SimplicityIT

Free technical checklist

Microsoft 365 AI Security and Governance Checklist

The identity, data and governance controls to verify in your tenant before Copilot and agents are switched on.

Copilot and Microsoft 365 agents inherit the permissions and the data hygiene that already exist in a tenant. Where sharing is loose or labelling is absent, an assistant that can search everything a user can reach will surface that fact quickly and at scale. This checklist walks twelve control areas, each item stating what to verify, why it matters for AI specifically, and where to check it, with a Microsoft Learn reference for every technical assertion.

Version 1.0. Published 24 August 2026.
Prepared for IT managers, security leads and Microsoft 365 administrators preparing a tenant for Microsoft 365 Copilot, Copilot Studio agents, or any assistant that reads organizational content.
simplicityitinc.com

Contents

How to use this checklist

Work through it in order. The domains are sequenced so that each one assumes the previous ones are done, and the identity work at the front is what everything after it depends on. A sensitivity label protects nothing from someone signed in as a person entitled to read the content.

Each item states what to verify, why it matters specifically for AI, and where to look. Record an owner, a status and a date against each one. The items that must be closed before Copilot is enabled are collected into a single gate near the back, so a deployment decision does not require rereading the whole document.

Items marked Product describe behaviour Microsoft documents, and cite the article. Items marked Practice are Simplicity IT delivery judgement. Both are worth doing. Only the first carries Microsoft as its authority.

What this checklist does not do

- It does not make an organization compliant. Compliance depends on the regulation, the scope, the evidence and an assessor. This is preparation. No audit outcome is promised or implied.
- It is not a penetration test or a threat model. It verifies configuration and governance, which is a different question from whether a determined attacker gets in.
- It is not exhaustive for every tenant. A regulated organization, a multitenant estate or a tenant with heavy third party integration will have material items that are not here.
- It does not replace Microsoft documentation. Where an item cites an article, read the article before acting. Product behaviour changes, and the verification date on each source tells you how fresh our reading of it is.

SECTION 1

Domain 1. Microsoft Entra ID foundations

The identity baseline. Every later control assumes this one holds.

ID-1 **Item 1**

Multifactor authentication is enforced for all users, including administrators and accounts used by services.

WHY IT MATTERS	An assistant that can read organizational content turns one compromised account into a fast, well indexed search across everything that account could reach.
HOW TO VERIFY	Entra admin center, review Conditional Access policies and the users excluded from them. Confirm no standing exclusions remain from a migration.

Sources 2, 7

ID-2 Item 2

Legacy authentication protocols are blocked.

WHY IT MATTERS	Legacy protocols do not support multifactor authentication, so leaving them enabled leaves a path around every policy in the next domain.
HOW TO VERIFY	Entra sign in logs filtered to legacy client apps, then a Conditional Access policy blocking them. Check the logs first, because the block is the easy part and the applications still using it are not.

Source 5

ID-3 Item 3

Administrators use phishing-resistant multifactor authentication.

WHY IT MATTERS	Administrative accounts can grant an application access to organizational content across the tenant. That is the grant an attacker wants, and code or push based factors can be relayed.
HOW TO VERIFY	Conditional Access policy targeting administrative roles with an authentication strength requiring phishing-resistant methods.

Source 6

ID-4 Item 4

The tenant has moved beyond security defaults to explicit Conditional Access policy, or has made a deliberate decision to stay on security defaults.

WHY IT MATTERS	Security defaults and Conditional Access cannot both be enabled. Tenants often disable defaults during a project and never replace them with equivalent policy.
HOW TO VERIFY	Entra properties for the security defaults state, then confirm the policies that replaced them actually cover the same population.

Sources 4, 13

ID-5 Item 5

Guest and external identities in the tenant have been reviewed against a current list of who should have them.

WHY IT MATTERS	Guests accumulate. A guest with access to a site is a guest whose queries a content aware assistant may answer from that site.
HOW TO VERIFY	Entra external identities, list guest accounts by last sign in date, and reconcile against the projects that created them.

Source 11

ID-6 Item 6

Joiner, mover and leaver processes actually remove access, and someone has tested that they do.

