e2e assure

M365 Security Review

Service Definition Document

M365 SECURITY REVIEW

Service Definition Document – G-Cloud 15

CONTENTS

SERVICE INTRODUCTION

Microsoft 365 (M365) is a core productivity platform for businesses of all types and size, due to its extensive feature set and cloud-based nature, this also makes it a prime target for cyber threats.

Misconfigurations, overly permissive access controls, inadequate logging, and inadequate security hygiene across key services—such as Entra ID (formerly Azure AD), Exchange Online, Microsoft Teams, and SharePoint Online—can expose organisations to risks including account takeovers, data leaks, and unauthorised access.

Under pressure security teams often struggle to continuously assess and improve their M365 security posture, potentially leaving critical gaps that threat actors can exploit.

SERVICE OVERVIEW

The e2e-assure M365 Security Review is a structured assessment designed to scrutinise, assess, and report on the security configurations of Entra ID, Exchange Online, Microsoft Teams, and SharePoint Online.

This review provides an in-depth analysis of security settings, access controls, detection capabilities, and potential risks across these services. The engagement delivers clear recommendations to strengthen security, improve compliance, and mitigate risks associated with misconfigured permissions, weak authentication policies, and insufficient monitoring.

SCOPE OF ACTIVITIES

The end-to-end review assignment will include the following actions and areas of assessment

Stage	Tasks
Initial Consultation	• Conduct a kick-off meeting to understand the client's security objectives, M365 environment, and compliance requirements. • Define the scope, identify key stakeholders, and establish access to necessary Microsoft 365 security tools.

Entra ID (Azure AD) Security Assessment	• Evaluate identity and access configurations, including:
	  ○ Multi-Factor Authentication (MFA) and Conditional Access policies
	  ○ Privileged identity management (PIM) & administrative role assignments
	  ○ Guest and external user access settings
	• Review sign-in logs and risk detection insights using Microsoft Entra ID Protection.
	• Analyse Entra ID Secure Score and recommend improvements.

Exchange Online Security Assessment	• Review email authentication & anti-phishing configurations, including:
	  ○ SPF, DKIM, DMARC settings
	  ○ Microsoft Defender for Office 365 policies (anti-spam, anti-malware, anti-phishing)
	  ○ Safe Links & Safe Attachments settings
	• Assess Mailbox auditing & access control policies.
	• Identify risks related to Business Email Compromise (BEC) and unauthorised mailbox forwarding.

Microsoft Teams Security Assessment	• Review external access and guest user settings. • Assess data loss prevention (DLP) and sensitivity label policies. • Evaluate Teams governance, including meeting & messaging policies. • Review Microsoft Defender for Office 365's Teams security monitoring settings.
SharePoint Online Security Assessment	• Audit external sharing and anonymous link configurations. • Assess data access policies and security controls for sensitive content. • Review conditional access policies for document access and collaboration. • Analyse SharePoint activity logs for signs of unauthorised data access.
Microsoft Secure Score Review & Hardening Plan	• Analyse the Microsoft Secure Score across Entra ID, Exchange Online, Teams, and SharePoint.

Stage	Tasks
	• Identify areas for security enhancement and prioritised action items. • Compare against industry best practices and compliance frameworks (e.g., NIST, CIS M365 Benchmark).

Reporting & Recommendations	• Detailed findings covering misconfigurations, security gaps, and risk exposure across all reviewed services.
	• Prioritised recommendations for risk reduction and security improvements.
	• Strategic roadmap to implement best practices, including:
	  ○ Immediate remediation actions
	  ○ Medium-term security enhancements
	  ○ Long-term security posture improvements

Presentation & Knowledge Transfer	• Conduct an executive briefing summarising key findings and recommendations. • Provide a technical deep dive session for IT/security teams on next steps. • Offer guidance on implementing recommended security changes.

SCOPE OF DELIVERABLES

The following tangible outputs will be provided as part of the Report and Knowledge transfer stages:

Output	Description
M365 Security Review Report	• In-depth security assessment of Entra ID, Exchange Online, Microsoft Teams, and SharePoint. • Identification of security weaknesses, misconfigurations, and high-risk areas. • Mapped findings to industry best practices and Microsoft Secure Score recommendations.
Executive Summary Report	• A high-level overview of security gaps and recommendations, tailored for CISOs, IT Directors, and Security Leadership.
Security Hardening Roadmap	• Step-by-step plan to implement security enhancements. • Quick wins, medium-term actions, and long-term improvements.

SERVICE OUTCOMES

- Gain a comprehensive understanding of current Microsoft collaboration tools security configuration strengths and weaknesses.
- Enhance detection and response capabilities against M365-based threats.
- Reduce the risk of account takeovers and business email compromise incidents.
- Improved Data Security with stronger access control, external sharing restrictions, and secure collaboration policies.
- Alignment with Industry Standards, improving compliance and governance posture.