COPILOT HEALTH CHECK

Microsoft 365 Copilot Security and Adoption Checklist

A practical two-week review of tenant configuration, permissions, sensitivity labels, data loss prevention and operational readiness.

Start with a Copilot Health Check

If Copilot is already live, the usual starting point is an audit of your Microsoft 365 tenant configuration, permissions, sensitivity labels and data loss prevention controls. We identify security and configuration gaps, agree priorities and provide a clear remediation plan. A standard assessment is normally completed within ten working days, subject to tenant size, access and the complexity of any issues found.

Prepared by PSTG

Modern Workplace, Cyber Security and AI Adoption Services

PSTG

Copilot can expose existing weaknesses faster

Microsoft 365 Copilot works with the identity, permissions and information protection controls already configured in Microsoft 365. It does not give a user new access by itself. However, it can make information that a user can already access much easier to locate, summarise and reuse. This means historic oversharing, weak permissions or inconsistent data classification can become more visible once Copilot is introduced.

A Copilot Health Check establishes whether the service is operating on a secure and governed foundation. It also checks whether licences, reporting, user support and adoption controls are delivering value rather than simply adding cost.

> **The objective**
>
> To give leadership a clear view of the current risk position, immediate actions and the practical steps required to use Copilot securely and productively.

Who should use this checklist?

- Organisations that have already assigned Microsoft 365 Copilot licences.
- Businesses that enabled Copilot quickly and now want to confirm the configuration is secure.
- IT and security teams concerned about SharePoint, Teams or OneDrive oversharing.
- Organisations that need evidence of AI governance, data protection and user oversight.
- Businesses with low Copilot usage or uncertainty about measurable value.

What the health check produces

Risk findings	Remediation plan	Adoption baseline
A prioritised register of security, configuration and governance gaps.	Actions, owners, dependencies and recommended completion dates.	Usage, licensing and support findings with practical next steps.

Eight areas of assessment

The checklist is designed to provide a balanced review. It covers the security controls around Copilot, but also checks whether the service is licensed, supported and adopted in a way that can deliver business value.

1. Service scope and licensing

Confirm which Copilot services are enabled, who has access and whether licences match business need.

2. Identity and administration

Review privileged roles, multifactor authentication, Conditional Access and administrative ownership.

3. Permissions and oversharing

Identify broad SharePoint, Teams and OneDrive access that may expose unnecessary information.

4. Sensitivity labels

Check whether important information is classified and whether labels apply suitable protection.

5. Data loss prevention

Review whether DLP policies address sensitive prompts, files, emails and AI interactions.

6. Audit and compliance

Confirm interactions can be investigated and that retention, eDiscovery and incident processes are understood.

7. Agents and connected data

Review Copilot agents, plugins, connectors and any additional data sources or actions.

8. Adoption and support

Measure use, identify training gaps and confirm employees know where to get help.

Suggested rating scale

Rating	Meaning	Recommended response
Critical	Immediate exposure	Contain or restrict the risk and assign an urgent owner.
High	Material weakness	Remediate as a priority, normally within 30 days.
Medium	Control improvement	Include in the agreed improvement plan.
Low	Optimisation	Address through normal service improvement activity.

3 | SERVICE SCOPE, LICENSING AND TENANT CONFIGURATION

Confirm that the service has a controlled scope, named ownership and a reliable configuration baseline.

#	Assessment question	Evidence to review	Status / action
1	Is there an accurate list of users with Microsoft 365 Copilot, Copilot Chat and any related AI licences?	Admin centre licence export; group-based licensing	Not reviewed Gap Partial Met N/A
2	Are licences assigned to roles with an agreed business case rather than to users without a defined need?	Licence assignment list; role/use-case mapping	Not reviewed Gap Partial Met N/A
3	Are Microsoft 365 Apps, Teams and network settings compatible with the intended Copilot experience?	Update channels; app versions; network configuration	Not reviewed Gap Partial Met N/A
4	Are optional Copilot features and previews reviewed before they are enabled?	Release preferences; message centre; change process	Not reviewed Gap Partial Met N/A
5	Is there a named technical owner and a named business owner for Copilot?	Service ownership record; RACI	Not reviewed Gap Partial Met N/A
6	Is there a current record of the tenant configuration and any approved exceptions?	Configuration baseline; exception register	Not reviewed Gap Partial Met N/A

4 | IDENTITY, ACCESS AND ADMINISTRATION

Copilot inherits the organisation's identity and access model. Strong identity controls remain the first line of defence.

