|  |
| --- |
| Microsoft Logo |
| Microsoft Security Assessment  Customer Questionnaire |
| v2.0 - July 2019 |

Table of Contents

[Introduction 2](#_Toc17357904)

[Audience 2](#_Toc17357905)

[Overview 3](#_Toc17357906)

[Questionnaire 4](#_Toc17357907)

[Organization Essentials 4](#_Toc17357908)

[Microsoft 365 Considerations 5](#_Toc17357909)

[Cloud Security Objectives and Requirements 7](#_Toc17357910)

[Identity Access and Management 8](#_Toc17357911)

[Information Protection 9](#_Toc17357912)

[Exploit Mitigation 11](#_Toc17357913)

[Business Continuity / Disaster Recovery (BC/DR) 13](#_Toc17357914)

[Securing Privileged Access 14](#_Toc17357915)

[Outsourcing 16](#_Toc17357916)

[Attack Surface Reduction 17](#_Toc17357917)

[End User Education 18](#_Toc17357918)

[Microsoft 365 Security Readiness 19](#_Toc17357919)

[Windows 10 Client Security Readiness 20](#_Toc17357920)

[Mobile Device Security Readiness 20](#_Toc17357921)

Version History

|  |  |  |
| --- | --- | --- |
| Version | Changes | Date |
| 1.0 | Initial Release | 31-Mar-2017 |
| 1.1 | Minor fixes | 16-Jun-2017 |
| 1.2 | Updated questionnaire to cover Microsoft 365 | 01-Jul-2018 |
| 1.3 | Minor tweaks | 31-Oct-2018 |
| 2.0 | Minor tweaks | 01-Jul-2019 |

Disclaimer

© 2019 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. Microsoft 365 customers and partners may copy, use and share these materials for planning, deployment and operation of Microsoft 365 features.

We look forward to your feedback!

|  |  |
| --- | --- |
|  | Thank you for your continued trust and partnership. The resources within this toolkit will be iteratively improved upon based on product releases as well as direct feedback from delivered engagements. We encourage you to provide feedback to help us improve our products and toolkits. Please use the feedback process available through following web site: <http://aka.ms/securityassessmentfeedback> |

# Introduction

Before beginning the on-site workshop delivered as part of the Microsoft Security Assessment engagement, we will use this questionnaire to get a better understanding of your security objectives and requirements, cloud usage and adoption, regulations, and frameworks as well as the identification of any dependencies.

## Audience

Completion of the questionnaire typically requires input from several project team members. Depending on company structure, the following roles are typical participants in completing the questionnaire. The same team members that participate in completing the questionnaire should be expected to participate in the questionnaire review, which will take place during the on-site workshops.

* Executive Sponsor/Stakeholder
* Project Manager
* Security Lead/Architect
* Security Engineer/Consultant
* Cloud and infrastructure Engineer/Consultant
* Client/Endpoint Architect/Consultant/Engineer

## Overview

The questionnaire is broken down into sections and will be reviewed during the on-site workshop. The questionnaire should be completed prior to the on-site workshop taking place.

**Important.**

Information deemed to be sensitive in nature can be shared as part of the on-site assessment workshops instead of being documented within this questionnaire. In addition, it’s highly recommended to share the completed questionnaire over a secure connection.

# Questionnaire

This section contains document details related to the company essentials, existing production environment, and highlight known deployment blockers.

Organization Essentials

Please provide the essential organization information, in the following table.

*Table 2 – Organization essentials*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| Name |  |  |
| Based in (Country of HQ) |  |  |
| Number of Users per country/region | 🞎 Australia:  🞎 Canada:  🞎 France:  🞎 Germany:  🞎 India:  🞎 Japan:  🞎 South Korea:  🞎 UK:  🞎 North America:  🞎 Rest of Americas:  🞎 Rest of EMEA:  🞎 Rest of Asia Pacific: |  |
| Short summary of Organization profile (history, goods/services company produce) |  |  |
| Has Premier account | 🞎 Yes  🞎 No |  |
| What is the success criteria for this engagement? |  |  |
| Are there any concerns within the organization about moving to the cloud? If so, what are those concerns? |  |  |

Microsoft 365 Considerations

Please provide information about the Microsoft 365 implementation.

