MICROSOFT 365 / AGENT GOVERNANCE

Secure your agents. Start with these 10 checks.

Know what is running. Know who owns it. Check what it can do.

ORGANISATION / TENANT

REVIEWED BY

REVIEW DATE

NEXT REVIEW

CHECK		ADMIN ACTION	ACTION REF
☐	01	Assign a named owner to every agent	
☐	02	Check Shadow AI for unapproved installations	
☐	03	Keep one inventory of approved agents	
☐	04	Restrict who can build, publish and share	
☐	05	Verify sign-in and the identity behind every tool	
☐	06	Check the data the agent can reach	
☐	07	Approve tools, connectors and MCP servers	
☐	08	Put approval before consequential actions	
☐	09	Review activity and make someone responsible for alerts	
☐	10	Prove you can stop and retire an agent	

Check an item only when you have evidence. For gaps, record an action owner and due date. For **not applicable**, record why. Use pages 2-5 for the how-to and completion tests.

Start before production rollout, then repeat during regular reviews. These checks reduce risk; they do not certify that an environment is secure.

Availability, licensing and preview requirements vary. See page 6 before planning changes. Microsoft references checked 10 November 2026.

CHECKS 01-03 / DISCOVERY AND OWNERSHIP

Find it. Name an owner.

Verify individual records and source platforms. Keep a current inventory.

01 Assign a named owner to every agent

How to: Open each production agent's record in its source platform and, where available, the Microsoft 365 Agent Registry. Confirm a named person accepts responsibility for its purpose, access and support. Verify the person is still active; record a backup contact. Use the platform's ownership controls where supported and keep an accountable business owner in your inventory.

Complete when: Every production agent has a verified, reachable owner and a backup contact. Recheck ownership when staff leave or change roles.

REFERENCES [1] / [2]

☐ CHECKED ☐ NEEDS ACTION ☐ N/A EVIDENCE / ACTION REF

02 Check Shadow AI for unapproved installations

How to: Where available, open Microsoft 365 admin center > Agents > Shadow AI. Review detected apps, devices and last-seen details against your approved-software list. Ask the user what the app does and what data it handles. Investigate unapproved use and apply your endpoint-management process. Detection alone doesn't prove a policy violation; blocking support varies by app. If the page is unavailable, use your endpoint inventory and software review process.

Complete when: Each detection has a decision: approved, investigate or remediate. Record device-coverage gaps; "not detected" isn't proof of absence.

REFERENCES [3]

☐ CHECKED ☐ NEEDS ACTION ☐ N/A EVIDENCE / ACTION REF

03 Keep one inventory of approved agents

How to: Reconcile the Microsoft 365 registry with Copilot Studio environments, SharePoint agents and other platforms your teams use. Record the agent ID, platform, environment, purpose, owner, audience, data sources, tools and approval status. Check source-platform records rather than assuming registry coverage or synchronization is complete.

Complete when: Every discovered agent has a current record and an approved purpose, or a named person investigating it.

REFERENCES [1] / [4]

☐ CHECKED ☐ NEEDS ACTION ☐ N/A EVIDENCE / ACTION REF

CHECKS 04-06 / ACCESS AND DATA

Check who gets access.

Review users, makers, connections and the data behind the agent.

04 Restrict who can build, publish and share

How to: Review maker and administrator roles, production-environment access, agent co-authors, shared users/groups and published channels. Remove access that isn't needed. Use the relevant Microsoft 365 and Power Platform controls to limit deployment and channels. Give public or external sharing an explicit approval decision.

Complete when: An approved user can access the agent, while an unapproved user cannot. Test every published channel and review who can change the agent.

REFERENCES [2] / [5] / [6]

☐ CHECKED ☐ NEEDS ACTION ☐ N/A EVIDENCE / ACTION REF

05 Verify sign-in and the identity behind every tool

How to: Require authentication for internal agents. In Copilot Studio, check Settings > Security > Authentication, then inspect each tool's connection and permissions. Prefer user authentication for work on a user's behalf; review maker-provided credentials carefully. For unattended work, document a supported identity with narrowly scoped access. Protect human admin and maker accounts with MFA; workload identities need their own supported controls.

Complete when: You know whose permissions each action uses. Limited-access users cannot retrieve data or trigger actions outside their approved access.

REFERENCES [6] / [7] / [14] / [15]

☐ CHECKED ☐ NEEDS ACTION ☐ N/A EVIDENCE / ACTION REF

06 Check the data the agent can reach

How to: Review knowledge sources and the underlying SharePoint, OneDrive and business-system permissions. Remove unnecessary broad access and sharing links. Apply sensitivity labels and data loss prevention policies where supported. Test with an ordinary user and a user who should be denied access, using harmless test data.

Complete when: The agent retrieves only the information approved for that user or workload. Restricted test content stays inaccessible.

