2	**Email security** against phishing, malicious links and attachments,	Microsoft Defender for Office 365 Plan 1 — Safe Links, Safe	**Yes**

#	What insurers ask about	Where it lives in Microsoft	Included in Business Premium?
	impersonation	Attachments, anti-phishing	
3	**EDR / MDR** — endpoint detection and response, and someone watching it	Microsoft Defender for Business (EDR, automated investigation) + a monitoring team	**EDR yes.** Monitoring is a service, not a license
4	**Security awareness training** with phishing simulation	Attack simulation training in Defender for Office 365 Plan 2	**No** — add-on (Microsoft Defender Suite for Business Premium)
5	**Backups protected from ransomware**	Microsoft 365 Backup (immutable, append-only restore points)	**No** — separately billed. See the note on "segregated" below

1. Multi-factor authentication

Why insurers care. Stolen passwords are the most common way in. MFA stops a stolen password from being enough on its own.

What you already own. Business Premium includes Microsoft Entra ID P1, which includes Conditional Access — the policy engine that enforces MFA by user, app, device and location.

What "done" looks like

- MFA enforced by Conditional Access for **every** user — not just "registered" or "encouraged."
- Admin accounts separated from daily accounts, with phishing-resistant MFA where possible.
- Legacy authentication blocked (old protocols that skip MFA).
- MFA required on remote access, including VPN and remote desktop if you still run them.

Evidence to keep: Conditional Access policy export, MFA registration report, list of exceptions with the reason and an owner for each.

Common gap: a handful of shared mailboxes, service accounts or board members exempted "for now." Insurers ask about *all* users. Answer for every account, including the exceptions.

2. Email security

Why insurers care. Email is the front door for phishing, business email compromise (BEC) and malware. The FBI's 2025 Internet Crime Report counted more than $3 billion in reported BEC losses, from nearly 25,000 complaints.

What you already own. Business Premium includes Microsoft Defender for Office 365 Plan 1: Safe Links (checks links at click time), Safe Attachments (opens attachments in a sandbox before delivery, including in SharePoint, OneDrive and Teams), and anti-phishing with impersonation protection.

What "done" looks like

- Safe Links and Safe Attachments policies on for all users, not the defaults only.
- Impersonation protection set for your executives, finance staff and your own domains.
- SPF, DKIM and DMARC published for every domain you send from, with DMARC moving toward enforcement.
- External-sender tagging on, so staff can see when "the CEO" is writing from outside.

Evidence to keep: Defender for Office 365 policy summary, DMARC record and report, a monthly count of blocked phishing and malware.

Common gap: a third-party email filter sitting in front of Microsoft 365 that you also pay for. Often Defender for Office 365 can replace it — one less tool and one less bill.

---

3. Endpoint detection and response (EDR) and managed detection and response (MDR)

Why insurers care. Antivirus alone looks for known threats. EDR watches behavior on every laptop, desktop and server and can stop an attack in progress. MDR adds people who respond when an alert fires at 2 a.m.

What you already own. Business Premium includes Microsoft Defender for Business, which provides next-generation protection, attack surface reduction, endpoint detection and response, and automated investigation and remediation, for organizations up to 300 users. Servers need the Defender for Business Servers add-on (or Defender for Servers).

What "done" looks like

- Every device onboarded — Windows, Mac and mobile — with a report showing none are missing.
- Servers covered by a server license, not skipped.
- Attack surface reduction rules on, tamper protection on.
- **Someone watching after hours.** EDR raises the alarm; it doesn't decide what to do on a holiday weekend. This is the question insurers increasingly ask: *who responds, and how fast?*

How Centered Networks covers the "who watches" question. CompleteCare Shield runs on the Microsoft Defender tools you already license. The CN SOC works your Defender alerts during business hours, and CN's 24/7 SOC partner monitors identities and endpoints around the clock with active response.

Evidence to keep: device onboarding report (total / not onboarded), Shield or MDR service description, incident summaries from the last 12 months.

---

4. Security awareness training

Why insurers care. People click. Training and realistic phishing tests lower the odds and show the insurer that you measure it.

