M365 Copilot Readiness Assessment

Contoso Ltd — 07 May 2026

Readiness score 87.6%

NOT READY

Confidential — prepared by JFDI Consulting

NOT READY

NOT READY

Readiness score 87.6% | Deployment verdict based on 31 high-priority findings | Resolve 16 to reach next level

Score reflects breadth of passing checks; deployment verdict is driven by high-priority blockers.

MEDIUM

72.5%

IDENTITY & ACCESS

MFA 95% members (95% all) | CA 18 policies
4 non-compliant devices

MEDIUM

57.2%

DATA PROTECTION

0 sensitivity labels
0 DLP policies | Audit off

MEDIUM

72.6%

THREAT POSTURE

4 high-sev incidents
61 phishing alerts

MEDIUM

At Risk

SHADOW AI

6 GenAI apps (5 sanctioned)
20 users | 0 high-risk

MEDIUM

Developing

COLLABORATION

100% Teams adoption
2% SharePoint activity

Priority Actions

1. Resolve critical data governance gaps before allowing Copilot to access organisational data. DLP, sensitivity labels, and audit logging are essential for AI data protection.

2. Remediate security gaps for all Copilot-licensed users before deployment: enforce MFA registration, block Copilot access from non-compliant devices via Conditional Access, and investigate any risky user flags via Entra ID Protection.

3. Create sensitivity labels and DLP policies immediately to protect content before Copilot deployment.

Identity & Access

72.5%

8 critical findings | 0 warning findings | Entra domain

Authentication

MFA reg. (active members)	**95%**
MFA reg. (all accounts)	**95%**
Passwordless adoption	**59%**
FIDO2 users	**0**
Legacy auth attempts	**0**
Risky users (total)	**7**

Conditional Access

Policies (enabled / total)	**12 / 18**
Require MFA	**10**
Require compliant device	**4**
Block legacy auth	**3**
Sign-in risk policy	**None**

Device Compliance

Managed devices	**22**
Compliant	**18 (81%)**
Non-compliant	**4**
Compliance policies	**5**

Privileged Access

Permanent privileged roles	**11**
PIM-enabled roles	**1**
Permanent global admins	**0**
Guest users	**3**

Data Protection

57.2%

7 critical findings | 1 warning findings | Purview domain

Sensitivity Labels

Labels configured	0
Labels with encryption	0
Labels with content marking	0
Label policies published	No
Auto-labelling policies	0

Data Loss Prevention

DLP policies (total)	0
Endpoint DLP policies	0
Unclassified files at risk	78,774
Copilot users exposed	1
Azure RMS enabled	No

Audit & Compliance

Unified audit log	Disabled
Retention labels	0
eDiscovery cases	0

Insider Risk & Barriers

Insider risk policies	0
Communication compliance	0
Information barriers	0

Threat Posture

72.6%

6 critical findings | 1 warning findings | Defender domain

Active Threats

Total incidents	**214**
Active incidents	**9**
High-severity incidents	**4**
Suspicious process devices	**3**

Email Threats

Phishing alerts	**61**
Malware alerts	**47**
Total alerts	**139**
Copilot-related phishing	**0**

Security Posture

Secure Score	**83%**
Score (current/max)	**994/1,194**
Risky users (Defender)	**0**

App Governance

Total registered apps	**312**
High-privilege apps	**9**
Unverified publishers	**312**

At Risk

5 apps sanctioned

Discovery Summary

GenAI apps discovered	**6**
Sanctioned	**5**
Untagged	**1**
Unsanctioned	**0**

Usage & Risk

Users accessing GenAI	**20**
Total transactions	**2,214**
High-risk apps	**0**
Medium-risk apps	**1**

Discovered GenAI Applications

Application	Trust	Users	Transactions	Status
Google Gemini	7/10	9	1,402	Sanctioned
GitHub Copilot	10/10	5	188	Sanctioned
ChatGPT (Consumer & Enterprise)	9/10	3	311	Sanctioned
DeepSeek	5/10	1	6	Untagged
Microsoft Copilot	10/10	1	240	Sanctioned
Grammarly	9/10	1	67	Sanctioned

Developing

Maturity 2/5 | M365 94% | Basic collaboration in place but significant gaps remain.