REFERENCES [8] / [9]

☐ CHECKED ☐ NEEDS ACTION ☐ N/A EVIDENCE / ACTION REF

CHECKS 07-08 / TOOLS AND ACTIONS

Control what it can do.

Approve the integrations. Test the boundary before consequential actions.

07 Approve tools, connectors and MCP servers

How to: List each tool, connector, Model Context Protocol (MCP) server and external endpoint. Check the publisher, requested permissions, read/write capabilities and destination for company data. Remove unnecessary tools. Use Power Platform data policies and supported endpoint restrictions. Microsoft 365's Power Platform connector view provides visibility; connector policy changes are made in Power Platform.

Complete when: Every enabled tool has an approved purpose, identity and data boundary. A harmless test confirms prohibited connections are blocked.

REFERENCES [6] / [10]

☐ CHECKED ☐ NEEDS ACTION ☐ N/A EVIDENCE / ACTION REF

08 Put approval before consequential actions

How to: Identify actions that send messages, change records, delete files, grant access or spend money. Require human approval through an enforced workflow or tool control before actions that need it. Don't rely on an instruction saying "ask first." Test rejection, missing approval, repeat requests and malicious instructions hidden in sample documents or tool results.

Complete when: The protected action cannot execute without the required approval, and rejected or repeated requests don't cause unintended changes.

REFERENCES [11] / [12]

☐ CHECKED ☐ NEEDS ACTION ☐ N/A EVIDENCE / ACTION REF

TOOL / CONNECTOR / MCP SERVER TO REVIEW - PERMISSION AND DESTINATION

APPROVAL TEST - ACTION, APPROVER, REJECTION RESULT AND EVIDENCE

Use harmless test data. The completion tests above describe what to verify; they are not results of tests performed on your environment.

CHECKS 09-10 / MONITORING AND RETIREMENT

Watch it. Be ready to stop.

Assign the alert contact and prove the stop procedure works.

09 Review activity and make someone responsible for alerts

How to: Use the agent's analytics and available Microsoft Purview, Defender or platform-native logs to review changes, tool use, failures, unexpected access and unusual usage. Verify what your licences and logging settings actually capture. Protect transcript access and set appropriate retention. Assign an alert contact and send a harmless test event through the investigation process.

Complete when: You can find the test event, identify the agent and responsible owner, and show who will investigate it.

REFERENCES [5] / [13]

☐ CHECKED ☐ NEEDS ACTION ☐ N/A EVIDENCE / ACTION REF

10 Prove you can stop and retire an agent

How to: Document the platform-specific steps to block access or unpublish the agent, stop triggers and revoke dedicated connections or permissions. Check dependencies before changing shared identities. Test stopping a non-production copy, including background work and external integrations. Retire unused agents, remove residual access and preserve required records.

Complete when: A named admin can stop user access and unattended execution. Record the last test, any propagation delay and the next review date.

REFERENCES [2] / [4] / [11]

☐ CHECKED ☐ NEEDS ACTION ☐ N/A EVIDENCE / ACTION REF

ACTION REGISTER / COPY THIS SECTION FOR MORE GAPS

REF	GAP / NEXT ACTION	OWNER	DUE	EVIDENCE

Suggested cadence: discovery and alerts weekly; ownership, sharing and tools monthly. Repeat access and stop tests before rollout and after material changes. Increase frequency for sensitive data or consequential actions.

This cadence is an Automate Already recommendation, not a Microsoft-mandated schedule.

MICROSOFT REFERENCE CHECK / 10 NOVEMBER 2026

Check the exact controls.

Use current documentation, then verify behaviour in your own environment.

Before you start: menu names, licensing, roles and preview access vary. Microsoft currently documents the Shadow AI page as a Frontier preview requiring Microsoft 365 E5, Defender for Endpoint and Intune-enrolled managed Windows devices. Global Secure Access supplies additional usage metadata. Confirm current prerequisites; other checks can still be performed in the relevant source platform. [3]

OFFICIAL MICROSOFT REFERENCES

[1] Agent Registry

[2] Agent governance and lifecycle actions

[3] Shadow AI prerequisites, detection and blocking limitations

[4] Connected platforms and synchronization limitations

[5] Copilot Studio security and governance

[6] Copilot Studio data policies

[7] Tool authentication and connection identity

[8] SharePoint knowledge-source permission behaviour

[9] Prepare SharePoint permissions for Copilot and agents

[10] Tools page: MCP controls and connector visibility

[11] Autonomous-agent design and oversight

[12] Tool approval and untrusted inputs

[13] Microsoft Purview for Copilot Studio

[14] MFA for human user sign-ins

[15] Maker credentials and impact on autonomous agents

Documentation supports the listed controls, not a completed tenant assessment. No client environment, permissions or agent configuration was tested for this pack. Recheck after product or configuration changes.

Need help working through the list? We help teams review Microsoft 365 agents and put practical controls in place.

automatealready.ca / hello@automatealready.ca

Production, not promises.