Ready-Set-Go.AI

AI READINESS & MICROSOFT 365 GOVERNANCE · CONTOSO

AI Readiness & Governance Intelligence Report

An evidence-driven, read-only delegated assessment of the Contoso Microsoft 365 tenant's readiness to safely enable modern AI platforms, assembled across eleven governance domains spanning identity, application consent, data classification, external sharing, endpoint and audit.

PREPARED FOR	PREPARED BY	ENGINE	ISSUED	ASSESSMENT
Contoso	Ready-Set-Go.AI	AI Readiness v1 assembled	May 2026	Read-only delegated

DOCUMENT

Contents & Report Information

A structured walk-through of the identity, application-consent, data-governance, collaboration-exposure, endpoint and audit posture of the Contoso Microsoft 365 tenant, with prioritised remediation across eleven assessed governance domains.

REPORT INFORMATION

REPORT ID	`ai-readiness-v1-assembled`
PREPARED FOR	Contoso
PREPARED BY	Ready-Set-Go.AI
ASSESSMENT ENGINE	AI Readiness v1, assembled report contract
ASSESSMENT MODE	Read-only delegated; assembled from per-domain v1 control-assessment evidence
EVIDENCE SOURCE	Microsoft Graph · control-assessments.json
GENERATED	14 May 2026
CLASSIFICATION	Confidential

CONTENTS

READING THIS REPORT

All classifications and findings are assembled from per-domain v1 control-assessment evidence collected read-only from Microsoft Graph. Risk distributions are preserved exactly as derived from the source assessments; no domain is scored from naming conventions or keyword heuristics, and no AI-specific framework tag is assigned from an application name alone.

SECTION 01 / 01

Executive Summary

This assessment evaluates the Contoso Microsoft 365 tenant's readiness to safely enable modern AI platforms, assembled from per-domain v1 control-assessment evidence across eleven governance domains.

The assessment attempted 11 governance domains: Tenant and Licensing Baseline, Identity and Conditional Access Governance, App Consent and OAuth Governance, Microsoft Purview Data Governance Baseline, Data Classification and Sensitivity Labels, Data Loss Prevention Readiness, SharePoint, OneDrive and Teams Exposure, Exchange and Email Data Exposure, Defender for Cloud Apps and Shadow IT, Endpoint and Device Governance, and Audit, Monitoring and Incident Response. 889 assessment rows / control evaluations were scored across 11 scored domains. One domain, Exchange and Email Data Exposure, was only partially collected and scored from the available controls.

Overall verdict

NOT READY FOR BROAD AI ROLLOUT

Elevated findings across **6 action-required domains** and **2 review-required domains** must be remediated or validated before broad enablement. Risk distribution across domain control evaluations: **0 critical / 15 high / 135 medium / 669 low / 70 info**. In addition, **1 cross-domain critical** and **2 cross-domain high** findings were synthesized from the per-domain evidence.

PRIMARY FOCUS AREAS

- Identity & conditional access hardening
- Elevated app-consent & OAuth grants
- Sensitivity-label coverage for Copilot gating
- External sharing & email egress control
- DLP enforcement & Purview retention lifecycle

POSTURE SUMMARY

- 6 domains **Action required** (maturity 2/5)
- 2 domains **Review required** (maturity 3/5)
- 3 domains **Monitor** (maturity 4/5)
- 15 high controls require manual review
- 1 critical cross-domain pathway (Copilot exposure)

NET POSITION

Contoso is **not yet ready for broad AI rollout**. The 15 high-risk controls, the critical cross-domain Copilot exposure pathway, and the elevated controls across the action-required domains must be remediated, and the domain guardrail caps lifted, before advanced AI tooling is enabled against organisational data.

SECTION 02 / 02

Executive Priorities

The three initiatives below group the assessed domains into fundable programs of work, ordered by current readiness (lowest first). Each estimates the readiness improvement achievable on completion.

01 Protect AI-accessible information

2 / 5 → 4 / 5

Govern the data Copilot can reach: publish sensitivity labels with a default and mandatory labelling, enforce DLP across the sensitive collaboration workloads, establish Purview retention, and tighten SharePoint/OneDrive external sharing. Together these ensure AI surfaces only classification-gated, egress-controlled content.

- Microsoft Purview Data Governance Baseline
- Data Classification and Sensitivity Labels
- Data Loss Prevention Readiness
- SharePoint, OneDrive and Teams Exposure

02 Control access and third-party risk

2 / 5 → 4 / 5

Control who and what can reach Microsoft 365 data: review and reduce elevated OAuth/app-consent grants and enforce Conditional Access (MFA, block legacy authentication, restrict user consent) so AI and third-party connectors operate under least privilege.

- Identity and Conditional Access Governance
- App Consent and OAuth Governance

03 Trust devices and detect threats

2 / 5 → 4 / 5

Ensure AI is accessed from trusted, monitored endpoints: enforce device compliance, resolve active Defender alerts, restrict external mail forwarding, and enable sign-in/audit monitoring so misuse of AI-accessible data can be both prevented and investigated.

- Defender for Cloud Apps and Shadow IT
- Exchange and Email Data Exposure
- Supporting: Endpoint and Device Governance
- Supporting: Audit, Monitoring and Incident Response

TOP CANDIDATE USERS

Not assessed in this run. A pilot group requires Microsoft 365 usage / adoption evidence before it can be recommended.

SECTION 03 / 03

Key Outcomes & KPI Cover

HIGH / CRITICAL CONTROLS REQUIRING REVIEW

15 high

15 high control(s) require manual review before broad AI rollout, alongside 1 critical cross-domain pathway. Zero critical findings were observed at the individual domain-control level.