Teams & Meetings

Teams active users	18 / 18 (100%)
Total meetings	416
Avg meetings per user	23.1
Total calls	478

SharePoint & Content

Active sites / total	10 / 417 (2%)
Total files	78,774
Page views	148
Sites with content	224

Email & OneDrive

Active email users	18 / 18 (100%)
Avg sent per user	32.9
OneDrive adoption	82%
OneDrive files	600,210

Copilot Readiness

Copilot licensed	1 / 18 (6%)
Office activated users	23
Desktop activation rate	100%
Graph connectors	1

Executive Summary

31	87.6%	43	NOT READY
High Priority Findings	Readiness Score	Medium Priority	Deployment Verdict

Key Findings

- Your organisation has 18 licensed users, 1 of whom hold active Copilot licences.
- The assessment found that the organisation is not yet ready for Copilot deployment, with 31 high-priority and 43 medium-priority findings (based on 91 of 177 assessed modules).
- Key gaps span 5 domains: Purview (13), M365 (6), Defender (5), Power Platform (4), Entra (3).

Resolve 16 high-priority findings to achieve At Risk status.

Domain Readiness Scorecards

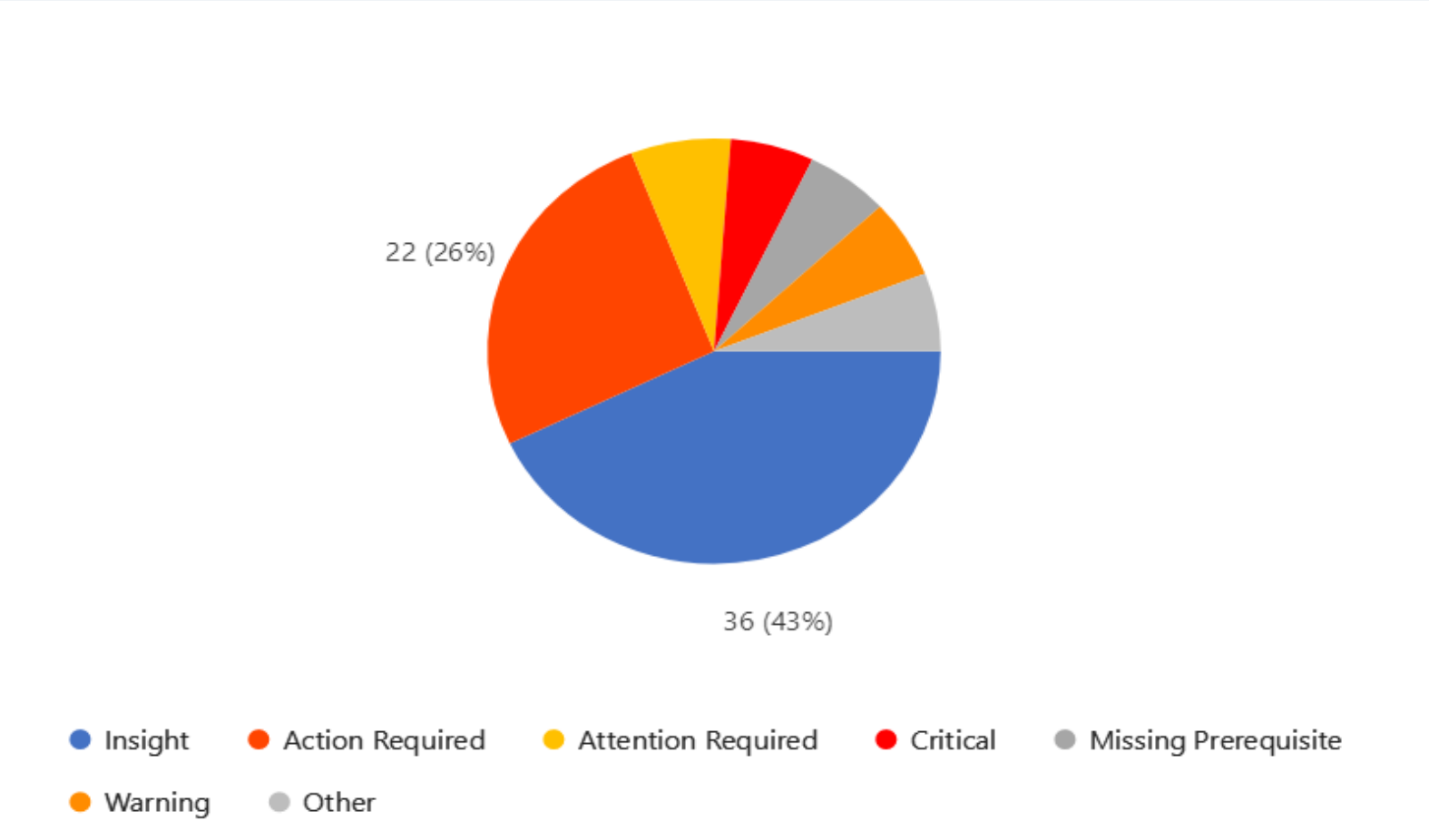
6 domains assessed. Compliance & Governance (Purview) (57.2%) is the weakest; Copilot Studio (100.0%) leads.

