Asceris Microsoft 365 Cyber Risk Assessment

The threat of business email compromise

Cyber criminals routinely compromise Microsoft 365 accounts to commit financial fraud and access confidential data

Attackers are continually finding new ways to exploit security gaps, from weak and stolen credentials to bypassing multi-factor authentication. Once threat actors gain entry, they can access and copy data, compromise new accounts, and attempt to steal funds. These attacks affect businesses of all sizes and industry sectors, and even well-protected businesses are at risk.

Assess the risk and target new controls

The Microsoft 365 Cyber Risk Assessment by Asceris uses proprietary technology to identify areas of risk and potential security controls

Our assessment leverages real-world incident analysis, industry best practice guidance, and advanced threat intelligence to evaluate environments and provide actionable recommendations to strengthen security posture and substantially reduce the risk of suffering a business email compromise attack.

A risk assessment that goes beyond the basic checks

Environment-level configuration

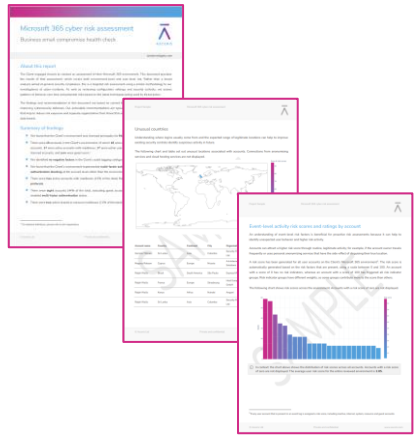
- User account and product license analysis
- Logging and audit settings
- MFA enforcement and authentication security
- Conditional Access and device compliance policies
- Admin role assignments and privilege separation
- Third-party app consent settings
- Microsoft Teams and SharePoint security settings

User-level configuration

- MFA enforcement
- Passwordless authentication
- Microsoft Authenticator settings
- Separation of admin and standard user accounts
- Shared and resource mailbox security

Unusual user activity

- Risk scoring for all accounts
- Recent logins from unusual countries
- Logins from cloud-hosting services
- Logins from VPNs and anonymous proxies
- Detection of suspicious mailbox rules and email forwarding
- Identification of risky consent grants and high-risk apps
- Authentication attempts from known malicious sources



The assessment delivers a **comprehensive report** covering **configuration**, recent **activity**, and key **recommendations**

Our accelerators

1 Comprehensive analysis
We review a wide range of configuration settings and analyse every account in the environment to identify unexpected activity

2 Continuous improvement
New checks are constantly added based on feedback from our clients and partners

3 Minimal permissions
Only a subset of admin permissions is required—no Global Admin needed

4 Smooth on-boarding
We gather initial on-boarding information via an online form, saving time and ensuring a smooth client experience

ASCERIS

Strengthen your Microsoft 365 security and prevent Business Email Compromise (BEC) attacks