Unicorn IT Group

Cloud & Microsoft 365 Security Assessment Report

Configuration review of Azure AD, Microsoft 365 and cloud identity controls

Prepared for: Sample Professional Services

Date: 28 August 2026

Classification: CONFIDENTIAL

1300 904 635 | hello@uitg.com.au | www.uitg.com.au

Document Information

Document title	Sample Penetration Test Report
Version	1.0
Author	Unicorn IT Group Security Team
Classification	Confidential
Contact	hello@uitg.com.au | 1300 904 635

This is a sample report for demonstration purposes. Names, IP addresses and findings have been fictionalised.

Executive Summary

This sample report documents a cloud and Microsoft 365 security assessment. The most significant risk is a Global Administrator account without multi-factor authentication. A compromised privileged account would provide full access to email, files and identities. SharePoint oversharing and legacy authentication are also notable risks that should be addressed quickly.

Metric	Value
Test type	Cloud / Microsoft 365 security assessment
Targets	Azure AD, Microsoft 365 tenant, SharePoint and Exchange Online
Duration	4 business days
Critical findings	1
High findings	1
Medium findings	1
Low findings	1

Findings Overview

ID	Finding	Risk	Status
CLD-001	Global admin account without MFA	**Critical**	Open
CLD-002	Overly permissive SharePoint sharing	**High**	Open
CLD-003	Legacy authentication enabled	**Medium**	Open
CLD-004	Unmonitored Azure AD risky sign-ins	**Low**	Open

Detailed Findings

CLD-001 — Global admin account without MFA

Risk rating: Critical

Description

A Microsoft 365 Global Administrator account is protected only by a password. Compromise of this account would grant full control over email, identities and data.

Evidence

Microsoft Graph API enumeration showed perUser MFA state disabled for the account.

Recommendation

Require MFA for all privileged roles and use phishing-resistant authentication methods where possible.

CLD-002 — Overly permissive SharePoint sharing

Risk rating: High

Description

Multiple SharePoint sites allow anonymous guest links, and one site contains payroll spreadsheets shared with 'Anyone with the link'.

Evidence

Microsoft 365 audit log and SharePoint admin scan identified public links.

Recommendation

Disable anonymous sharing, review existing guest links and apply sensitivity labels.

CLD-003 — Legacy authentication enabled

Risk rating: Medium

Description

Basic authentication remains enabled for Exchange Online, allowing password-only attacks against email.

Evidence

Azure AD sign-in logs show successful basic-auth protocols in the last 30 days.

Recommendation

Block legacy authentication with Conditional Access policies.

CLD-004 — Unmonitored Azure AD risky sign-ins

Risk rating: Low

Description

Risky sign-in detections are not automatically reviewed or remediated.

Evidence

Identity Protection risky sign-ins report shows unconfirmed risky events older than 7 days.

Recommendation

Configure automated risk policies and alert routing to the IT team.

Scope & Methodology

Scope

- Azure AD identity configuration and Conditional Access policies
- Microsoft 365 tenant-wide security settings
- SharePoint and OneDrive sharing configuration
- Exchange Online and Teams security controls

Methodology

The assessment combined Microsoft Secure Score review, Azure AD and Graph API enumeration, manual configuration checks and policy analysis against the Microsoft 365 security baseline and Essential Eight.

Standards & Frameworks

- Microsoft 365 Security Baseline
- ACSC Essential Eight
- NIST SP 800-115
- CIS Microsoft 365 Benchmark

Remediation Tracker

ID	Action	Owner	Target
CLD-001	Require MFA for all privileged roles and use phishing-resistant authentication methods where possible.	IT Team	30 days
CLD-002	Disable anonymous sharing, review existing guest links and apply sensitivity labels.	IT Team	30 days
CLD-003	Block legacy authentication with Conditional Access policies.	IT Team	30 days
CLD-004	Configure automated risk policies and alert routing to the IT team.	IT Team	30 days

Unicorn IT Group can assist with remediation, re-testing and ongoing security management. Contact us at hello@uitg.com.au or 1300 904 635.