VIRTUELLE GROUP

MICROSOFT COMMERCIAL MARKETPLACE · PRODUCT INFORMATION DOCUMENT

Microsoft 365 Copilot Readiness Assessment

A structured, expert-led engagement to assess your Microsoft 365 environment and build the security foundations for a confident Copilot deployment.

ONE-OFF FIXED FEE	130+ SECURITY CHECKS	DELIVERED IN 5 BUSINESS DAYS	7 SECURITY DOMAINS

Virtuelle Group Pty Ltd · ABN 86 166 876 811
info@virtuellegroup.com.au · 1300 653 059 · virtuellegroup.com.au

DELIVERED WITHIN
5 Business Days

THE CHALLENGE

Copilot surfaces what your permissions already allow.

Microsoft 365 Copilot does not grant new permissions — it amplifies existing access instantly, at scale, across every document your users can already reach. Organisations that deploy Copilot without first hardening their environment are not adopting AI safely — they are exposing their entire M365 data estate to a highly capable retrieval engine with no guardrails.

Overshared Content Surfaced Instantly

Documents shared with "Everyone" or broad security groups become accessible to Copilot queries from any licensed user, regardless of business need.

Unlabelled Data Has No Protection

Without Microsoft Purview sensitivity labels, Copilot cannot apply data protection policies. Confidential content is indistinguishable from public content.

Ungoverned Agent Creation

By default, any Copilot-licensed user can build AI agents and share them org-wide. Without controls, agents can connect to sensitive data and distribute it at scale.

Weak Identity Amplified

A compromised account without MFA or PIM controls becomes exponentially more dangerous when paired with Copilot's ability to search, summarise, and generate from accessible content.

THE OFFER

What the Copilot Readiness Assessment delivers

Virtuelle Group's Copilot Readiness Assessment is a point-in-time, expert-led evaluation of your Microsoft 365 environment against 130+ Copilot security readiness controls across 7 security domains. You receive a branded findings report, a domain scorecard, and a prioritised remediation roadmap — all within 5 business days of engagement commencement.

130+	7	5	10+
SECURITY CHECKS	SECURITY DOMAINS	BUSINESS DAYS	YEARS IN M365 SECURITY

"The security work required before Copilot deployment is fundamentally about tightening the access model you should have had in place all along. Virtuelle Group makes that process structured, fast, and verifiable."

WHAT'S COVERED

Seven security domains. 130+ checks. Full coverage.

Virtuelle engineers run both automated and manual checks across your Microsoft 365 tenant. Automated tooling covers approximately 60% of all checks; manual portal verification and expert review covers the remaining 40%.

1 · Identity & Access Hardening

MFA enforcement via Conditional Access, Copilot-specific CA policies, legacy authentication blocking, Privileged Identity Management (PIM), AI Administrator role assignment, guest user audit, and device compliance policies.

2 · Data Governance & Information Protection

Sensitivity label taxonomy assessment, auto-labelling policy review, SharePoint Data Access Governance (DAG) oversharing reports, Restricted SharePoint Search (RSS) configuration, and DLP policy review for Copilot workloads.

3 · Compliance, Audit & Legal

Purview Audit Premium configuration, Copilot interaction log verification, retention policy review, Privacy Impact Assessment guidance, eDiscovery readiness, and DSPM for AI (Purview) setup review.

4 · Endpoint & Device Security

Intune compliance policy gap analysis, Microsoft Defender for Endpoint (MDE) deployment status review, and Attack Surface Reduction (ASR) rules review and enforcement assessment.

5 · Copilot Control System

CCS Readiness page review across Deployment Essentials, Data Security, and End-User Experience. Licence scoping, web search settings, Graph connector review, MDCA session policies, and self-service purchase controls.

6 · Copilot Agent Security & Governance

Full Agent Registry audit across Microsoft, partner, and creator-shared agents. Org-wide sharing restriction review, admin approval workflow assessment, Power Platform Managed Environments, Copilot Studio DLP policies, and agent knowledge source audit.

7 · People, Process & Change

Acceptable Use Policy review and AI/Copilot addendum guidance, incident response plan review for Copilot scenarios, and readiness review for pilot group deployment and phased rollout planning.