#	Assessment question	Evidence to review	Status / action
1	Is multifactor authentication enforced for all users, with stronger protection for administrators?	Entra ID policies; authentication methods	Not reviewed Gap Partial Met N/A
2	Are Conditional Access policies appropriate for Copilot users, devices and locations?	Conditional Access export; sign-in logs	Not reviewed Gap Partial Met N/A
3	Are privileged roles limited, reviewed and protected through least privilege or privileged identity management?	Role assignments; PIM records; access reviews	Not reviewed Gap Partial Met N/A
4	Are emergency access accounts controlled, tested and excluded only where necessary?	Break-glass procedure; test evidence	Not reviewed Gap Partial Met N/A
5	Are joiner, mover and leaver processes removing Copilot licences and access promptly?	JML workflow; sample user records	Not reviewed Gap Partial Met N/A
6	Are guest accounts and external collaboration settings reviewed regularly?	Guest inventory; access reviews; B2B settings	Not reviewed Gap Partial Met N/A

5 | SHAREPOINT, TEAMS, ONEDRIVE AND OVERSHARING

Copilot respects existing permissions, which makes historic oversharing one of the most important areas to assess.

#	Assessment question	Evidence to review	Status / action
1	Are sites, teams and libraries with broad access such as Everyone or organisation-wide membership identified?	Sharing reports; site permissions; team membership	Not reviewed Gap Partial Met N/A
2	Are anonymous or open sharing links controlled and reviewed?	SharePoint sharing settings; link reports	Not reviewed Gap Partial Met N/A
3	Are inactive, ownerless or obsolete sites and teams identified for closure or remediation?	Site inventory; ownership report; activity data	Not reviewed Gap Partial Met N/A
4	Are highly sensitive repositories excluded, restricted or otherwise protected where necessary?	Restricted access settings; label controls; site policies	Not reviewed Gap Partial Met N/A
5	Are users prevented from creating uncontrolled sharing structures without suitable governance?	Site creation settings; group governance; lifecycle policy	Not reviewed Gap Partial Met N/A
6	Is there a process to remediate oversharing without disrupting legitimate collaboration?	Remediation runbook; owner communication; test plan	Not reviewed Gap Partial Met N/A
7	Are OneDrive external sharing and former-employee data handling controlled?	OneDrive settings; retention and ownership transfer process	Not reviewed Gap Partial Met N/A

6 | SENSITIVITY LABELS AND INFORMATION PROTECTION

Sensitivity labels help employees and systems recognise important information and apply appropriate protection.

#	Assessment question	Evidence to review	Status / action
1	Is there a clear sensitivity label structure that employees understand?	Label catalogue; user guidance	Not reviewed Gap Partial Met N/A
2	Are labels published to the correct users and locations?	Label policies; publication scope	Not reviewed Gap Partial Met N/A
3	Do labels apply encryption, access restrictions or markings where appropriate?	Label configuration; sample protected files	Not reviewed Gap Partial Met N/A
4	Are priority SharePoint sites, Teams and Microsoft 365 groups labelled appropriately?	Container labels; site inventory	Not reviewed Gap Partial Met N/A
5	Are default, recommended or automatic labelling options used where the licence and risk justify them?	Auto-labelling policies; simulation results	Not reviewed Gap Partial Met N/A
6	Have the effects of encrypted content and user-defined permissions on Copilot been tested?	Test cases; sample outputs; access matrix	Not reviewed Gap Partial Met N/A
7	Are label changes and exceptions monitored and periodically reviewed?	Audit records; exception register	Not reviewed Gap Partial Met N/A

7 | DATA LOSS PREVENTION AND AI INTERACTIONS

DLP provides policy-based controls to identify, monitor and restrict sensitive information across Microsoft 365 and supported Copilot interactions.

#	Assessment question	Evidence to review	Status / action
1	Do DLP policies cover the sensitive information types relevant to the organisation?	DLP policy inventory; regulatory mapping	Not reviewed Gap Partial Met N/A
2	Has the Microsoft 365 Copilot and Copilot Chat policy location been assessed where available?	Purview DLP configuration; licensing	Not reviewed Gap Partial Met N/A
3	Are there controls to restrict Copilot processing of content with selected sensitivity labels where required?	DLP conditions and actions; test evidence	Not reviewed Gap Partial Met N/A
4	Are prompt and response risks included in the organisation's DLP design and incident process?	Policy scope; alert workflow; playbook	Not reviewed Gap Partial Met N/A
5	Are policies tested in simulation or audit mode before broad enforcement?	Simulation results; change approvals	Not reviewed Gap Partial Met N/A
6	Are DLP alerts assigned to owners with clear investigation and escalation procedures?	Alert queue; SOC/service desk workflow	Not reviewed Gap Partial Met N/A
7	Are endpoint and browser controls aligned with the wider risk of employees moving data to unapproved AI services?	Endpoint DLP; browser controls; cloud app policies	Not reviewed Gap Partial Met N/A

8 | AUDIT, RETENTION, COMPLIANCE AND INCIDENT RESPONSE

Audit, retention and incident processes provide evidence, accountability and a route to investigate problems.