*Table 3 – Microsoft 365 considerations*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| What are the key business goals that the organization is looking to achieve with the deployment of Microsoft 365? |  |  |
| Is Skype for Business deployed? | Yes, Office 365  Yes, Online, Dedicated (MS)  Yes, Hosted, Dedicated (3rd party)  Yes, Hosted, Shared (3rd party)  Yes, On Premises  Yes, Hybrid (with Office 365)  No, other |  |
| Is Exchange deployed? | Yes, Office 365  Yes, Online, Dedicated (MS)  Yes, Hosted, Dedicated (3rd party)  Yes, Hosted, Shared (3rd party)  Yes, On Premises  Yes, Hybrid (with Office 365)  No, other |  |
| Is SharePoint deployed? | Yes, Office 365  Yes, Online, Dedicated (MS)  Yes, Hosted, Dedicated (3rd party)  Yes, Hosted, Shared (3rd party)  Yes, On Premises  Yes, Hybrid (with Office 365)  No, other |  |
| Is Teams deployed? | Yes  No |  |
| What Microsoft Security products have been deployed/enabled? Please add any planned deployments in the comments field. | Exchange Online Protection  Office 365 Advanced Threat Protection  Office 365 Cloud App Security  Office 365 Data Loss Prevention  Office 365 Advanced eDiscovery  Office 365 Threat Intelligence  Microsoft Cloud App Security  Microsoft Intune  Azure AD Premium  Microsoft Advanced Threat Analytics  Azure Rights Management / Azure Information Protection  Windows Defender Advanced Threat Protection  Azure Advanced Threat Protection  Azure Security Center |  |
| What types of devices do you have within your organization? | Windows 10 desktops and laptops  Windows 8 desktops and laptops  Windows 7 desktops and laptops  Windows Phone devices  Apple macOS desktops and laptops  Apple IOS devices  Google Android devices |  |
| Are there any major changes planned for the Microsoft 365 implementation? If so, please add the change and expected timeline. |  |  |
| Are there any specific security concerns for the current Microsoft 365 implementation? |  |  |
| What type and number of licenses do you currently hold? | Office 365 ProPlus  Office 365  Enterprise E1  Office 365  Enterprise E3  Office 365  Enterprise E5  Microsoft 365 Business  Microsoft 365 E3  Microsoft 365 E5  Microsoft 365 E5 Security  Microsoft 365 E5 Compliance  Microsoft 365 Education A3  Microsoft 365 Education A5 |  |
| Are you currently using a Security Information and Event Management (SIEM) tool? If so, Which tool and have you integrated this with any Microsoft products? |  |  |

Cloud Security Objectives and Requirements

Please provide information about the cloud security objectives and requirements.

*Table 4 – Cloud security objectives and requirements*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| What are the top security challenges you are facing with cloud deployment and usage? | Sophisticated and persistent attacks directed to your organization  No strategy on how to holistically secure cloud resources  Ability to identify and track compromised user identities  Lack of controls over access to SaaS Applications, Devices, and Corporate data  Security / data protectability to work on both on-premises and cloud environment with similar tools (hybrid solution)  Other, please specify |  |
| Please list other relevant cloud related security concerns. |  |  |
| Do you have to meet any specific compliance obligations including laws, regulations, and standards? If so, which ones? Examples, HIPAA, GDPR and PCI DSS etc. |  |  |
| Have you implemented any security control frameworks such as COBIT, ISO 270001 and/or NIST 800-53? If so, which ones? |  |  |

Identity Access and Management

Please provide information about identity access and management and strategies.