Assessment methodology

Checks are scored as **Pass**, **Partial**, or **Fail** across each domain, producing a domain-level scorecard. Findings are then prioritised as **Critical**, **High**, **Medium**, or **Low**, with each finding mapped to a

WHAT YOU RECEIVE

Deliverables

Deliverable	Description
Assessment Report	Branded, executive-ready PDF covering all 7 domains with Pass/Partial/Fail ratings and detailed findings narrative
Domain Scorecards	Visual scorecard per security domain showing overall readiness rating and check-level results
Prioritised Gap Analysis	All findings categorised as Critical, High, Medium, or Low with risk context for each
Remediation Plan	Structured remediation roadmap with recommended actions, ownership guidance, and suggested timelines
Findings Readout Session	Live stakeholder session walking through domain scorecards, critical gaps, and remediation priorities
Agent Registry Audit Summary	Inventory of all Microsoft, partner, and creator-shared agents currently active in your tenant

HOW IT'S DELIVERED

Delivery phases

1

DAYS 1–2

Discovery & Tenant Access

Virtuelle establishes delegated access to your Microsoft 365 tenant. Automated assessment tooling is run across all readiness domains, covering approximately 60% of total checks.

2

DAYS 2–4

Manual Verification & Portal Review

Virtuelle engineers complete manual portal checks, Agent Registry audit, licence review, and stakeholder briefing preparation. All 130+ checks are verified and scored.

3

DAY 5

Report Delivery & Readout Session

The completed assessment report is delivered to nominated stakeholders. A readout session walks through domain scorecards, critical findings, and the prioritised remediation plan.

WHO THIS IS FOR

Ideal customer profile

This assessment is designed for **IT leaders, security managers, and Microsoft 365 administrators** in mid-market and enterprise organisations who are planning or evaluating a Microsoft 365 Copilot deployment.

- ✓ Organisations planning a Microsoft 365 Copilot rollout in the next 3–12 months
- ✓ IT and security teams that want an independent, expert view of their Copilot readiness posture
- ✓ Organisations subject to Australian privacy or regulatory obligations (Privacy Act, APRA CPS 234, DISP)
- ✓ Microsoft 365 tenants with active E3, E5, or Business Premium licensing
- ✓ Organisations advised by Microsoft to address security posture before Copilot deployment

WAYS TO ENGAGE

Three engagement options — contact us to discuss the right fit

The Copilot Readiness Assessment is available as a standalone point-in-time assessment, a full remediation engagement, or an ongoing managed service. Contact Virtuelle Group to discuss which option best suits your environment and timeline.

THIS MARKETPLACE OFFER

Readiness Assessment

Point-in-time assessment with executive report and readout session. Delivered within 5 business days.

- ✓ 130+ checks across 7 domains
- ✓ Domain scorecard with Pass/ Partial/Fail
- ✓ Prioritised gap analysis
- ✓ Executive-ready report
- ✓ Remediation plan
- ✓ Findings readout session

Contact us for pricing →

UPGRADE OPTION

Readiness & Remediation

Full assessment plus hands-on remediation of all Critical and High findings. 6–10 week delivery.

- ✓ Everything in the Assessment
- ✓ MFA & Conditional Access hardening
- ✓ PIM for privileged roles
- ✓ Sensitivity label deployment
- ✓ SharePoint permission remediation
- ✓ Agent governance controls
- ✓ Pilot group go-live support

Contact us for pricing →

ONGOING SERVICE

Managed Copilot Security

Continuous monitoring, quarterly reviews, and agent governance post go-live. Monthly subscription.

- ✓ Everything in Assessment + Remediation
- ✓ Copilot monitoring via Sentinel
- ✓ Agent Registry monthly review
- ✓ DSPM for AI observability
- ✓ Quarterly security review & report
- ✓ Incident response for Copilot events
- ✓ 24/7 SOC access

Contact us for pricing →

WHY VIRTUELLE GROUP

Deep Microsoft Security Specialisation

Advanced certifications across Microsoft Defender XDR, Sentinel, Purview, and Entra ID — the exact stack that governs Copilot security.

Copilot-Specific Methodology

Proprietary 130+ check framework purpose-built for Copilot deployments — not a repurposed generic security assessment.

Agent Governance Leadership

We actively track the evolving Copilot agent landscape — Agent Registry controls, DSPM for AI, and Copilot Studio policy configuration.

Australian Compliance Focus

Assessments designed for organisations subject to the Privacy Act 1988, APRA CPS 234, DISP, and industry-specific frameworks.

- **Microsoft-Certified Partner**
- **Microsoft Security Specialisation**
- **24/7 Sentinel SOC**
- **Essential Eight Aligned**

Talk to us about your Copilot readiness.

Contact Virtuelle Group to discuss your environment, confirm scope, and get started within 5 business days.

1300 653 059
info@virtuellegroup.com.au
virtuellegroup.com.au