WHY IT MATTERS	Every later control assumes the account list reflects the staff list. Movers are the usual failure: access accumulates across roles and is never withdrawn.
HOW TO VERIFY	Pick five people who changed role in the last year and check what they can still reach.

SECTION 2

Domain 2. Conditional Access

The conditions under which access is granted, beyond a correct password.

CA-1 Item 7

A baseline set of Conditional Access policies is deployed and each one has a stated purpose.

WHY IT MATTERS	Policies accumulate across projects until nobody can say what the combined effect is, which means nobody can say what an assistant running in a user context is permitted to do.
HOW TO VERIFY	List every policy with its target, its condition and its control. Compare against the common policy set Microsoft publishes.

Sources 1, 3

CA-2 Item 8

Access to organizational content requires a compliant or a hybrid joined device where the data sensitivity warrants it.

WHY IT MATTERS	Content an assistant surfaces is content that lands on the device that asked for it. Device state is what determines whether that is acceptable.
HOW TO VERIFY	Conditional Access grant controls for the applications in scope, cross referenced with Intune compliance policy.

Source 3

CA-3 Item 9

Continuous access evaluation is in effect for supported services.

WHY IT MATTERS	Without it, revoking access waits for a token to expire. With an assistant able to retrieve content quickly, the length of that window matters more than it used to.
HOW TO VERIFY	Confirm the services in scope support it and that no policy or configuration is suppressing it.

Source 10

CA-4 Item 10

Every Conditional Access exclusion has a named owner and a review date.

WHY IT MATTERS	Exclusions are added under delivery pressure and removed almost never. The excluded accounts are frequently the privileged ones.
HOW TO VERIFY	Export the exclusions from every policy into one list. It is usually longer than the person maintaining the policies expects.

CA-5 Item 11

Policy changes are reported through a monitored channel to someone who did not make them.

WHY IT MATTERS	A weakened access policy is a quiet change with a large effect, and it looks identical to a legitimate one in the audit log unless a second person is reading it.
HOW TO VERIFY	Confirm an alert exists on Conditional Access policy modification and that a person receives it.

SECTION 3

Domain 3. Least privilege and privileged access

Who holds standing power in the tenant, and for how long at a time.

LP-1 Item 12

Global Administrator assignments are counted, justified and few.

WHY IT MATTERS	Microsoft recommends a small number of Global Administrators with role specific roles used in preference. Every one of them can consent to an application reading organizational content tenant wide.
HOW TO VERIFY	Entra roles and administrators. Count the standing Global Administrator assignments and name a reason for each.

Source 9

LP-2 Item 13

Privileged roles are activated on request and for a limited time rather than held permanently.

WHY IT MATTERS	Standing privilege is available to anyone who compromises the account at any moment. Time bound activation reduces that to the moments it is in use, and produces a record of why.
HOW TO VERIFY	Privileged Identity Management, review which roles are eligible against which are permanently assigned.

Source 8

LP-3 Item 14

Administrative accounts are separate from the accounts those people use for daily work and email.

WHY IT MATTERS	An administrator who reads email on the privileged account has joined the highest privilege in the tenant to its most commonly attacked surface.
HOW TO VERIFY	Check whether privileged accounts are licensed for mailboxes and whether they appear in sign in logs against ordinary productivity applications.

Source 9

LP-4 Item 15

Application permissions and consent grants have been reviewed, particularly any granting broad access to organizational content.

WHY IT MATTERS	An application with tenant wide content permissions reads content on its own authority rather than the user's, which means user level access controls do not constrain it.
HOW TO VERIFY	Enterprise applications, review permissions granted, prioritising anything with tenant wide read across mail, files or sites.

Source 9

LP-5 Item 16

Elevated access to content, as distinct from elevated access to configuration, is time bound and approved.

WHY IT MATTERS	Administrative roles that can reach content are a different risk from those that change settings, and are often overlooked because the role names sound operational.
HOW TO VERIFY	Review privileged access management configuration for the tasks that expose content.

Source 12

LP-6 Item 17

At least two emergency access accounts exist, are excluded from Conditional Access deliberately, and are monitored.

