



Microsoft 365 Security Audit – Sample Overview Report

(Demo Version – No Customer Data)

Executive Summary

This example report shows the type of insights you receive when we carry out a full Microsoft 365 Security Audit. We assess your environment against **over 100 best practices**, industry benchmarks, and real world cyber threats affecting UK SMEs.

This sample does *not* include customer-specific data or detailed remediation steps. It is intended to demonstrate our methodology and the value of a full audit.

Audit Scope

Our assessment covers the following areas:

Identity & Access Management

- Admin account security
- Multifactor authentication
- Emergency access accounts
- User permissions & role separation

Device Management

- Device compliance
- Mobile & BYOD protection
- Encryption & update policies
- Firewall & antivirus configuration

Email & Collaboration Security

- SPF, DKIM, DMARC
- Safe links & antimalware policies
- Guest sharing & Teams permissions
- External collaboration controls

Data Protection & Governance

- Sensitivity labels
- Retention settings
- Information protection policies
- External sharing restrictions

Cloud Application & App Governance

- App permissions
- Third-party app controls
- Consent policies

Example of Audit Output

Overall Items Audited: 102

Passed: 15

Failed: 87

(Figures shown are for illustration only.)

Failure Priority Breakdown

We categorise every finding by severity:

- **High Priority:** Immediate security risk
- **Medium Priority:** Important improvements
- **Low Priority:** Recommended best practice

Example Breakdown:

- High: 21
- Medium: 46
- Low: 21

(This breakdown shows the format only — no customer data is included.)

Sample Page Layout – What You Receive

Each finding in a full audit includes:

- What We Checked
- Why It Matters
- Priority Level
- Whether Your License Covers the Fix
- High level recommendation

In this demo version, all remediation steps and customer-specific results have been removed.

Example Finding (Sanitized)

Audit Item: External File Sharing

What we check: Whether external sharing is appropriately restricted in OneDrive and SharePoint.

Why it matters: Unrestricted sharing can lead to accidental data exposure and unauthorised access to sensitive information.

Priority: High License **requirement:** Included in most Microsoft 365 plans

Audit Item: Multi Factor Authentication for Administrators

What we check: Whether privileged accounts are protected by strong MFA.

Why it matter's accounts are prime targets for attackers. MFA significantly reduces the risk of compromise.

Priority: High License **requirement:** May require elevated licensing depending on policy type

What the Full Report Contains That This Demo Doesn't

- Specific pass/fail results
- The detailed, step-by-step remediation guidance seen in your internal version
- CIS or NCSC references
- Licensing conflict details
- Screenshots
- Exact policy configurations

Want your own detailed audit?

We perform a full end-to-end security review and produce a personalised report with actionable steps tailored to your business.

Get in touch to arrange your 365-security audit

Tel: **01642 062510** Email: info@circlecloud.co.uk