DOMAINS SCORED	11 / 11
PARTIALLY COLLECTED	1
ROWS SCORED	889
CROSS-DOMAIN FINDINGS	1 crit · 2 high

DOMAINS SCORED
11
0 not scored (collection incomplete) · 1 partially collected.

ASSESSMENT ROWS SCORED
889
Control evaluations across the 11 scored domains.

HIGH / CRITICAL CONTROLS
15
1 critical pathway(s) · 15 high control(s) as readiness blockers.

CROSS-DOMAIN FINDINGS
3
1 critical / 2 high synthesized findings.

KPI cover

Domains scored	11
Domains not scored (collection incomplete)	0
Domains partially collected	1
Total assessment rows scored	889
Risk distribution (domain control evaluations)	0 crit / 15 high / 135 med / 669 low / 70 info
Cross-domain synthesized findings	1 critical / 2 high
Overall readiness blockers	1 critical pathway · 15 high controls
High / Critical controls	15
Method limits	Domain-specific: see Evidence Appendix Limit column

SECTION 04 / 04

Top Risks & Risk Distribution

Lead risks

Cross-domain critical: Copilot can surface ungoverned sensitive content — CRITICAL

Cross-domain high: Over-consented apps can extract data with limited compensating control — HIGH

Cross-domain high: External sharing is enabled with no data-egress control — HIGH

15 high/critical control(s) require manual review before broad AI rollout. Method limits are domain-specific: see each domain narrative and the Evidence Appendix Limit column.

Risk distribution across domains

889 domain control evaluations, tiered exactly as derived from the source assessments.

Critical · 0 High · 15 Medium · 135 Low · 669 Info · 70

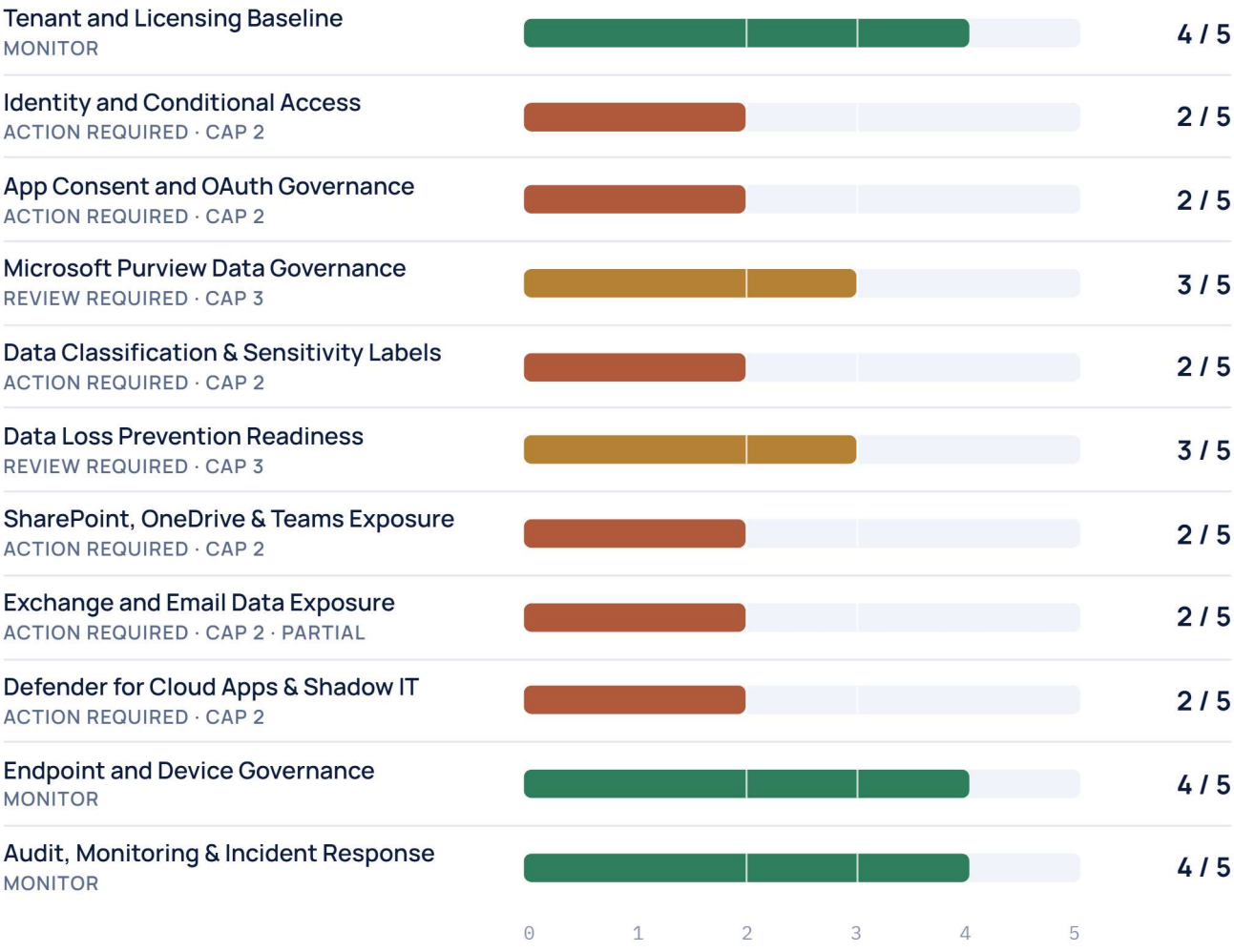
Per-domain verdicts

- Tenant and Licensing Baseline: Monitor (4/5)
- Identity and Conditional Access Governance: Action required (2/5)
- App Consent and OAuth Governance: Action required (2/5)
- Microsoft Purview Data Governance Baseline: Review required (3/5)
- Data Classification and Sensitivity Labels: Action required (2/5)
- Data Loss Prevention Readiness: Review required (3/5)
- SharePoint, OneDrive and Teams Exposure: Action required (2/5)
- Exchange and Email Data Exposure: Action required (2/5)
- Defender for Cloud Apps and Shadow IT: Action required (2/5)
- Endpoint and Device Governance: Monitor (4/5)
- Audit, Monitoring and Incident Response: Monitor (4/5)