Overall Readiness Score: 87.6%

Domain	Score	Critical	Warning	Attention	Total
Productivity & Collaboration (M365)	94.1%	2	3	2	205
Identity & Access (Entra)	72.5%	8	0	3	36
Security Posture (Defender)	72.6%	6	1	0	23
Compliance & Governance (Purview)	57.2%	7	1	1	23
Power Platform	82.9%	4	0	0	21
Copilot Studio	100.0%	0	0	0	13

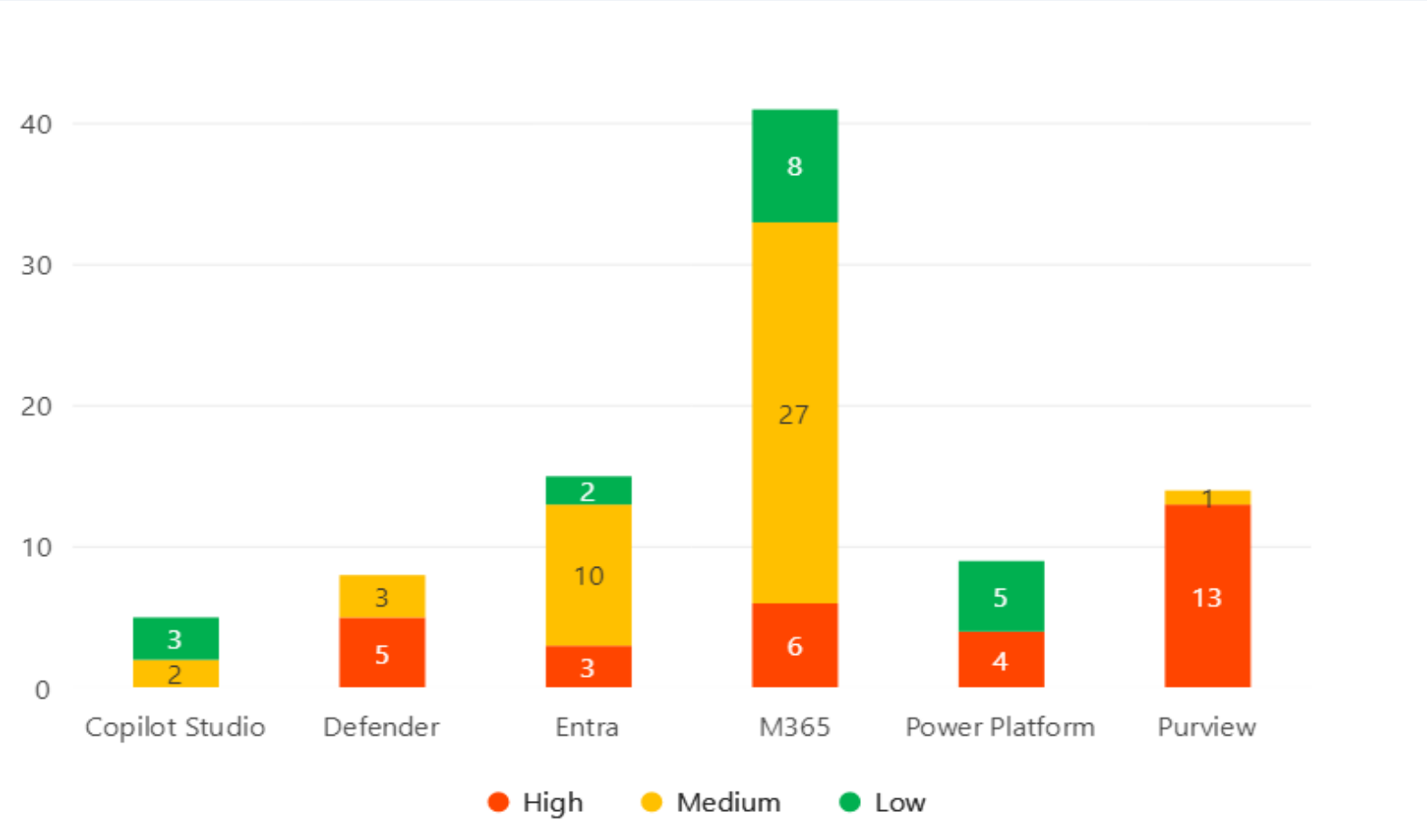
Findings Distribution

237 of 321 checks passed. 84 findings require attention: 31 high-priority and 43 medium-priority. Address blockers before Copilot rollout to avoid governance gaps.



