Microsoft Security Assessment

Organisations across the globe are undertaking Digital Transformation initiatives to enhance their internal and external operations, and are doing so by leveraging cloud technologies such as Office 365 and Microsoft Azure. Security in the cloud is a shared responsibility. Microsoft, as the cloud provider, and you, the customer, both bear the responsibility of securing your data in the cloud. Understanding your responsibilities, as well as the security capabilities that are available in O365 and Microsoft Azure, are key requirements to successfully fulfilling this responsibility.

Why do you need the Microsoft Security Assessment?

Whether you have just decided to move to the Microsoft Cloud, or are already fully deployed, conducting a Security Assessment can identify potential security gaps in your current environment and reveal new security features, capabilities and industry standard practices that may have been recently added to the O365 service. This offering enables your organisation to confidently secure your cloud platform by defining security responsibilities, identifying potential security gaps and providing recommendations to improve security posture.

What is the Microsoft Security Assessment?

The Cloud Collective Microsoft Security Assessment is a security review performed in accordance with industry best practices that includes recommendations to improve your security posture and to address security issues that are discovered as part of this review.

AS PART OF THE ASSESSMENT, OUR CONSULTANT WILL ADDRESS ELEMENTS SUCH AS:

- How your organisation is using O365 and Azure from a business perspective;
- High level understanding of your documents and their sensitivity;
- Your security posture and security scorecard;
- Current and future security and productivity goals; and
- Relevant threat scenarios applicable to your business.

How do we do it?

The assessment is prepared by a Microsoft Cloud certified senior consultant with a deep understanding of cloud and on-premises security technologies and the newest Microsoft technologies.

KEY ACTIVITIES

- A security assessment calculated by the Microsoft Security Scorecard
- A vulnerability analysis and evaluation of level of risk based on industry statistics;
- Security control and best practice recommendations based on the assessment;
- Recommendations to address vulnerabilities, security weaknesses, or other security related issues discovered during the assessment;
- Recommendations on how to secure your Microsoft Cloud investments.

MAPA 2017

Microsoft Australia Partner Awards
Celebrating Excellence | Winner
A Cloud for Good Award

CLOUD collective
© 2018 Cloud Collective   www.cloudcollective.com.au

Microsoft Security Assessment

Our Process

Identify & define scope for the security assessment	Review existing security documentation	Gather security assessments data using automated tools
Review prior risk assessments to assess progress towards implementing management actions	Construct a view into the organisation's current security posture, with potential security gaps identified	Synthesise data gathered into a management report of prioritised findings, recommendations and industry standard guidance

What do you get?

- Documented Security Assessment Work Plan, with steps, tools and procedures used to conduct the assessment.

- Management Report containing current security posture, potential security gaps, prioritised findings, as well as recommendations and industry standard guidance.

Audience

This service is designed for your organisation's IT staff, Information Security team and Internal Audit team, who have direct involvement and understanding of the organisation's security and compliance requirements, as it relates to he Microsoft Cloud.

Estimated Effort

4 - 5 days. Final Statement of Work details will be mutually agreed upon by the Client and the Cloud Collective.

Technical Aspects

Understand how Microsoft helps protect you against spoof, phish, malware, and spam emails and gain visibility and control with Enterprise Mobility + Security

- Data Loss Prevention (DLP)
- Multi-Factor Authentication (MFA)
- Azure Information Protection (AIP)
- Conditional Access
- Azure Security Center
- Data encryption & protection
- Advanced Threat Protection (ATP)
- Windows Defender Advanced Threat Protection (WDATP)
- Cloud App Security
- Privileged Identity Management
- Mobile Device Management (MDM)
- Mobile Applications Management (MAM)

Microsoft Security Assessment Workshop (5 days at $9,200.00 (ex))

Final statement of work details will be mutually agreed between the client and the Cloud Collective.