#	Assessment question	Evidence to review	Status / action
1	Are Copilot interactions included in the organisation's audit and compliance operating model?	Purview Audit settings; role access	Not reviewed Gap Partial Met N/A
2	Are retention requirements for Copilot interaction data understood and configured where necessary?	Retention policies; legal requirements	Not reviewed Gap Partial Met N/A
3	Can the security or compliance team investigate a reported Copilot data incident?	Investigation procedure; audit search test	Not reviewed Gap Partial Met N/A
4	Are eDiscovery and legal hold requirements understood for AI-generated or AI-assisted content?	eDiscovery process; legal guidance	Not reviewed Gap Partial Met N/A
5	Are insider risk, communication compliance or other advanced controls assessed where proportionate?	Purview solution review; risk assessment	Not reviewed Gap Partial Met N/A
6	Does the incident response plan include incorrect disclosure, harmful output and misuse of AI?	Incident plan; tabletop exercise	Not reviewed Gap Partial Met N/A
7	Are privacy notices, acceptable-use policies and records of processing updated where required?	Policy set; DPIA/AI impact assessment	Not reviewed Gap Partial Met N/A

9 | COPILOT AGENTS, CONNECTORS AND EXTENSIONS

Agents and connectors can extend Copilot to more data and actions, so they require explicit ownership and proportionate controls.

#	Assessment question	Evidence to review	Status / action
1	Is there an inventory of Copilot agents, plugins, connectors and custom AI solutions?	Agent catalogue; app inventory	Not reviewed Gap Partial Met N/A
2	Is there an approval process before an agent can access business data or perform actions?	Design authority; approval workflow	Not reviewed Gap Partial Met N/A
3	Are agent permissions limited to the minimum data and actions required?	Connection settings; service accounts; scopes	Not reviewed Gap Partial Met N/A
4	Are maker and publisher permissions controlled for Copilot Studio and related platforms?	Environment roles; DLP policies; tenant settings	Not reviewed Gap Partial Met N/A
5	Are third-party data handling, security and contractual terms reviewed?	Supplier assessment; DPA; security evidence	Not reviewed Gap Partial Met N/A
6	Are inactive, duplicate or unowned agents removed or reassigned?	Usage records; ownership register	Not reviewed Gap Partial Met N/A
7	Can agent activity be monitored, investigated and disabled quickly if needed?	Logging; support process; emergency controls	Not reviewed Gap Partial Met N/A

10 | ADOPTION, USAGE, TRAINING AND SUPPORT

A secure deployment still needs active adoption, training and support to create measurable business value.

#	Assessment question	Evidence to review	Status / action
1	Is Copilot usage measured through the available Microsoft 365 reports and agreed business metrics?	Usage reports; dashboard; KPI definition	Not reviewed Gap Partial Met N/A
2	Are inactive licensed users identified for support, reassignment or licence optimisation?	Active-user data; last activity; licence list	Not reviewed Gap Partial Met N/A
3	Have priority teams received role-relevant training rather than generic demonstrations only?	Training records; role curriculum	Not reviewed Gap Partial Met N/A
4	Do users understand what information they may enter and how to check AI-generated content?	Acceptable-use policy; awareness assessment	Not reviewed Gap Partial Met N/A
5	Are AI champions, service desk teams and escalation routes in place?	Champion network; knowledge articles; support model	Not reviewed Gap Partial Met N/A
6	Are valuable use cases documented and shared across the organisation?	Use-case library; internal communications	Not reviewed Gap Partial Met N/A
7	Are benefits such as time saved, quality, response times or employee experience being measured?	Baseline and outcome measures; feedback surveys	Not reviewed Gap Partial Met N/A

From discovery to an agreed remediation plan

A standard Copilot Health Check is normally completed within ten working days. The exact timetable depends on tenant size, access to the required portals, stakeholder availability and the volume of permissions or information protection issues discovered. Significant data clean-up may require a separate remediation phase.