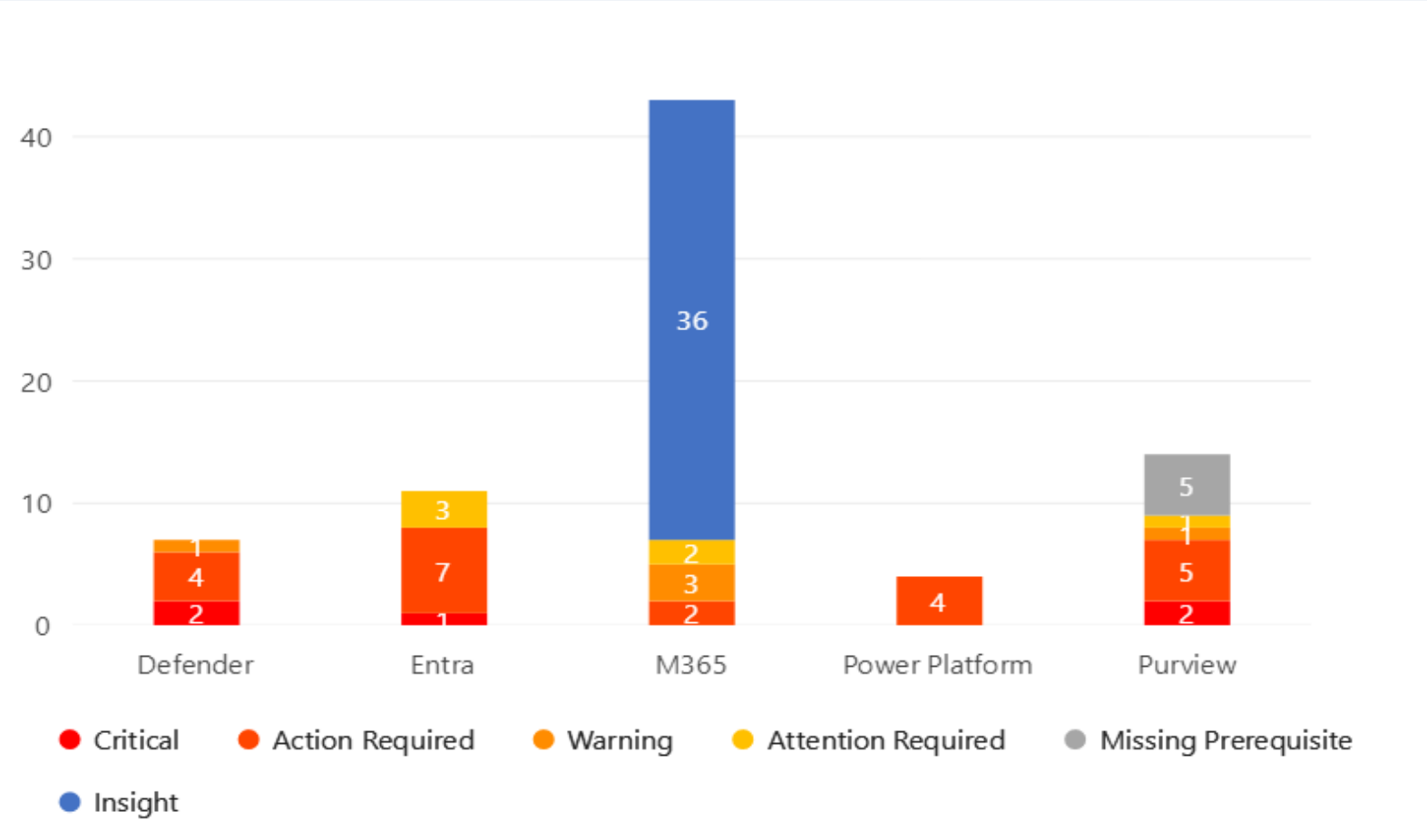
Findings by Priority

M365 has the most findings at 41, spread across 6 domains. Prioritise domains with the tallest bars to maximise readiness improvement per unit of effort.