What Microsoft offers. Attack simulation training — phishing simulations with built-in training — is part of Defender for Office 365 Plan 2. Business Premium includes Plan 1, so this is an add-on. The cleanest route is **Microsoft Defender Suite for Business Premium**, which is available for both commercial and nonprofit Business Premium and also adds Entra ID P2, Defender for Identity, Defender for Endpoint Plan 2 and Defender for Cloud Apps.

What "done" looks like

- Onboarding training for every new hire, then a regular cadence (quarterly is common).
- Phishing simulations with a tracked click rate and repeat-clicker follow-up.
- A simple "report phishing" button staff actually use.

Evidence to keep: completion rates, simulation results over time, the policy that says how often training runs.

---

5. Backups protected from ransomware

Why insurers care. If ransomware encrypts your files, a clean backup decides whether you pay or recover.

What Microsoft offers. Microsoft 365 Backup backs up OneDrive, SharePoint and Exchange Online with append-only restore points that can't be overwritten, and can restore large volumes quickly. It is billed separately from Business Premium.

A note on "segregated" backups. Microsoft 365 Backup keeps backup data inside the Microsoft 365 data trust boundary. Some insurers' questionnaires ask for backups that are *offline, off-site or logically separated* from production. Read the exact wording on your application. Depending on the answer, you may need Microsoft 365 Backup, a partner backup built on Microsoft 365 Backup Storage, or a separate copy. We'll help you pick the one that matches what you attest to.

What "done" looks like

- Mailboxes, OneDrive and SharePoint sites covered by a backup policy — including new users.
- Servers and line-of-business systems backed up too, if you still have them.
- **A tested restore**, on a schedule, with the result written down.
- Backup admin access protected by MFA and limited to a few named people.

Evidence to keep: backup policy scope, last test-restore date and result, list of backup admins.

Beyond the five: what else is showing up on applications

Applications keep getting longer. Questions now common on renewal forms include:

- **Device management** — are company devices encrypted and patched? (Intune, included in Business Premium.)
- **Privileged access** — who has admin rights, and is it reviewed?
- **Incident response plan** — is it written down, and does everyone know their role?
- **Data protection** — do you know where sensitive data lives and who can share it? (Microsoft Purview; this is also what keeps Copilot from surfacing the wrong files.)

Your renewal-readiness checklist

Answer each one honestly before you sign:

- ☐ MFA is enforced by policy for **every** user, including admins and exceptions.
- ☐ Legacy authentication is blocked.
- ☐ Safe Links, Safe Attachments and impersonation protection are configured.
- ☐ DMARC is published for every sending domain.
- ☐ Every laptop, desktop and server is onboarded to Defender, with a report to prove it.
- ☐ Someone responds to security alerts 24/7, and we can name who.
- ☐ Staff complete security training and phishing simulations on a schedule.
- ☐ Email, files and servers are backed up in a way that matches what our application asks.
- ☐ We've tested a restore in the last 6 months and written down the result.
- ☐ We have a written incident response plan.
- ☐ We keep the evidence for each answer in one place.

If you checked fewer than all of them, you're not alone — and most of the gap is usually configuration, not new spending.

How Centered Networks helps

Cyber Insurance Readiness Review. We compare your insurance questionnaire against your Microsoft 365 tenant, control by control. You get:

- A plain-language **gap list**: what's on, what's licensed but off, and what's missing.
- An **evidence pack** you can keep on file for each control.

- A **plan timed to your renewal date**, fiscal year and budget cycle.

Then, if you want us to:

- **M365 InstantOn** turns on the Business Premium security baseline you already pay for.
- **CompleteCare Foundations** keeps it on, with a weekly Security & Compliance Monitoring Report.
- **CompleteCare Shield** answers "who watches after hours" on the Microsoft Defender stack.

Centered Networks has served mission-driven organizations since 2004 and holds five Microsoft Solutions Partner designations, including Security and Modern Work.

The Review is a fixed **$1,950**, credited in full toward M365 InstantOn if you go ahead within 30 days.

Book your Cyber Insurance Readiness Review · centerednetworks.com/cyber-insurance-readiness

Centered Networks, Inc. · PO Box 1801, Ennis, MT 59729-1801

© 2026 Centered Networks. Microsoft product names are trademarks of Microsoft Corporation; licensing facts were verified against Microsoft Learn on 2026-10-15 and may change. This guide is general information, not insurance or legal advice; Centered Networks is not an insurance broker.