*Table 5 – Identity access and management*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| What are your security concerns on password usage and management? |  |  |
| What form of authentication/authorization have you configured? | Password Hash Sync  Pass-through Authentication  Pass-through Authentication with Password Hash Sync  Federation using ADFS  Federation using ADFS with Password Hash Sync  Other, please specify |  |
| Do you use single sign-on for on-premises and cloud applications? |  |  |
| Do you leverage a Multi-Factor Authentication (MFA) today? If so, have you enabled MFA for administrators only or for all users? |  |  |
| What type of Multi-Factor Authentication solution have you implemented? If you are planning to implement a Multi-Factor solution, which one are you likely to implement? | FIDO2 security key  Biometric verification  Mobile app  Phone call  SMS Text  Smart Card  Other, please specify in comment field |  |
| Do you have a password/pin policy in place for computers which requires users to use strong passwords/pins? |  |  |
| Do you have a password/pin policy in place for mobile devices such as phones and tablets which requires users to use strong passwords/pins? |  |  |
| Where do you primarily store user credentials (passwords, identity and account information) to provide access to applications and data? | On-premises Directory  Cloud Directory  On-premises and Cloud Directory  Other, please specify |  |
| Are you able to control access to applications and data based on conditions such as user location or whether the user device is managed or unmanaged? |  |  |

Information Protection

Please provide information about information protection strategy and deployments.

*Table 6 – Information protection*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| Do you have security controls to prevent accidental corporate-data leakage such as copying & pasting to external SaaS application? |  |  |
| Do you share confidential information with corporate partners? |  |  |
| Do you share confidential information with your customers? |  |  |
| Are you leveraging any type of secure data sharing solution today? if yes, which solution? |  |  |
| Are you using a Rights Management solution? If yes, which solution? |  |  |
| Do you currently classify and label data, ensuring that more sensitive data can be protected with better controls? |  |  |
| What is your Encryption Key requirement for SaaS applications? | Use provider encryption key  Own and use your own encryption key |  |
| Do you have critical assets inside mobile devices, including BYOD? |  |  |
| What measures do you have in place to address data loss on lost devices? |  |  |
| Do you have a solution in place which allows you to control and revoke access to company data and application on personal devices? |  |  |
| Do you have a solution in place which can help prevent accidental sharing of sensitive information? |  |  |
| Are you able to automatically identify sensitive information across your organization? |  |  |

Exploit Mitigation

Please provide information about exploit mitigation.

*Table 7 – Exploit Mitigation Table*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| How long does it take to deploy critical security updates to all (99%+) Windows operating systems? | 🞎 4 days or less  🞎 5-30 days  🞎 30+ days  🞎 Never |  |
| How long does it take to deploy critical security updates to all (99%+) deployed software? (operating systems, applications, middleware, routers/switches/devices, etc.) | 🞎 4 days or less  🞎 5-30 days  🞎 30+ days  🞎 Never |  |
| What strategy do you use to mitigate risk of Windows operating systems that cannot be updated and patched? | 🞎 We fully isolate computers from the intranet on dedicated network(s)  🞎 We upgrade or retire systems as they reach end of life  🞎 None of the above |  |
| What is your strategy on staying current with technology | 🞎 We adopt Cloud Services for workloads when available  🞎 We upgrade to the latest desktops operating systems and applications to protect against modern threats (currently deployed or actively deploying Windows 10 and Office 365 Pro Plus)  🞎 We upgrade to the latest server operating systems to protect against modern threats (currently deployed or actively deploying Windows Server 2016)  🞎 We regularly and consistently upgrade to the latest revisions of other operating systems (Mobile Devices, Mac OSX, Linux, and Router/Switch/Devices)  🞎 None of the above |  |
| What is your antimalware solution to protect endpoints? (vendor/products) |  |  |
| What is your current defense against Advanced Persistent Threats (APT)? |  |  |
| What is your Endpoint Detection and Response Solution? |  |  |
| Have you implemented a solution to manage and control SaaS applications? including:   * Cloud applications discovery (Shadow IT) * Data control * Threat detection and protection   If so, which solution? |  |  |
| Do you use any application whitelisting solution?  (list of applications and components like libraries, configuration files, etc. that are authorized to be present or active on a host according to a well-defined baseline) |  |  |

Business Continuity / Disaster Recovery (BC/DR)

Please provide information about Business Continuity and Disaster Recovery.