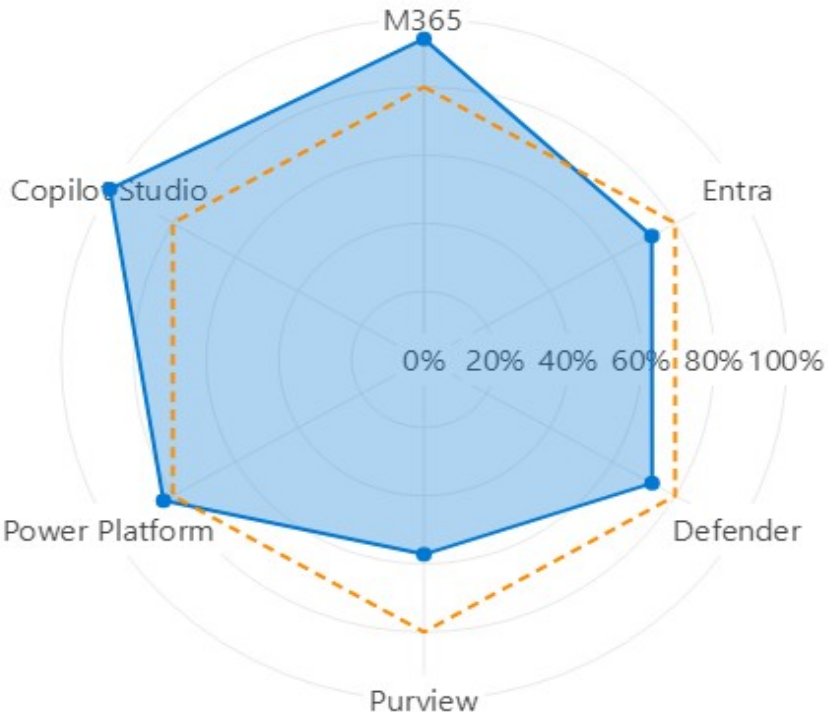
Findings by Status

5 critical and 22 action-required findings across domains. Focus on red and orange segments first — these represent issues that must be resolved before Copilot rollout.



Domain Readiness

Purview is the weakest domain at 57%, while Copilot Studio leads at 100%. Aim to bring all domains above 80% before enterprise Copilot rollout.



Remediation Roadmap

Estimated 3–7 weeks to deployment readiness

Phase	Timeline	Findings	Simple	Moderate	Complex
Phase 0: Blockers — resolve before any rollout	Immediate	5	0	2	3
Phase 1: Pre-deployment — complete before Copilot rollout	1–2 weeks	26	12	9	3
Phase 2: Early lifecycle — address within 30 days	30 days	43	20	21	2
Phase 3: Optimisation — enhance over time	90 days	18	15	3	0

92 findings across all phases. 47 simple (quick wins), 8 complex (require planning). See the spreadsheet export for full remediation detail by domain and feature.

Quick Wins (1 of 3)

High-priority findings that can be resolved with minimal effort.

#	Domain	Feature	Recommended Action
1	Productivity & Collaboration (M365)	Microsoft 365 Copilot - Business Chat	Train users on cross-app Business Chat queries that leverage your...
2	Productivity & Collaboration (M365)	Microsoft 365 Copilot in Teams	Deploy Teams Copilot training focused on meeting efficiency: Enable...
3	Productivity & Collaboration (M365)	Skype for Business Online (Plan 1)	Immediately migrate remaining Skype for Business users to Microsoft...
4	Productivity & Collaboration (M365)	Skype for Business Online (Plan 1)	Plan comprehensive Skype to Teams migration.

See detailed report for additional quick wins.

Quick Wins (2 of 3)

High-priority findings that can be resolved with minimal effort.

#	Domain	Feature	Recommended Action
5	Productivity & Collaboration (M365)	Viva Insights	Use Viva Insights to identify teams with excessive meeting load (15+...
6	Power Platform	Common Data Service for Copilot Studio	Deploy Copilot Studio agents with Dataverse: 1) Build HR agent that...
7	Power Platform	Power Automate for Copilot Studio - Action Agents	Deploy action agents with Power Automate: 1) Build 'IT Helpdesk Agent'...
8	Compliance & Governance (Purview)	Azure Rights Management	Enable Azure RMS in Exchange Online to ensure encryption protects...

See detailed report for additional quick wins.

Quick Wins (3 of 3)

High-priority findings that can be resolved with minimal effort.