WHY IT MATTERS	Tightening identity policy is how organizations lock themselves out of their own tenant. The accounts that prevent that are also the accounts an attacker most wants.
HOW TO VERIFY	Confirm the accounts exist, that their credentials are held securely offline, and that any sign in raises an alert.

SECTION 4

Domain 4. Microsoft Purview foundations

Knowing what data you hold before deciding how to protect it. This domain is where most tenants discover the work is larger than expected.

PV-1 Item 18

Someone owns data governance, and the Purview roles reflect that ownership.

WHY IT MATTERS	Purview spans security, compliance, records and IT. Without an owner, labels get created and never applied, and the resulting scheme is worse than none because it implies protection that is absent.
HOW TO VERIFY	Purview portal permissions, confirm named role holders rather than a shared administrative account.

Source 14

PV-2 Item 19

Sensitive information types relevant to your business are configured, not just the built in defaults.

WHY IT MATTERS	The default types cover common regulated identifiers. They do not know your contract numbers, your client reference format or your project code names, which is where your actual confidential material is.
HOW TO VERIFY	Purview data classification, review sensitive information types and confirm which are custom.

Source 22

PV-3 Item 20

Trainable classifiers have been considered for categories that pattern matching cannot catch.

WHY IT MATTERS	Some categories, source code, legal agreements, sensitive discussions, are recognisable by their character rather than by any string a pattern can match.
HOW TO VERIFY	Purview data classification, review trainable classifiers available and in use.

Source 23

PV-4 Item 21

Content explorer has been used to look at what is actually there, and someone has read the result.

WHY IT MATTERS	This is the step that converts assumptions about data holdings into a number. It is routinely the point at which an AI programme is repriced.
HOW TO VERIFY	Purview content explorer, review by sensitive information type and by location.

Source 24

PV-5 Item 22

Data Security Posture Management for AI has been reviewed if it is available to you.

WHY IT MATTERS	It reports on how AI applications in the tenant are interacting with sensitive data, which is otherwise difficult to see.
HOW TO VERIFY	Purview portal, review Data Security Posture Management and confirm licensing covers it.

Source 25

SECTION 5

Domain 5. Information protection

Sensitivity labels, and whether the protection travels with the content.

IP-1 Item 23

A sensitivity label taxonomy exists, is small enough to be used correctly, and has been agreed with the business.

WHY IT MATTERS	A label scheme with fifteen options gets applied at random. Labelling is a judgement staff make many times a day, and it has to be a judgement they can make quickly.
HOW TO VERIFY	Purview information protection, review the published label set and its scope.

Sources 17, 18

IP-2 Item 24

Labels apply encryption and usage rights where the classification warrants it, not just a visual marking.

WHY IT MATTERS	A header saying Confidential constrains nobody. Protection that travels with the file is what still applies after the file has left.
HOW TO VERIFY	Review each label configuration for encryption and rights settings.

Source 15

IP-3 Item 25

Automatic and recommended labelling is in use, so protection does not depend entirely on user diligence.

WHY IT MATTERS	Manual labelling covers new content created by attentive people. It does not cover the existing estate, which is where the sensitive material already is.
HOW TO VERIFY	Review auto labelling policies for both client side and service side application, and confirm they have been run against existing content.

Source 16

IP-4 Item 26

Labels are applied to containers, not only to files.

WHY IT MATTERS	A site or team labelled correctly constrains what can be created in it and who can be added. File level labelling alone leaves the container open.
HOW TO VERIFY	Confirm labels are scoped to groups and sites, and that new site creation applies one.

Source 17

IP-5 Item 27

Someone has checked what proportion of content in the locations in scope actually carries a label.

WHY IT MATTERS	A deployed scheme and an applied scheme are different things, and the gap between them is the part that is unprotected.
HOW TO VERIFY	Content explorer, review label coverage by location rather than tenant wide.

Source 24

IP-6 Item 28

Content protected by older rights management technology has been identified.

WHY IT MATTERS	Documents protected with legacy information rights management are not used for grounding, so a body of important content can be silently invisible to an assistant while appearing to be in scope.
HOW TO VERIFY	Identify content protected outside current Purview labelling, particularly older document libraries and archives.