Timing	Stage	What happens
Day 1	**Kick-off and scope**	Confirm objectives, licences, stakeholders, access, business priorities and known concerns.
Days 2-3	**Configuration evidence**	Collect tenant, identity, sharing, label, DLP, audit, agent and usage evidence.
Days 4-5	**Security analysis**	Review permissions, oversharing, privileged access and high-risk information repositories.
Days 6-7	**Governance and adoption**	Assess policies, reporting, training, support, ownership and licence utilisation.
Day 8	**Validation**	Test key findings with technical owners and distinguish genuine risk from approved exceptions.
Day 9	**Remediation design**	Define priority actions, dependencies, owners, expected effort and quick wins.
Day 10	**Readout and handover**	Present the risk position, agree the roadmap and hand over the evidence pack and action plan.

Typical deliverables

- Executive summary with the overall risk rating and key decisions required.
- Detailed findings register with evidence, affected services and risk priority.
- Remediation roadmap separating immediate containment, short-term fixes and longer-term improvement.
- Configuration and governance recommendations aligned to the organisation's Microsoft 365 licensing.
- Licence and adoption baseline with recommendations for training, support and optimisation.
- Management presentation and technical handover session.

> **Important scope note**
>
> The health check identifies and prioritises issues. Priority configuration fixes can often be implemented during the two-week window when authorised, but extensive SharePoint permissions restructuring, data classification or policy redesign may require a separately agreed remediation workstream.

Information to prepare before the health check

Evidence area	What to provide
Copilot licences and user list	List of licensed users, pilot groups and expected business roles.
Administrative access	Read-only or approved review access to relevant Microsoft 365, Entra and Purview portals.
Information protection	Current sensitivity label and DLP policies, including any exceptions.
Collaboration estate	SharePoint, Teams and OneDrive inventory, ownership and sharing reports where available.
Governance documents	AI policy, acceptable-use policy, data classification policy and incident procedures.
Adoption evidence	Usage reports, training records, employee feedback and known support issues.
Agents and integrations	Inventory of Copilot agents, Copilot Studio solutions, plugins and connected data sources.

Rapid self-assessment

Answer the following before the formal review. Three or more “No” answers normally indicate that a structured health check would be valuable.

#	Statement	Yes	No
1	We can identify every person with a Copilot licence and explain why they have it.	[ ]	[ ]
2	We know which SharePoint and Teams locations are broadly shared across the organisation.	[ ]	[ ]
3	Our sensitivity labels are in active use and are understood by employees.	[ ]	[ ]
4	Our DLP design has been reviewed for AI and Copilot interactions.	[ ]	[ ]
5	We can investigate a Copilot-related data or security incident.	[ ]	[ ]
6	We have an approval and ownership process for Copilot agents and connectors.	[ ]	[ ]
7	Users have received practical training on secure and responsible AI use.	[ ]	[ ]
8	We measure adoption and can identify unused or underused licences.	[ ]	[ ]

Start with a Copilot Health Check

Where Copilot is already live, the most useful next step is to establish a verified baseline. PSTG reviews the tenant configuration, permissions, sensitivity labels, DLP, audit controls, connected agents and adoption position. We then translate technical findings into a prioritised remediation plan that leadership and technical teams can act on.

> **A practical outcome in two weeks**
>
> You receive a clear view of the current position, urgent risks, quick wins and the longer-term actions needed to operate Copilot securely and achieve stronger adoption.

Discuss your Copilot environment

Contact PSTG to arrange an initial scoping session and confirm the tenant access, stakeholders and evidence required for the review.

Official Microsoft guidance used in this checklist

Data, Privacy, and Security for Microsoft 365 Copilot: https://learn.microsoft.com/microsoft-365/copilot/microsoft-365-copilot-privacy

Microsoft 365 Copilot data protection architecture: https://learn.microsoft.com/microsoft-365/copilot/microsoft-365-copilot-architecture-data-protection-auditing

Secure and govern Microsoft 365 Copilot: foundational deployment guidance: https://learn.microsoft.com/microsoft-365/copilot/secure-govern-copilot-foundational-deployment-guidance

Configure a secure and governed data foundation for Microsoft 365 Copilot: https://learn.microsoft.com/microsoft-365/copilot/configure-secure-governed-data-foundation-microsoft-365-copilot

Microsoft Purview DLP for Microsoft 365 Copilot and Copilot Chat: https://learn.microsoft.com/purview/dlp-microsoft365-copilot-location-learn-about

Microsoft 365 Copilot usage and readiness reports: https://learn.microsoft.com/microsoft-365/admin/activity-reports/microsoft-365-copilot-usage

This checklist is general guidance and is not a substitute for legal, regulatory or data protection advice. Microsoft licensing and product capabilities change over time; final recommendations should be validated against the tenant licences and current Microsoft documentation.