*Table 8 – Business Continuity / Disaster Recovery table*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| Which of the following is true about your disaster recovery program?  Select all that apply. | 🞎 All critical dependencies, and data are backed up automatically on a regular cadence  🞎 Backups are protected against online deletion with multi-factor authentication or a fully offline copy of backups  🞎 Backup files are validated regularly using standard restore procedures  🞎 We regularly conduct business continuity / disaster recovery exercises that includes a “complete IT system down” scenario (including online copies of BC/DR guidance/procedures)  🞎 We use a cloud based recovery services like Azure Site Recovery  🞎 None of the above |  |
| Do you identify and classify data in your organization and apply controls based on their relative importance to your business? |  |  |
| Is there an identifiable person or team responsible for data protection matters? |  |  |
| Do you have a backup solution in place? (If Yes, please specify vendor and product names) |  |  |
| Do you have documented backup and restore strategy and procedures? |  |  |
| Does your backup solution include offline backups? |  |  |
| Does your backup solution include Offsite backups, and if yes, is it with a public cloud provides? (Please specify Vendor/solution) |  |  |
| Is there an identifiable person or team responsible for data backup and recovery plans? |  |  |
| Do you have training in place for those responsible for performing the backups and recovery plans?  and for the users who may need to access the backups? |  |  |
| Do you periodically audit system backups and recovery controls in your organization? (for example, if backups are performed in accordance with policies, procedures, and best practice. If restoration tests have been performed, etc.) |  |  |
| Do security controls or procedures include measures to safeguard the physical  security of the data environment? |  |  |
| Do you have policies in place to prevent delete/overwrite of online archives by your administrator accounts? |  |  |

Securing Privileged Access

Please provide information about lateral traversal and securing privileged access.

*Table 9 –Securing Privileged Access table*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| Which of the following measures have you implemented to mitigate against credential theft attacks? | 🞎 All workstations have unique local administrator password  🞎 All servers have a unique local administrator account password  🞎 Only local accounts with random passwords are ever enabled  🞎 None of the above |  |
| Which of the following measures have you implemented to protect privileged accounts and credentials against credential theft attacks? | 🞎 Create separate accounts for privilege activities (vs. standard account for email/browsing/etc.)  🞎 Enforce multi-factor authentication on all privileged accounts  🞎 All privileged users are prevented from using e-mail and browsing the internet  🞎 Restrict Tier 0 (http://aka.ms/tier0) privileged accounts to only logon on Tier 0 servers and trusted workstations (such as PAWs. http://aka.ms/cyberpaw)  🞎 None of the above |  |
| Which of the following risk mitigation measures have you implemented to protect Tier 0 assets (Domain Controllers, Domain Administrators) in your environment? | 🞎 Privileges are requested and assigned when needed using a “just-in-time” system and automatically revoked after certain time  🞎 We use Just Enough Admin (JEA) to perform domain controller maintenance tasks without exposing Domain Admin equivalent (Tier 0) credentials  🞎 We minimize privileged credentials by regularly receiving a list of all accounts with Domain administrator or equivalent (Tier 0) permissions (including service accounts) – http://aka.ms/tier0  🞎 We minimize attack surface of domain controllers by restricting which management and security agents are installed on them  🞎 None of the above |  |
| Do you enforce separation of Administrative privileges and duties?  (by restricting what Admins can control and where they can log on - for instance see: [Active Directory administrative tier model](https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material#ADATM_BM)) |  |  |
| Do you periodically review administrative privileges to determine which personnel still have a legitimate business need for administrative access? |  |  |
| Do you have policies in place to enforce and verify that Admins don’t use privileged user accounts to perform high-risk activities such as Internet browsing? |  |  |
| Do you implement dedicated physical hardened workstations for sensitive Admin tasks? Or any other alternate approach (like privilege management solutions, Admin VMs, etc.) |  |  |
| Do administrators receive formal training on their role in managing the security risk, at least yearly? |  |  |

Outsourcing

Please provide information about outsourcing.

*Table 10 – Outsourcing*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| Which of the following is true with regards to your partners, vendors and outsources? | 🞎 Our outsourcing contracts are aligned with our security requirements (e.g. SLAs for emergency patching, protection controls for privileged accounts, etc.)  🞎 We validate vendors in supply chain using Security Development Lifecycle (SDL) to maintain and improve security of their products  🞎 We validate vendors protect their infrastructure from intrusion by applying regular security updates and getting critical mitigations in place  🞎 We validate vendors have appropriate detection controls in place to detect compromise  🞎 We validate vendor supply chain strategy (4th party risk)  🞎 None of the above |  |

Attack Surface Reduction

Please provide information about attack surface reduction.