Source 27

SECTION 6

Domain 6. Data loss prevention

Stopping sensitive content leaving by the routes it usually leaves by, including the new ones.

DL-1 Item 29

Data loss prevention policies exist for the locations in scope and are in enforcement rather than test mode.

WHY IT MATTERS	Policies left in simulation generate reports that look like protection. Nobody notices because the reports arrive either way.
HOW TO VERIFY	Purview data loss prevention, check the mode of every policy, not just its existence.

Source 19

DL-2 Item 30

Policies cover endpoints and browsers as well as email and files.

WHY IT MATTERS	Content leaves by upload and by paste at least as often as by attachment, and pasting into a web based assistant is now one of those routes.
HOW TO VERIFY	Review endpoint data loss prevention configuration and which devices are onboarded.

Source 19

DL-3 Item 31

The Microsoft 365 Copilot data loss prevention location is configured if it is available to you.

WHY IT MATTERS	It is the control that keeps labelled content out of Copilot responses, which is a different question from who can open the file.
HOW TO VERIFY	Purview data loss prevention, review the Copilot location and the labels it excludes.

Source 26

DL-4 Item 32

Policy tips are enabled so users are told at the moment they would otherwise make the mistake.

WHY IT MATTERS	A block with no explanation gets worked around. A tip at the point of action is the only user education that reliably lands.
HOW TO VERIFY	Confirm policy tips are enabled and that the text is comprehensible to someone who is not in IT.

Source 19

DL-5 Item 33

Someone reviews data loss prevention alerts on a schedule and can say what last month showed.

WHY IT MATTERS	Unread alerts are equivalent to no alerts, except that they create a record showing the organization was told.
HOW TO VERIFY	Ask for the last review. If it cannot be produced, the control is reporting into a void.

SECTION 7

Domain 7. Retention and lifecycle

Keeping what must be kept and disposing of what should not be there. Content you no longer need is content an assistant can still find.

RT-1 **Item 34**

Retention policies exist for the major workloads and reflect an actual retention schedule.

WHY IT MATTERS Without disposal, every mistake and every superseded draft stays indefinitely and remains discoverable, including by an assistant summarising a topic.

HOW TO VERIFY Purview data lifecycle management, review policies by workload against the organization's retention schedule.

Sources 20, 21

RT-2 **Item 35**

Retention labels are applied to records that require them, and disposal review is configured where needed.

WHY IT MATTERS Policies act on locations, labels act on items. Records obligations usually need the second.

HOW TO VERIFY Review retention labels, their publication and their auto apply rules.

Source 20

RT-3 **Item 36**

Legal holds in force are known, listed, and reviewed for whether they still need to be.

WHY IT MATTERS Holds prevent deletion and can prevent migration. They also outlive the matters that created them, and nobody notices because nothing visibly breaks.

HOW TO VERIFY Purview eDiscovery, list holds with the matter and the date each was placed.

Source 20

RT-4 **Item 37**

Inactive sites, teams and mailboxes have been identified and dealt with.

WHY IT MATTERS Abandoned workspaces hold content nobody owns or remembers, with permissions nobody reviews. An assistant treats it as current unless something says otherwise.

HOW TO VERIFY SharePoint site lifecycle management for inactive site policy, plus a review of teams with no recent activity.

Source 36

RT-5 **Item 38**

There is a written answer to what happens to content when a person leaves.

WHY IT MATTERS Leaver content is a recurring source of both unowned sensitive material and lost business records, and the default answer is usually accidental.

HOW TO VERIFY Ask what happened to the mailbox and OneDrive of the last three leavers.

SECTION 8

Domain 8. Auditability and monitoring

Being able to answer, later, what happened. This is the domain that is cheapest to configure and impossible to retrofit.

AU-1 Item 39

Unified audit logging is on and the retention period is a deliberate decision.

WHY IT MATTERS	Investigations start weeks after the event. A retention period shorter than the time it takes to notice is a retention period that answers nothing.
HOW TO VERIFY	Purview audit, confirm logging is enabled and check the retention against your incident detection reality.

Source 32

AU-2 Item 40

Copilot and agent interactions are captured in the audit log, and someone has confirmed by looking at a record.