SECTION 05 / 05

Domain Maturity Overview

Maturity score (x / 5) for each of the 11 assessed domains, coloured by verdict. Bars are plotted to the exact per-domain scores; gridlines mark L2 and L3.



READING THE SCORES

The six action-required domains carry a guardrail cap of 2 and the two review-required domains a cap of 3; each cap holds the domain (and overall readiness) at that ceiling until the elevated controls are remediated. The three Monitor domains (4/5) are within baseline and are tracked, not remediated. Mean domain maturity is 2.7 / 5 (derived); the per-domain scores above, not the mean, are authoritative.

SECTION 06 / 06

Domain Summary

DOMAIN	MATURITY	VERDICT	CAP	NARRATIVE
Tenant and Licensing Baseline	4/5	Monitor	None	17 Licensing control(s) assessed (16 SKU inventory, 1 licensing posture). Establishes whether Purview, Entra P1/P2, Defender and Copilot capabilities are present to support AI-governance controls. Risk: 0 crit / 0 high / 0 med / 1 low / 16 info.
Identity and Conditional Access Governance	2/5	Action required	2	2 identity & conditional-access control(s) assessed (Conditional Access posture, app-consent/guest authorization, privileged-role census). Risk: 0 crit / 2 high / 0 med / 0 low / 0 info.
App Consent and OAuth Governance	2/5	Action required	2	808 app-consent assessment row(s) assembled from locked v1 scorer output. Risk: 0 crit / 9 high / 133 med / 666 low / 0 info. Identity-source distribution: 105 publisher-confirmed Microsoft / 65 publisher-confirmed named third-party / 538 owner-tenant Microsoft / 35 owner-tenant self LOB / 59 owner-tenant external / 6 true unknown.
Microsoft Purview Data Governance Baseline	3/5	Review required	3	1 Purview control(s) assessed (0 retention-policy inventory, 0 retention-label inventory, 1 retention governance posture). Retention policies and published labels establish the data lifecycle baseline for AI-exposed content. Risk: 0 crit / 0 high / 1 med / 0 low / 0 info.
Data Classification and Sensitivity Labels	2/5	Action required	2	6 sensitivity-label control(s) assessed (label inventory, label-policy coverage, published-coverage posture). Label coverage is the load-bearing Copilot content-gating metric. Risk: 0 crit / 1 high / 0 med / 0 low / 5 info.
Data Loss Prevention Readiness	3/5	Review required	3	16 DLP control(s) assessed (7 policy inventory, 8 rule inventory, 1 enforced-workload coverage posture). DLP coverage is the data-egress control baseline for AI-exposed collaboration workloads. Risk: 0 crit / 0 high / 1 med / 0 low / 15 info.

Domains 7–11 continue on the next page.

SECTION 06 · PART II

/ 06

Domain Summary (continued)

DOMAIN	MATURITY	VERDICT	CAP	NARRATIVE
SharePoint, OneDrive and Teams Exposure	2/5	Action required	2	1 SharePoint/OneDrive/Teams control(s) assessed (0 site inventory, 1 tenant-sharing posture). Tracks anyone links, guest sharing, re-sharing and sampled site exposure. Per-site permission/oversharing depth requires SharePoint Administrator; scored from tenant-level sharing configuration only. Risk: 0 crit / 1 high / 0 med / 0 low / 0 info.
Exchange and Email Data Exposure	2/5	Action required	2	10 Exchange control(s) assessed (8 transport-rule inventory, 1 sharing-policy inventory, 1 forwarding/sharing posture). Email-egress and external-sharing baseline for AI-exposed content. Risk: 0 crit / 1 high / 0 med / 0 low / 9 info. Collection partial: 1 surface(s) could not be read this run (see scope findings); scored from available controls only.
Defender for Cloud Apps and Shadow IT	2/5	Action required	2	11 Defender control(s) assessed (10 security-alert inventory, 1 Secure Score / alert posture). Tracks threat alerts and cloud-app discovery coverage. Full Shadow-IT / cloud-app discovery requires Microsoft Defender for Cloud Apps licensing; this slice uses Graph security-posture signals (Secure Score + alerts). Risk: 0 crit / 1 high / 0 med / 0 low / 10 info.
Endpoint and Device Governance	4/5	Monitor	None	16 Endpoint control(s) assessed (6 compliance-policy inventory, 9 configuration-profile inventory, 1 device-compliance posture). Device-compliance baseline for AI/Copilot access. Risk: 0 crit / 0 high / 0 med / 1 low / 15 info.
Audit, Monitoring and Incident Response	4/5	Monitor	None	1 Audit control(s) assessed (1 audit/sign-in monitoring posture). Incident-response visibility baseline for AI/Copilot access. Risk: 0 crit / 0 high / 0 med / 1 low / 0 info.

11 of 11 domains scored; 0 not scored (collection incomplete); 1 partially collected.

