Fortis INFORMATION SECURITY & RISK MANAGEMENT

CREST PEN TEST

Microsoft 365 Security Configuration Audit

Microsoft 365 is an invaluable corporate tool; however, configuring it securely can be time-consuming and complicated, leaving organisations open to attack.

A Microsoft 365 Security Configuration Audit systematically assesses the security settings and configuration of an organisation's Microsoft 365 environment to pinpoint vulnerabilities and identify misconfigurations. The outputs from the audit then enable organisations to address gaps and optimise their controls to protect against cyber threats and data breaches.

What are the benefits?

A Microsoft 365 Security Configuration Audit is essential for organisations looking to enhance the security, compliance, and resilience of their Microsoft 365 environment in the face of evolving cyber threats and regulatory requirements. Specific benefits include:

- Robust controls & enhanced security posture to protect sensitive & business critical data
- Mitigate risk by identifying gaps and vulnerabilities that could be open to exploitation
- Maintain compliance with regulatory & legal requirements e.g. GDPR, PCI, HIPAA, or SOC 2
- Reduce administrative burden by streamlining or automating security configurations
- Build stakeholder confidence through the organisation's commitment to protecting data
- Improve incident response capabilities within the Microsoft 365 environment
- Fine tune configurations to protect against advanced threats e.g. sophisticated phishing & ransomware

Audit Overview

The audit process involves reviewing existing configurations; comparing them against security best practices and industry standards, such as the Centre for Information Security Benchmark (developed in partnership with Microsoft) and Critical Security Controls; identifying any misconfigurations or weaknesses; and providing recommendations for remediation.

The Fortis Cyber® M365 Security Configuration Audit is a comprehensive assessment of an organisation's Microsoft 365 environment that typically includes but is not limited to:

- User access controls and permissions
- Email security configuration
- Service hardening
- Microsoft Teams sites and activity
- Activity reports and alerts for suspicious activity
- External apps with access to accounts
- Audit logging and monitoring configurations for detecting and responding to security incidents
- Mobile device management (MDM) and mobile application management (MAM) configuration
- Data protection measures such as encryption and data loss prevention (DLP) policies
- Compliance settings to ensure adherence to regulatory requirements

www.fortiscyber.co.uk
enquiries@fortiscyber.co.uk
+44 (0)207 898 3971

Engagement Structure

Preparation:

- Define the scope, including which components of the Microsoft 365 tenant will be audited e.g. SharePoint, Teams, Azure Active Directory
- Identify objectives, including compliance requirements, security best practices, and specific concerns or risks
- Gather relevant documentation e.g. security policies, access controls and configurations
- Obtain necessary permissions to access the Microsoft 365 tenant with “Global Reader” privileges

Discovery:

- Conduct an inventory of Microsoft 365 assets and configurations
- Identify all user accounts, groups, roles, and permissions
- Document existing security settings and configurations across Microsoft 365 services
- Review security-related logs and reports to gain insights into past security incidents or anomalies

Analysis:

- Evaluate the effectiveness of existing security measures against security best practices, industry standards, and regulatory requirements
- Identify misconfigurations, vulnerabilities, or gaps in security controls
- Assess the impact of identified issues on the organisation's overall security posture and compliance status
- Prioritise findings based on the level of risk and potential impact on security

Reporting:

- Record the findings of the audit, including identified issues and associated risks
- Document remediation options to address vulnerabilities and strengthen the security posture of the Microsoft 365 environment, including recommendations for further improvement
- Present the audit report to relevant stakeholders

Once the client has implemented all the remediation advice and recommendations for improvement, such as deploying security updates, patches, or additional security solutions, Fortis Cyber® can then perform a final re-test if required.

Validation:

- Verify that remediation measures have been successfully implemented and address identified security issues
- Conduct tests to confirm security configurations are functioning as intended
- Review audit logs and reports to ensure security controls are effectively mitigating risks and protecting against threats

Fortis Cyber® CREST Accreditation

Fortis Cyber® is a CREST accredited Penetration Testing company. Through CREST’s demanding accreditation process, organisations buying security testing services get the assurance that:

- The services will be delivered by trusted companies with best practice policies and procedures.
- The work will be conducted by highly qualified individuals with up-to-date knowledge, skills, and competence to deal with all the latest vulnerabilities and techniques used by real attackers.
- Both the company assessments and individual qualifications are underpinned by meaningful and enforceable codes of conduct.