WHY IT MATTERS	Prompts and responses are auditable, but assuming it is on is not the same as having seen an entry. The moment to find out is not during an investigation.
HOW TO VERIFY	Generate an interaction in a test account and retrieve it from the audit log.

Sources 27, 32

AU-3 Item 41

Alerts exist for the events that would matter, and they reach a person who acts.

WHY IT MATTERS	Logging without alerting means an event is discoverable in principle and undiscovered in practice.
HOW TO VERIFY	List the configured alerts and who receives them. Confirm the recipient is a monitored destination and not a departed administrator.

AU-4 Item 42

The audit evidence a regulator or client would ask for has been identified in advance.

WHY IT MATTERS	Working out what evidence exists during an audit is how organizations discover the answer is none.
HOW TO VERIFY	Write the three questions you would most likely be asked, and produce the evidence for one of them now.

AU-5 **Item 43**

Communication compliance has been considered where the sector or the risk warrants it.

WHY IT MATTERS	Some obligations attach to what people say rather than to what they can access, and AI generated content is now part of that record.
HOW TO VERIFY	Review Purview communication compliance against the obligations identified in domain 11.

Source 14

SECTION 9

Domain 9. Copilot readiness and oversharing

The domain that determines whether switching Copilot on is uneventful. Copilot surfaces only content the signed in user already has permission to access, which is reassuring exactly to the degree that those permissions are correct.

CP-1 **Item 44**

The licensing and tenant prerequisites for Microsoft 365 Copilot are met and confirmed rather than assumed.

WHY IT MATTERS	Prerequisites change, and discovering a gap after announcing a rollout date is an avoidable and public failure.
HOW TO VERIFY	Check the current requirements article against the tenant configuration.

Sources 28, 31

CP-2 **Item 45**

Data access governance reports have been run and the sites with broad access have been remediated.

WHY IT MATTERS	These reports name the sites shared with everyone, shared anonymously, or shared widely. This is where oversharing stops being a theory and becomes a list.
HOW TO VERIFY	SharePoint admin center, run the data access governance reports and work the list.

Sources 30, 35

CP-3 Item 46

Restricted Content Discovery is applied to sites that must stay out of Copilot results.

WHY IT MATTERS	Some sites hold content that specific people legitimately need and that should not be surfaced through search or an assistant. This is the control for that case.
HOW TO VERIFY	Review Restricted Content Discovery configuration against a list of sensitive sites agreed with the business.

Source 33

CP-4 Item 47

Restricted Access Control is used where site membership itself should be constrained.

WHY IT MATTERS	It limits access to a defined group regardless of individual sharing, which is what stops a well meaning share reopening a closed site.
HOW TO VERIFY	Review Restricted Access Control policy on the sites identified as sensitive.

Source 34

CP-5 Item 48

Default external sharing settings have been reviewed at both tenant and site level.

WHY IT MATTERS	SharePoint defaults to the most permissive sharing option, so an unreviewed tenant is permissive by inheritance rather than by decision.
HOW TO VERIFY	SharePoint admin center sharing settings, tenant level then per site, particularly sites created before any review.

Source 37

CP-6 Item 49

A site lifecycle policy handles inactive sites so the estate stops growing unowned.

WHY IT MATTERS	Oversharing remediation is a one off project unless something prevents the estate regenerating the problem.
HOW TO VERIFY	Confirm inactive site policy is configured and that site owners receive and act on the attestations.

Sources 29, 36

SECTION 10

Domain 10. Agent governance

Agents differ from an assistant in one respect that matters more than any other: they act. This domain is weighted toward Simplicity IT delivery practice, and is marked accordingly.

AG-1 Item 50

There is a register of agents in the organization, including the ones built by people who are not in IT.

WHY IT MATTERS	You cannot govern what you have not enumerated, and low code platforms mean agents get created by people with no obligation to tell anyone.
HOW TO VERIFY	Review the platform admin centers for what exists, then compare against what IT believed existed.

AG-2 Item 51

Every agent has a named owner who is accountable for what it does.

WHY IT MATTERS	An unowned agent taking action in a production system has no one answerable for the action, which becomes apparent at the worst possible time.
HOW TO VERIFY	Check the register has a person, not a team, against each entry, and that the person knows.