SECTION 07 / 07

Domain Evidence Coverage

Assessment depth, collection status and rollout impact per domain. **Blocks broad rollout** = each domain's verdict (Monitor = **No**, Review = **Review**, Action-required = **Yes**), stated exactly as assessed.

DOMAIN	SCORED	DEGRADED	COLLECTION	ASSESSMENT DEPTH	MATURITY	IN MODEL	BLOCKS ROLLOUT
Tenant and Licensing Baseline	17	0	complete	Capability presence (SKU/service-plan)	4/5	Yes	No
Identity and Conditional Access Governance	2	0	complete	Full available delegated surface	2/5	Yes	Yes
App Consent and OAuth Governance	808	0	complete	v1 app-consent scorer slice	2/5	Yes	Yes
Microsoft Purview Data Governance Baseline	1	0	complete	Full available delegated surface	3/5	Yes	Review
Data Classification and Sensitivity Labels	6	0	complete	Full available delegated surface	2/5	Yes	Yes
Data Loss Prevention Readiness	16	0	complete	Full available delegated surface	3/5	Yes	Review
SharePoint, OneDrive and Teams Exposure	1	0	complete	Tenant-level sharing config only (per-site depth needs SharePoint Admin)	2/5	Yes	Yes
Exchange and Email Data Exposure	10	1	partial	Partial: 1 surface unavailable	2/5	Yes	Yes
Defender for Cloud Apps and Shadow IT	11	0	complete	Graph Secure Score + alerts (MDCA licence for full Shadow-IT)	2/5	Yes	Yes
Endpoint and Device Governance	16	0	complete	Full available delegated surface	4/5	Yes	No
Audit, Monitoring and Incident Response	1	0	complete	Sampled log availability	4/5	Yes	No

11 of 11 domains scored; 0 not scored; 1 partially collected; all contribute to the readiness model. Partial-collection and capped-depth limits are stated in the columns above and detailed in Section 15 (Boundary & Limits): limitations, not assessed passes.

SECTION 08 · PART I / 08

Detailed Findings: Baseline, Identity & App Consent

Tenant and Licensing Baseline

Monitor | Maturity 4 / 5 | 17 controls

Tenant licensing within baseline

LOW | INFORMATIONAL

Purview and Entra P1/P2 licensing are present in this assessment slice.

Recommendation. Maintain licensing coverage for AI-governance controls.

NIST AI RMF | Copilot Readiness

Identity and Conditional Access Governance

Action required | Maturity 2 / 5 | Guardrail cap 2 | 2 controls

Risk distribution: 0 critical / 2 high / 0 medium / 0 low / 0 info.

Identity & Conditional Access controls require remediation

HIGH | FAIL

2 Identity & Conditional Access control(s) are high or critical risk and should be remediated before broad AI rollout.

Recommendation. Enforce MFA and block legacy authentication via Conditional Access, restrict application consent to administrators, and reduce standing privileged-role membership before broad AI rollout.

NIST AI RMF

App Consent and OAuth Governance

Action required | Maturity 2 / 5 | Guardrail cap 2 | 808 rows

808 app-consent assessment row(s) assembled from locked v1 scorer output. Risk distribution: 0 critical / 9 high / 133 medium / 666 low / 0 info. Identity-source distribution is detailed in Section 10.

Elevated app-consent grants require manual review

HIGH | FAIL

9 assessment row(s) are high or critical risk. Broad/admin app grants can expose Microsoft 365 data before AI or automation workflows are approved.

Recommendation. Confirm owner, business justification, admin consent, and granted scopes; reduce or remove access unless explicitly approved.

NIST AI RMF | Copilot Readiness | MITRE ATLAS · AML.T0060

SECTION 08 · PART II

Detailed Findings: App Consent (cont.) & Data Governance

/ 08

App Consent and OAuth Governance (continued)

Action required | 2 / 5

Medium-risk app-consent inventory requires owner validation

MED | REVIEW

133 medium-risk assessment row(s) need owner and business-purpose validation before AI rollout decisions rely on the inventory.

Recommendation. Validate owners and business purpose during the app-consent review cycle.

NIST AI RMF

Publisher and owner identity gaps remain visible

HIGH | REVIEW

Identity-source buckets needing manual validation: 65 publisher-confirmed named third-party, 59 owner-tenant external, 6 true unknown.

Recommendation. Use publisher, owner tenant, and client allowlist validation before approving app access.

NIST AI RMF

Method limits constrain publisher confidence

LOW | INFORMATIONAL

Residual publisher-confidence limits remain until richer Graph fields and MSP allowlist evidence are collected.

Recommendation. Add verifiedPublisherId/MPN, application tags, disabledByMicrosoftStatus, and MSP allowlist validation in a later collector pass.

Microsoft Purview Data Governance Baseline

Review required | Maturity 3 / 5 | Guardrail cap 3 | 1 control

Purview data governance has retention lifecycle gaps

MED | REVIEW

1 Purview control(s) are medium risk; retention/disposition lifecycle governance is not enforced for AI-exposed content.

Recommendation. Define and publish Purview retention policies or labels so data lifecycle governance is enforceable before broad AI rollout.

NIST AI RMF | Copilot Readiness

Data Classification and Sensitivity Labels

Action required | Maturity 2 / 5 | Guardrail cap 2 | 6 controls

Sensitivity-label coverage gaps leave Copilot-exposed content ungated

HIGH | FAIL

1 sensitivity-label control(s) are high or critical risk. Without published label coverage, Copilot and other AI retrieval surfaces can surface content that is not classification-gated.