*Table 11 – Attack Surface Reduction*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| Which measures have you deployed to protect your environment from malware? | 🞎 We deploy anti-malware software on all endpoints and regularly validate signatures updates are healthy  🞎 Our anti-malware software gets real-time blocking responses from a cloud service  🞎 We filter inbound e-mail for spam, viruses, malware and phishing attacks  🞎 We use sandbox detection / detonation chamber technology to protect against unknown malware attachments and URLs  🞎 We have enabled cloud based protection from malicious websites in our web browsers (e.g. Windows Defender Smartscreen in Microsoft Edge)  🞎 None of the above |  |
| We reduce enterprise attack surface by disabling support for the following legacy protocols | 🞎 Server Message Block v1 (SMBv1)  🞎 LanMan (LM) authentication  🞎 NTLMv1 authentication (including service accounts) – http://aka.ms/tier0  🞎 None of the above |  |
| How do you manage risk from excessive permissions to unstructured data (files on Fileshares, SharePoint, etc.)? | 🞎 We have set policy and performed enterprise discovery and analysis of permissions (once)  🞎 We have set policy and continuously monitor permissions for policy violations  🞎 We have set policy and regularly perform enterprise discovery and analysis of permissions  🞎 We have set policy but do not actively monitor  🞎 None of the above |  |

End User Education

Please provide information about end user security readiness.

*Table 12 – End User Education*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| Does a security awareness program exist?  If yes, what percentage of employees has participated in the security awareness program? |  |  |
| What was the date of the last awareness campaign? |  |  |
| Are communications regarding information security requirements distributed to employees and contractors? |  |  |
| Do you educate users on how to create strong passwords? |  |  |
| Do you educate users on how to detect and respond to phishing emails? |  |  |
| Do you train users to protect sensitive information using Rights Management Services? |  |  |

Microsoft 365 Security Readiness

Please provide information about Microsoft 365 security readiness.

*Table 13 – Microsoft 365 Security Readiness*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| What are the Microsoft 365 security capabilities you are most interested in from a readiness perspective? | Email Protection  Data Loss Prevention  SaaS application controls including Shadow IT discovery  Threat detection and reporting  eDiscovery  Digital Rights Management  Mobile and Client Management |  |
| Do you feel that your security staff has adequate training to deploy and manage Microsoft 365 security controls? If not, please list specific areas where additional readiness will help. |  |  |

Windows 10 Client Security Readiness

Please provide information about Windows 10 Client security readiness.

*Table 14 – Org platform strategy/possible issues*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| Are you using a device management service for your Windows clients? (Please specify Vendor/solution) |  |  |
| Do you use device health attestation features with Windows 10? |  |  |
| Use Secure Boot for UEFI/TPM validation of OS boot file integrity? |  |  |
| What Windows 10 security controls have you enabled/implemented? | Microsoft Defender ATP  Windows Defender Antivirus  Windows Defender Exploit Guard  Windows Defender Credential Guard  Windows Defender Application Control  Windows Defender SmartScreen  Windows Firewall  AppLocker  BitLocker  Windows Hello (including Windows Hello for Business) |  |

Mobile Device Security Readiness

Please provide information about Mobile Device security readiness.

*Table 15 – Org platform strategy/possible issues*

|  |  |  |
| --- | --- | --- |
| Question | Answer | Comment |
| Are you using a mobile device management service? (Please specify Vendor/solution) |  |  |
| Do you require mobile devices to block access and report policy violations? |  |  |
| Do you enforce management of user’s email profile? |  |  |
| Do you require mobile devices to be kept up-to-date? |  |  |
| Do you require mobile devices to have anti-virus and firewalls enabled? |  |  |
| Do you require mobile devices to use encryption? |  |  |
| Do you require mobile devices to lock on inactivity? |  |  |
| Do you require mobile devices to wipe on multiple failed sign-ins? |  |  |
| Do you allow jail broken or rooted mobile devices to connect to your applications and data? |  |  |