AG-3 Item 52

Each agent runs with an identity whose permissions have been enumerated and scoped.

WHY IT MATTERS	Agents are frequently given the permissions of whoever built them, which is broader than the task and permanent.
HOW TO VERIFY	For each agent, list the connections and permissions it holds, and confirm each is needed.

Source 9

AG-4 Item 53

Agents that write, send or commit are separated from agents that only read, and are governed more tightly.

WHY IT MATTERS	A wrong answer is recoverable. A wrong action already taken in a finance or customer system is a different category of problem.
HOW TO VERIFY	Classify the register by whether each agent can change anything outside itself.

AG-5 Item 54

Agent instructions and configuration are under change control, with a record of who changed what.

WHY IT MATTERS	Instruction text is production configuration. Editing it changes system behaviour without changing any code, and without review it changes silently.
HOW TO VERIFY	Confirm changes are recorded and reviewable, and that the record includes instruction text.

AG-6 Item 55

Someone can disable any given agent quickly, and knows how.

WHY IT MATTERS	The interval between noticing an agent is behaving wrongly and stopping it is the interval in which the damage accumulates.
HOW TO VERIFY	Ask the named owner of one agent to describe how they would stop it. If the answer requires finding somebody else, the control does not exist.

SECTION 11

Domain 11. Human approval and acceptable use

Where a person decides. Every item in this domain is Simplicity IT delivery practice, because these are organizational decisions rather than product settings.

HA-1 Item 56

A written acceptable use position exists for AI, and staff have seen it.

WHY IT MATTERS	In the absence of a position, every individual forms their own, and some of those involve pasting client material into whatever tool is convenient.
HOW TO VERIFY	Ask three people outside IT what they are allowed to put into an AI tool. The consistency of the answers is the measurement.

HA-2 Item 57

For each AI supported process, the point at which a person approves the output is defined and cannot be skipped.

WHY IT MATTERS	A review step that depends on diligence is a review step that stops happening when the queue is long, which is exactly when it matters.
HOW TO VERIFY	Walk one process end to end and try to complete it without approving anything.

HA-3 Item 58

Approvers can see what the output was based on.

WHY IT MATTERS	Approval without visible sources is acceptance, and it produces a record implying a review that did not occur.
HOW TO VERIFY	Look at what the approver actually sees, in the tool, rather than at what the design document says they see.

HA-4 **Item 59**

The volume an approver is expected to handle has been calculated and is achievable.

WHY IT MATTERS	Arithmetic decides whether a human approval point is real. Items per day multiplied by minutes per item, against the hours available.
HOW TO VERIFY	Do the multiplication. Most designs have never had it done.

HA-5 **Item 60**

AI generated material is identifiable as such where the recipient would want to know.

WHY IT MATTERS	Client and regulatory expectations on disclosure are moving, and retrofitting provenance onto material already sent is not possible.
HOW TO VERIFY	Check what leaves the organization and whether anything marks its origin.

SECTION 12

Domain 12. Ongoing operations

Keeping all of the above true after the project that established it has closed.

OP-1 **Item 61**

A named person or team owns tenant security posture as continuing work, not as a project.

WHY IT MATTERS	Every control in this document decays. Configuration drifts, exclusions accumulate, and new sites are created permissively.
HOW TO VERIFY	Ask who owns it and what they did last month.

OP-2 **Item 62**

Oversharing reporting runs on a schedule rather than once before launch.

WHY IT MATTERS	The estate regenerates the problem continuously. A remediation with no recurring review is a snapshot.
HOW TO VERIFY	Confirm the data access governance reports are scheduled and that someone receives and acts on them.

Source 35

OP-3 Item 63

Microsoft roadmap and message center items affecting AI features are read by someone who can act.

WHY IT MATTERS	Features arrive enabled by default. A tenant governed only at project time will be governed to the state of a product that has since changed.
HOW TO VERIFY	Confirm a named person reads the message center and that changes reach a decision.

OP-4 Item 64

The label taxonomy and the data loss prevention rules are reviewed against how the business has changed.