Recommendation. Define and publish sensitivity labels with a default label and mandatory labeling so Copilot-exposed content is classification-gated; apply label-bound encryption to high-sensitivity content.

NIST AI RMF | MITRE ATLAS | Copilot Readiness

SECTION 08 · PART III / 08

Detailed Findings: Data Egress & Collaboration Exposure

Data Loss Prevention Readiness

Review required | 3 / 5 | cap 3 | 16 controls

DLP coverage is partial across sensitive workloads

MED | REVIEW

1 DLP control(s) are medium risk; enforced DLP exists but does not cover every sensitive workload in scope.

Recommendation. Create and enforce DLP policies across sensitive collaboration workloads so data egress is actively controlled before broad AI rollout.

NIST AI RMF | MITRE ATLAS | Copilot Readiness

SharePoint, OneDrive and Teams Exposure

Action required | 2 / 5 | cap 2 | 1 control

SharePoint tenant sharing permits anyone links

HIGH | FAIL

1 SharePoint exposure control(s) are high or critical risk. Anyone/anonymous links can make sensitive collaboration content externally accessible before broad AI rollout.

Recommendation. Restrict anyone links and validate guest-sharing scope so AI-exposed collaboration content is not overshared before broad rollout. **Depth:** tenant-level sharing configuration only; per-site permission/oversharing depth requires the SharePoint Administrator role.

NIST AI RMF | MITRE ATLAS | Copilot Readiness

Exchange and Email Data Exposure

Action required | 2 / 5 | cap 2 | 10 controls · partial

Exchange email exposure permits uncontrolled external data egress

HIGH | FAIL

1 Exchange control(s) are high or critical risk. If automatic external forwarding is permitted, AI-exposed organizational data can leave the tenant through email.

Recommendation. Restrict automatic external mail forwarding and scope Exchange sharing policies to approved external domains before broad AI rollout.

NIST AI RMF | MITRE ATLAS | Copilot Readiness

Assessment scope: Exchange exposure inventory

INFO | SCOPE

Re-run the assessment; the surface could not be read this run (transient collector/runtime error, not a permission gap). No grant change is required unless a re-run shows a permission gap. Reported as required engagement scope (UNKNOWN-not-DEAD), not a tenant finding.

SECTION 08 · PART IV / 08

Detailed Findings: Defender, Endpoint & Audit

Defender for Cloud Apps and Shadow IT

Action required | 2 / 5 | cap 2 | 11 controls

Defender posture has active high-severity security alerts

HIGH | FAIL

1 Defender control(s) are high or critical risk. Active high-severity security alerts indicate threats are present before broad AI rollout.

Recommendation. Triage high-severity security alerts, improve Microsoft Secure Score controls, and confirm Defender coverage before broad AI rollout. **Depth:** Graph security-posture signals (Secure Score + alerts); full Shadow-IT / cloud-app discovery requires Microsoft Defender for Cloud Apps licensing.

NIST AI RMF | MITRE ATLAS | Copilot Readiness

Endpoint & Device Governance

Monitor · 4/5

Endpoint governance within baseline

LOW

Device-compliance policies exist and the managed fleet is majority-compliant in this assessment slice.

Recommendation. Maintain compliance policy coverage and review managed-device compliance periodically.

Audit, Monitoring & IR

Monitor · 4/5

Audit monitoring within baseline

LOW

Audit and sign-in log monitoring are available in this assessment slice.

Recommendation. Maintain monitoring coverage and validate incident-response workflows periodically.

SECTION 09 / 09

Cross-Domain Findings

Synthesized by deterministic correlation over the scored per-domain evidence, with no additional tenant query. Individually these are separate domain findings; together they create combined AI-exposure pathways that must be remediated as one initiative.

COPILOT CAN SURFACE UNGOVERNED SENSITIVE CONTENT

CRITICAL

Microsoft Copilot inherits each user's existing access to SharePoint and OneDrive content. With sensitivity labels unpublished or weak and DLP coverage incomplete, confidential content can be retrieved and summarised by authorised users without classification-driven guardrails or any egress control. Individually these are separate domain findings; together they create a direct path for AI-amplified exposure of ungoverned sensitive data. Remediating Purview labelling, DLP enforcement, and SharePoint sharing together materially reduces AI data-exposure.

Recommendation. Treat these domains as one initiative: SharePoint, OneDrive and Teams Exposure; Data Classification and Sensitivity Labels; Data Loss Prevention Readiness. Remediating them together (not in isolation) is what reduces the combined AI exposure.

NIST AI RMF · MAP | sharepoint-exposure · 2/5 | sensitivity-label-inventory · 2/5 | dlp-readiness · 3/5

OVER-CONSENTED APPS CAN EXTRACT DATA WITH LIMITED COMPENSATING CONTROL

HIGH

Broad or over-consented OAuth applications can programmatically reach Microsoft 365 data on a user's behalf. With DLP coverage incomplete and app consent over-permissive, the tenant has limited compensating control over sensitive data once approved apps or connectors: including AI and automation connectors: can access it.

Recommendation. Treat these domains as one initiative: App Consent and OAuth Governance; Data Loss Prevention Readiness. Remediating them together (not in isolation) is what reduces the combined AI exposure.

NIST AI RMF · MAP | app-consent-oauth · 2/5 | dlp-readiness · 3/5

EXTERNAL SHARING IS ENABLED WITH NO DATA-EGRESS CONTROL

HIGH

External sharing is permitted on collaboration workloads while DLP is not enforced on those same workloads, so sensitive content can be shared externally with nothing inspecting or blocking the data leaving the boundary.