#	Domain	Feature	Recommended Action
9	Compliance & Governance (Purview)	Content Marking Coverage	Create sensitivity labels with content markings for visual...
10	Compliance & Governance (Purview)	Copilot Interaction Audit Trail	Enable the unified audit log in the Microsoft Purview compliance...

See detailed report for additional quick wins.

Time to Ready

Estimated deployment timeline based on finding complexity and phase allocation.

3–7 weeks

3-7 weeks | Based on 5 Phase 0 blockers and 26 Phase 1 findings. Assumes one dedicated resource working full-time on remediation.

Phase	Findings	Est. Hours	Timeline
Phase 0: 4-11 days	5	32–88	1–3 weeks
Phase 1: 10-23 days	26	80–184	2–5 weeks

Assumptions

- Based on 5 Phase 0 blockers and 26 Phase 1 findings. Assumes one dedicated resource working full-time on remediation.
- Phase 0 blockers must be resolved before Copilot licence provisioning.
- Timeline assumes dedicated IT resource availability during remediation.

Copilot Service Dependencies

2 of 6 capabilities ready or partially ready | Overall: Partially Ready

Capability	Status	Summary
Meeting Intelligence	At Risk	1 finding(s) require attention — Blocked by: Microsoft Teams
Document Drafting and Summarisation	Not Ready	2 critical finding(s) blocking this capability — Blocked by: SharePoint (Plan 2), Content-to-Label Coverage
Email Assistance	Partially Ready	Some key findings not yet assessed
Chat and Collaboration	At Risk	1 finding(s) require attention — Blocked by: Microsoft Teams
Security and Compliance Readiness	Not Ready	2 critical finding(s) blocking this capability — Blocked by: Defender for O365 P1, Content-to-Label Coverage
Power Platform Integration	Partially Ready	Some key findings not yet assessed

Overall Shadow AI Risk: LOW

6 GenAI apps discovered | 0 unsanctioned | 20 users | 0.6 GB traffic

Application	Trust	Users	Status	Last Seen
Google Gemini	7/10	9	Sanctioned	2026-05-07
GitHub Copilot	10/10	5	Sanctioned	2026-05-07
ChatGPT (Consumer & Enterprise)	9/10	3	Sanctioned	2026-05-06
DeepSeek	5/10	1	Untagged	2026-05-04
Microsoft Copilot	10/10	1	Sanctioned	2026-05-06
Grammarly	9/10	1	Sanctioned	2026-05-07

Risk breakdown: 0 high | 1 medium | 5 low

Phase 0: Resolve Before Copilot Rollout (1 of 2)

[Complex] Security Posture (Defender) — Copilot Data Governance

→ Resolve critical data governance gaps before allowing Copilot to access organisational data. DLP, sensitivity labels, and audit logging are essential for AI data protection.

[Moderate] Security Posture (Defender) — Copilot Security Posture

→ Resolve all critical security gaps before deploying Copilot. High-severity incidents and compromised users represent immediate threats to data accessed by AI assistants.

[Complex] Compliance & Governance (Purview) — Content-to-Label Coverage

→ Create sensitivity labels and DLP policies immediately to protect content before Copilot deployment.

[Complex] Compliance & Governance (Purview) — Copilot Data Exposure Surface

→ Deploy sensitivity labels immediately before any Copilot rollout. Minimum viable set: Public, General, Confidential, Highly Confidential. Enable auto-labelling policies targeting SharePoint. Configure DLP policies for Exchange, Teams, and SharePoint.

Phase 0: Resolve Before Copilot Rollout (2 of 2)

[Moderate] Identity & Access (Entra) — Copilot Licence–Security Baseline Alignment

→ Remediate security gaps for all Copilot-licensed users before deployment: enforce MFA registration, block Copilot access from non-compliant devices via Conditional Access, and investigate any risky user flags via Entra ID Protection.

Next Steps

1. Resolve 5 Phase 0 blockers before Copilot licence provisioning — these are critical pre-deployment requirements.

2. Prioritise Compliance & Governance (Purview) (57%) — lowest readiness score with 7 critical and 1 warning findings.

3. Address Identity & Access (Entra) (72%) — 8 findings requiring attention before full deployment.

4. Plan a phased pilot with the existing 1 Copilot-licensed users, then expand to the broader 58-user base.

5. Schedule a follow-up assessment in 30 days to track remediation progress and validate deployment readiness.

Contact JFDI Consulting for guidance on your Copilot deployment journey.