WHY IT MATTERS	New products, new clients and new obligations produce new sensitive material that existing rules do not recognise.
HOW TO VERIFY	Confirm a review date exists and that the last one produced changes rather than confirmation.

OP-5 Item 65

There is an incident path specifically for AI related events, and it names who is called.

WHY IT MATTERS	An assistant surfacing content to the wrong person is neither an ordinary security incident nor an ordinary service fault, and an undefined path means improvisation.
HOW TO VERIFY	Read the incident process and check that this scenario appears in it.

OP-6 Item 66

Someone reviews whether the AI supported processes are still producing acceptable output.

WHY IT MATTERS	Quality degrades as the underlying content changes, and it degrades invisibly. Nothing raises an alert when answers become subtly worse.
HOW TO VERIFY	Confirm a sampling schedule exists with a named reviewer and a threshold for stopping.

The pre-deployment gate

If you close nothing else before enabling Copilot or a content aware agent, close these. They are the items where the cost of being wrong is immediate and visible, and where remediation after launch means unwinding something people are already using.

- ID-1 and ID-2. Multifactor authentication enforced, legacy authentication blocked.
- LP-1 and LP-4. Global Administrator count justified, and application consent grants with tenant wide content access reviewed.

- CP-2. Data access governance reports run and the broadly shared sites remediated. This is the single highest value item in the document.
- CP-5. External sharing reviewed at tenant and site level rather than left at defaults.
- IP-5. Label coverage measured in the locations in scope, so you know what proportion is actually protected.
- AU-2. An audit record for an AI interaction retrieved successfully, once, by a person.
- HA-2 and HA-4. The human approval point defined, and the volume arithmetic done.
- AG-2. Every agent has an owner who knows they own it.

Glossary

For circulating this to stakeholders who are not administrators.

Conditional Access	Rules deciding whether a sign in is allowed based on conditions beyond the password, such as the device, the location, or the risk detected in the sign in.
Sensitivity label	A classification attached to a document or a container which can also apply encryption and usage rights, so the protection travels with the content rather than staying with its location.
Data loss prevention	Rules that detect sensitive content and prevent or warn about it leaving by a particular route, such as email, an upload, or a paste into a web application.
Oversharing	Content reachable by more people than intended, usually through broad site permissions or links shared with everyone in the organization. It is present in most tenants and is not visible until something searches across it.
Grounding	Using organizational content to inform an AI response, so the answer reflects your data rather than only what the model learned in training.
Agent	Software that carries out a task, which may include taking actions in other systems rather than only producing text for a person to read.
Privileged Identity Management	A mechanism for granting administrative roles on request and for a limited period, rather than holding them permanently.
Tenant	Your organization's instance of Microsoft 365 and Microsoft Entra ID, containing your users, your data and your configuration.

Claims and their basis

Every claim this document makes about itself is listed here with what it rests on. Nothing here is a claim about your organization, a guarantee of compliance, a predicted saving, or a promised outcome.

Copilot respects existing Microsoft 365 permissions.

Microsoft documents that Microsoft 365 Copilot only surfaces content the signed in user already has permission to access. Cited to the Copilot architecture and data protection article.

Completing this checklist does not make an organization compliant.

Stated plainly in the document. Compliance depends on the regulation, the scope, the evidence and an assessor. The checklist is preparation, not attestation, and no audit outcome is promised.

Every technical item is traceable to Microsoft documentation.

Each item carries a source id resolving to a Microsoft Learn URL in the register at the back of the document, with the verification date. Items that are Simplicity IT delivery judgement rather than product behaviour are marked as such.

Sources

Every source cited in this document, numbered in the order it is first referenced. The numbers on the items above point here. Each source was checked on the verification date shown. Microsoft documentation changes, so re-check anything you are about to act on.