Recommendation. Treat these domains as one initiative: SharePoint, OneDrive and Teams Exposure; Data Loss Prevention Readiness. Remediating them together (not in isolation) is what reduces the combined AI exposure.

NIST AI RMF · MAP | sharepoint-exposure · 2/5 | dlp-readiness · 3/5

SECTION 10 / 10

Identity Source Model & Distribution

The 808 app-consent assessment rows were attributed using deterministic identity-provenance modelling against the assembled v1 scorer evidence. Buckets and counts below are taken exactly from the App Consent and OAuth Governance domain.

Identity source distribution

Counts and share across 808 assessed app-consent assessment rows.

FIRST-PARTY MICROSOFT

643 · 79.6%

Owner-tenant + publisher-confirmed Microsoft.

MANUAL-VALIDATION QUEUE

130

65 named 3P + 59 external-owner + 6 true unknown.

TRUE UNKNOWN

6 · 0.7%

No reliable publisher or owner attribution.

WHAT THIS CONFIRMS

Provenance-anchored classification narrows governance attention to the 133 medium-risk rows requiring owner validation plus the identity buckets flagged for manual review: 65 publisher-confirmed named third-party, 59 owner-tenant external and 6 true unknown. Residual publisher-confidence limits remain until verifiedPublisherId/MPN, application tags, disabledByMicrosoftStatus and MSP allowlist evidence are collected in a later pass.

SECTION 11 / 11

Prioritized Remediation

Track A: Client remediation

Changes the client's M365 administrator makes to the tenant.

SEQ	ACTION	SEVERITY	EFFORT	OWNER	DEPENDENCY
1	Remediate elevated Identity & Conditional Access controls	HIGH	Medium	M365 administrator	Client confirms intended baseline
2	Review and reduce elevated app-consent grants	HIGH	Medium	M365 administrator	Client confirms owner and business justification
3	Resolve external-owner and unknown publisher identities	MED	Medium	M365 administrator	MSP/client allowlist decision
4	Validate medium-risk Purview controls	MED	Low	M365 administrator	None
5	Remediate elevated Sensitivity Labels controls	HIGH	Medium	M365 administrator	Client confirms intended baseline
6	Validate medium-risk DLP controls	MED	Low	M365 administrator	None
7	Remediate elevated SharePoint controls	HIGH	Medium	M365 administrator	Client confirms intended baseline
8	Remediate elevated Exchange controls	HIGH	Medium	M365 administrator	Client confirms intended baseline
9	Remediate elevated Defender controls	HIGH	Medium	M365 administrator	Client confirms intended baseline

Track B: Platform / collector remediation

RSG.AI-side assessment tooling & evidence enrichment.

SEQ	ACTION	SEVERITY	EFFORT	OWNER	DEPENDENCY
1	Extend collector metadata for publisher verification	LOW	Medium	Platform engineer	Graph field availability and allowlist source

SEQUENCING

Track A items are ordered by operational priority and map directly to the detailed findings. The high-severity items (1, 2, 5, 7, 8, 9) clear the elevated controls that hold the action-required domains at their guardrail caps; the medium items (3, 4, 6) validate the review-required controls. Track B is a platform enrichment task owned by RSG.AI, not a tenant change.

SECTION 12 / 12

Guardrail Caps

Each finding below caps the maximum domain / readiness score until it is remediated. The cap holds the domain at its ceiling regardless of other controls: a capped domain cannot score above the stated value.

FINDING	MAX SCORE
Identity & Conditional Access controls require remediation	Capped at 2
Elevated app-consent grants require manual review	Capped at 2
Medium-risk app-consent inventory requires owner validation	Capped at 3
Purview data governance has retention lifecycle gaps	Capped at 3
Sensitivity-label coverage gaps leave Copilot-exposed content ungated	Capped at 2
DLP coverage is partial across sensitive workloads	Capped at 3
SharePoint tenant sharing permits anyone links	Capped at 2
Exchange email exposure permits uncontrolled external data egress	Capped at 2
Defender posture has active high-severity security alerts	Capped at 2

HOW CAPS LIFT

A guardrail cap is released only when its underlying finding is remediated and re-assessed. Six findings cap their domain at 2 and three cap at 3; until they clear, overall readiness cannot rise above the elevated-domain ceiling: which is why the verdict remains **Not ready for broad AI rollout**.

SECTION 13 / 13

Governance Maturity Heatmap

Each cell is one assessed governance domain, coloured by verdict and labelled with its exact maturity score. Six domains are **action required**, two **review required**, and three within **monitor** baseline.

TENANT & LICENSING **L4 · Monitor** Purview & Entra P1/P2 present.	IDENTITY & COND. ACCESS **L2 · Action** 2 high controls; cap 2.	APP CONSENT & OAUTH **L2 · Action** 9 high grants; cap 2.	PURVIEW DATA GOVERNANCE **L3 · Review** Retention lifecycle gap; cap 3.
SENSITIVITY LABELS **L2 · Action** Coverage gap leaves content ungated; cap 2.	DLP READINESS **L3 · Review** Partial workload coverage; cap 3.	SHAREPOINT / ONEDRIVE / TEAMS **L2 · Action** Anyone links permitted; cap 2.	EXCHANGE & EMAIL **L2 · Action** External egress; partial collection; cap 2.
DEFENDER & SHADOW IT **L2 · Action** Active high-severity alerts; cap 2.	ENDPOINT & DEVICE **L4 · Monitor** Fleet majority-compliant.	AUDIT & MONITORING **L4 · Monitor** Sign-in/audit logs available.	CROSS-DOMAIN AI EXPOSURE **Critical pathway** Copilot exposure chain (see §09).

