CyberProva · reviewed 23 October 2026

Microsoft 365 Cyber Insurance Renewal Checklist

Use these eight questions to prepare an evidence discussion with your IT team. Keep your insurer's exact wording, definitions and scope with the final response.

> Illustrative preparation prompts, not universal requirements, insurance advice or an insurer-approved assessment. A planned fix or missing record is not a confirmed control. Your organisation reviews the answers with the broker or insurer.

What your insurer may ask

Illustrative question	What to check or request
Is MFA enforced for the users and services in scope?	Entra Conditional Access or Security Defaults configuration, policy state, target accounts/apps, exclusions and authentication-method records. Confirm the form's scope beyond Microsoft 365.
Are privileged accounts protected?	Entra role assignments, separate admin accounts, MFA enforcement and emergency-access review. If PIM is used, include eligible roles, activation/approval settings and the necessary P2/Governance licensing.
Is endpoint detection and response deployed?	Defender for Business or the chosen EDR service: reconciled device inventory, onboarding and sensor-health reports, exclusions and the provider's review. A purchased licence is not a deployment record.
Are systems and data backed up and recoverable?	Backup scope, retention, access separation and isolation/immutability where claimed, plus a completed restore test. Explain which Exchange/SharePoint retention or recycle-bin features are used and what separate backup covers.
Is external email forwarding controlled?	Exchange Online mailbox forwarding and inbox-rule review, applicable outbound anti-spam and mail-flow policies, external destinations and approved exceptions.
Are security incidents monitored and acted on?	Defender or other service alert coverage, redacted triage examples, monitoring responsibilities and hours, escalation contacts and tested response procedures.
Are devices patched and vulnerabilities managed?	Intune or other update policies, assignment/deployment results, device-compliance and vulnerability reports, unsupported software and outstanding exceptions.
Are relevant third-party suppliers assessed?	Supplier and connected-application register, service responsibilities, assurance documents, permission reviews, review dates and unresolved actions. Microsoft 365 findings do not audit every supplier.

Licensing: Conditional Access needs Entra P1/P2; Business Premium includes P1. Security Defaults is an Entra Free alternative. PIM needs P2 or Entra ID Governance for relevant users. A licence alone does not prove deployment or effective coverage.

Keep evidence states separate

Worked example: three different evidence states

Fictional preparation example, not a customer result or insurer-approved response. Keep the source and review state with each proposed answer.

- Automatically observed: the core read-only collector retrieved current Entra role assignments. This supports an inventory statement; it does not establish that the assignments are justified or that MFA always applies.
- Evidence supplied: the IT provider uploaded a dated Defender onboarding report. It remains supplied evidence until your organisation reviews its scope, device reconciliation and exceptions; upload alone is not verification.
- Not yet confirmed: no completed restore-test record is held. Keep recovery unconfirmed, request the result and clarify the final answer with the responsible reviewer and insurer rather than turning it into a pass.

Evidence review register

Print this sheet or copy the fields into your own register. Record the source, date, scope, exceptions and reviewer. Use states such as automatic observation, evidence supplied, reviewed evidence or not yet confirmed.

Organisation: _____ Renewal date: _____

Responsible reviewer: _____ Review date: _____

Complete one row for each question or gap

Question / scope	Source / date / evidence state	Reviewer / exceptions	Next action / owner / due date

> Retention policies, recycle bins and version history have different purposes and limits. Do not assume they equal an independently managed backup or meet the insurer's recovery definition. Request backup scope, separation and completed restore-test records.

CyberProva provides selected read-only observations and an evidence workflow. Free includes 3 lifetime core assessments and an on-screen summary; your own report exports and questionnaire workflow require Business or above. This worksheet needs no account.

References: NCSC cyber insurance guidance · Microsoft retention guidance · CyberProva check scope