1. Common Conditional Access policies
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/entra/identity/conditional-access/concept-conditional-access-policy-common

2. Secure identity with Zero Trust
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/security/zero-trust/deploy/identity

3. Common Zero Trust identity and device access policies
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/security/zero-trust/zero-trust-identity-device-access-policies-common

4. Prerequisite work for implementing Zero Trust identity and device access policies
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/security/zero-trust/zero-trust-identity-device-access-policies-prerequisite

5. Block legacy authentication with Conditional Access
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/entra/identity/conditional-access/block-legacy-authentication

6. Require phishing-resistant multifactor authentication for administrators
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/entra/identity/conditional-access/policy-admin-phish-resistant-mfa

7. Mandatory multifactor authentication for Microsoft Entra admin center sign-in
Microsoft Learn. Verified 2026-08-24.

https://learn.microsoft.com/entra/identity/authentication/concept-mandatory-multifactor-authentication

8. Start using Privileged Identity Management
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/entra/id-governance/privileged-identity-management/pim-getting-started

9. Best practices for Microsoft Entra roles
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/entra/identity/role-based-access-control/best-practices

10. Continuous access evaluation
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/entra/identity/conditional-access/concept-continuous-access-evaluation

11. Configure cross-tenant access settings for B2B collaboration
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/entra/external-id/cross-tenant-access-settings-b2b-collaboration

12. Privileged Access Management in Microsoft Purview
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/privileged-access-management

13. Security defaults in Microsoft Entra ID
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/entra/fundamentals/security-defaults

14. Get started with Microsoft Purview
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/purview-where-to-start

15. Microsoft Purview Information Protection
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/information-protection

16. Deploy a Microsoft Purview Information Protection solution
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/information-protection-solution

17. Learn about sensitivity labels
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/sensitivity-labels

18. Get started with sensitivity labels
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/get-started-with-sensitivity-labels

19. Learn about data loss prevention
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/dlp-learn-about-dlp

20. Learn about retention policies and retention labels
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/retention

21. Learn about data lifecycle management
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/data-lifecycle-management

22. Learn about sensitive information types
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/sit-sensitive-information-type-learn-about

23. Learn about trainable classifiers
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/trainable-classifiers-learn-about

24. Get started with content explorer
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/data-classification-content-explorer

25. Learn about Data Security Posture Management
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/data-security-posture-management-learn-about

26. Learn about the DLP policy location for Microsoft 365 Copilot
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/dlp-microsoft365-copilot-location-learn-about

27. Microsoft Purview data security and compliance protections for Microsoft 365 Copilot
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/purview/ai-m365-copilot

28. Microsoft 365 Copilot requirements
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/copilot/microsoft-365-copilot-minimum-requirements-data-compliance

29. Get ready for Microsoft 365 Copilot with SharePoint Advanced Management
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/copilot/get-ready-copilot-sharepoint-advanced-management

30. Configure a secure and governed data foundation for Microsoft 365 Copilot
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/copilot/configure-secure-governed-data-foundation-microsoft-365-copilot

31. Set up Microsoft 365 Copilot
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/copilot/microsoft-365-copilot-setup

32. Microsoft 365 Copilot architecture, data protection and auditing
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/microsoft-365/copilot/microsoft-365-copilot-architecture-data-protection-auditing

33. Restricted Content Discovery
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/sharepoint/restricted-content-discovery

34. Restricted Access Control for SharePoint sites
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/sharepoint/restricted-access-control

35. Data access governance reports for SharePoint sites
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/sharepoint/data-access-governance-reports

36. Site lifecycle management
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/sharepoint/site-lifecycle-management

37. Turn external sharing on or off for SharePoint and OneDrive
Microsoft Learn. Verified 2026-08-24.
https://learn.microsoft.com/sharepoint/turn-external-sharing-on-or-off

About Simplicity IT

Simplicity IT Inc. is a Microsoft-focused managed services, security and implementation company. We began in 2011. We assess, implement, migrate, integrate, secure, govern and operate Microsoft cloud environments, and we design the human approval points that keep automated work accountable.

If this document was useful

Book a tenant readiness review at simplicityitinc.com/contact/

Related reading

- Zero Trust architecture and Entra ID, simplicityitinc.com/solutions/zero-trust-m365/
- Managed security and Defender deployment, simplicityitinc.com/solutions/managed-security/

Privacy

We use your details to send you this resource and occasional related guidance. We do not sell your information and you can ask us to delete it at any time by emailing hello@simplicityitinc.com.

What requesting this document does not do

Requesting a resource does not create an account, a trial, a subscription, partner status, or an engagement. It sends you a document.