Monitor (4/5) · Review required (3/5) · Action required (2/5) · Cross-domain synthesized

MATURITY SUMMARY

The three Monitor domains anchor the estate's baseline, but six domains across identity, app-consent, data classification and collaboration exposure are **action required** and two **review required**. Overlaid on these is the critical cross-domain Copilot-exposure pathway: the focus of the joint remediation initiative in Section 09.

SECTION 14 · PART I

/ 14

Evidence Appendix

Every finding traces to collected evidence. All evidence was collected `2026-05-14T10:00:00Z` from `control-assessments.json` unless a domain source is stated. The Limit column records each item's method boundary.

EVIDENCE ID	RISK	LIMIT
`evidence-tenant-licensing-baseline-sku-e3d0ec29-3dc6-5ef2-0cdb-b1d82a8b8c2d`	low	Delegated Graph read of subscribed SKUs and service plans; capability presence only, not per-user entitlement.
`evidence-tenant-licensing-baseline-sku-dc4a3dfb-6120-4bab-8346-7c344d7aef32`	low	Delegated Graph read of subscribed SKUs and service plans; capability presence only, not per-user entitlement.
`evidence-tenant-licensing-baseline-sku-abc13b87-bdc7-a1e1-85c7-518e8675d0ea`	low	Delegated Graph read of subscribed SKUs and service plans; capability presence only, not per-user entitlement.
`evidence-tenant-licensing-baseline-sku-193bfc22-e8e3-8416-88f9-d3e4a2a362ee`	low	Delegated Graph read of subscribed SKUs and service plans; capability presence only, not per-user entitlement.
`evidence-tenant-licensing-baseline-sku-30e653da-0226-55f6-dcf1-f89b29e1d945`	low	Delegated Graph read of subscribed SKUs and service plans; capability presence only, not per-user entitlement.
`evidence-identity-ca-authorizationPolicy`	high	Delegated Microsoft Graph read of Conditional Access, authorization policy, and directory-role posture.
`evidence-identity-ca-posture`	high	Delegated Microsoft Graph read of Conditional Access, authorization policy, and directory-role posture.
`evidence-app-consent-92740551-c41b-404b-f795-0228fb0ed13f`	high	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
`evidence-app-consent-c6ba10dc-841d-941d-6faa-38d4feddfc2e`	high	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
`evidence-app-consent-f40d1dcd-23df-e4d2-b1a7-28bb0d854075`	high	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
`evidence-app-consent-d3b81404-2037-1caf-261b-f830752a5b95`	high	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
`evidence-app-consent-ef9097f3-b47c-6c05-9f16-4a7f08f48286`	high	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
`evidence-app-consent-ba26007e-824b-93d8-e893-1daa9e817e70`	medium	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
`evidence-app-consent-2b6a9d61-7833-5c7f-3dbb-f4fa8660c564`	medium	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.

Continued on next page (2 of 3).

SECTION 14 · PART II

Evidence Appendix (continued)

EVIDENCE ID	RISK	LIMIT
evidence-app-consent-0bffbc2c-9867-cc17-cb88-8a005e7bfa24	medium	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
evidence-app-consent-8c90b770-4ddf-5110-6064-31f795d9258f	medium	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
evidence-app-consent-48f4bf88-f02c-be10-b6a8-83f7d638d8da	medium	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
evidence-app-consent-3a6a4d80-e651-ff3a-ab61-6aad7cb9ea84	medium	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
evidence-app-consent-2a707afe-e666-5726-4ae9-6b20d984e8c8	medium	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
evidence-app-consent-d0986a11-e3c6-73a6-cde9-7fa46f671086	medium	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
evidence-app-consent-19b5d959-0226-809e-3c21-230666df98c7	medium	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
evidence-app-consent-ea91b543-7ac8-1a6c-ebf9-d7a658da02b3	medium	Derived from v1 control assessments; current Graph evidence does not include verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation is pending.
evidence-purview-data-governance-posture	medium	Delegated Purview / Security & Compliance read of retention policies and retention labels.
evidence-sensitivity-label-inventory-posture	high	Delegated Security & Compliance read of the sensitivity-label inventory and publishing state.
evidence-dlp-readiness-posture	medium	Delegated Security & Compliance read of DLP policies and rules.
evidence-sharepoint-exposure-posture	high	Tenant-level sharing configuration only; per-site permission and oversharing depth requires the SharePoint Administrator role.
evidence-exchange-email-exposure-posture	high	Delegated Exchange Online read of organisation config, transport rules, and sharing policies; one surface was partially collected this run.
evidence-defender-shadow-it-posture	high	Graph security-posture signals (Secure Score + alerts); full Shadow-IT / cloud-app discovery requires Microsoft Defender for Cloud Apps licensing.

Continued on next page (3 of 3).

SECTION 14 · PART III

Evidence Appendix: endpoint, audit & cross-domain

EVIDENCE ID	SOURCE	RISK	LIMIT
evidence-endpoint-intune-compliance-policy-fa117aed-57c0-ae05-16a2-0a9e5199bf4f	control-assessments.json	low	Delegated Graph read of Intune device-compliance policies, configuration profiles, and managed-device compliance state.
evidence-endpoint-intune-compliance-policy-740b742f-b04f-47ba-9558-72cbf37007e5	control-assessments.json	low	Delegated Graph read of Intune device-compliance policies, configuration profiles, and managed-device compliance state.
evidence-endpoint-intune-compliance-policy-e15ec8f0-c139-ee6f-5cd8-b6eb750265b5	control-assessments.json	low	Delegated Graph read of Intune device-compliance policies, configuration profiles, and managed-device compliance state.
evidence-endpoint-intune-compliance-policy-500030ee-a518-dcc8-0234-c619787c8114	control-assessments.json	low	Delegated Graph read of Intune device-compliance policies, configuration profiles, and managed-device compliance state.
evidence-endpoint-intune-compliance-policy-a50684ac-e2c0-9bb2-65cb-7a9865c5b0b3	control-assessments.json	low	Delegated Graph read of Intune device-compliance policies, configuration profiles, and managed-device compliance state.
evidence-audit-monitoring-posture	control-assessments.json	low	Audit and sign-in log availability sampled; not a full incident-response workflow validation.
evidence-exchange-email-exposure-scope-exchange-surfaces	control-assessments.json	info	Delegated Exchange Online read of organisation config, transport rules, and sharing policies; one surface was partially collected this run.
sharepoint-exposure	SharePoint, OneDrive and Teams Exposure	critical	Deterministic correlation over the scored per-domain evidence; no additional tenant query.
sensitivity-label-inventory	Data Classification and Sensitivity Labels	critical	Deterministic correlation over the scored per-domain evidence; no additional tenant query.
dlp-readiness	Data Loss Prevention Readiness	critical	Deterministic correlation over the scored per-domain evidence; no additional tenant query.
app-consent-oauth	App Consent and OAuth Governance	high	Deterministic correlation over the scored per-domain evidence; no additional tenant query.

39 evidence items across 11 domains and 4 cross-domain correlations.

SECTION 15 / 15

Boundary, Limits & Benchmark Commitments

Boundary and limits

Assembled from per-domain delegated read-only control-assessment evidence; per-domain method limits are noted with each domain and in the Evidence Appendix.

STATED METHOD LIMITS

- App consent: no verifiedPublisherId/MPN, application tags, or disabledByMicrosoftStatus; MSP allowlist validation pending.
- SharePoint: tenant-level sharing configuration only; per-site depth requires SharePoint Administrator.
- Defender: Graph Secure Score + alerts; full Shadow-IT discovery requires Defender for Cloud Apps licensing.
- Exchange: 1 surface partially collected this run (transient, not a permission gap); re-run to close.
- Audit: log availability sampled, not a full incident-response workflow validation.

HONESTY MARKERS PRESERVED

- 0 domains unscored; 1 domain partially collected (Exchange).
- Monitor domains block rollout = **No**; Review domains = **Review**; not upgraded.
- The scope finding is reported as required engagement scope (UNKNOWN-not-DEAD), not a tenant finding.
- Cross-domain findings retain their contributing-domain evidence references.

Benchmark commitments

01	Preserve each domain scorer's risk distribution exactly as derived from the input assessments.
02	Render native and P1-extended reports from the same assembled report contract.
03	Do not assign AI-specific framework tags from application name or keyword evidence alone.

SECTION 16 / 16

Methodology & Conclusion

Assessment methodology

Assembled from per-domain v1 control-assessment evidence collected read-only from Microsoft Graph and deterministic classification logic. This report does not re-query the tenant or rescore evidence; cross-domain findings are produced by deterministic correlation over the scored per-domain evidence with no additional tenant query.

- Tenant & licensing capability baseline
- Identity & conditional access assessment
- App-consent & OAuth provenance modelling
- Purview retention & sensitivity-label coverage
- DLP enforced-workload coverage
- SharePoint / Exchange exposure posture
- Defender Secure Score & alert posture
- Endpoint compliance & audit-log availability

Assessment limitations

The following metadata was **not** collected this cycle; later iterations may expand collection to improve attribution fidelity.

- `verifiedPublisherId` / MPN
- `application tags`
- `disabledByMicrosoftStatus`
- `MSP allowlist validation`

PARTIAL COLLECTION

Exchange and Email Data Exposure was scored from available controls with 1 surface unavailable this run: a transient collector/runtime error, not a permission gap. Re-run to close.

METHODOLOGY INTEGRITY STATEMENT

This assessment avoids heuristic-only trust inference, unsupported publisher assumptions, unsupported risk escalation and AI keyword-only framework mapping. Each domain scorer's risk distribution is preserved exactly; all findings are traceable to collected Microsoft Graph evidence and deterministic classification logic.

Conclusion

The Contoso environment is **not yet ready for broad AI rollout**. Elevated findings across 6 action-required domains and 2 review-required domains: 15 high controls and a critical cross-domain Copilot-exposure pathway: must be remediated or validated before broad enablement.

Six domains are rated **Action required** (maturity 2/5), two **Review required** (3/5), and three sit within **Monitor** baseline (4/5). The prioritised Track A / Track B remediation register and the guardrail caps define the path to lifting each domain ceiling and reaching a safe AI-enablement baseline.

SECTION 17

Assessment Metadata

Engine, evidence and attestation values for this assessment run. Hashes may be used to verify report provenance against source telemetry.

REPORT ID	ai-readiness-v1-assembled
PREPARED FOR	Contoso
ASSESSMENT ENGINE	AI Readiness v1, assembled report contract
EVIDENCE SOURCE	Microsoft Graph · control-assessments.json
EVIDENCE RUN ID	assembled-2026-05-14T10:00:00Z
EVIDENCE HASH	sha256:04006992cf38aba6d66095e7e94d72f4c0791ba73b0f738f39153ff605b40005
ASSESSMENT HASH	sha256:2288dba999a6ce8c2348073df24034fef6b4615bb49b5566aebe1ca2c123a1c4
DOCUMENT ID	AIRA-2026-CTSO
GENERATED	14 May 2026 · 10:00 UTC