Microsoft Office 365 Assessment

By Smart Profiler

Version 6.2

ABC Consulting Group

Assessment date: 12-03-2023

Phone: +1 90999 990909

Direct: +1 98988 998989

Email: Nirmal@ABCConsulting.com

Project: Security & Compliance Status for Office 365
Effective Date: 12-03-2023
Customer: ABC Corporation
Office 365 Tenant: [Office-365-Tenant]
Domain: [Office-365-Tenant-Domain]

1. Introduction

This Introduction contains a global summary of security and compliance scans performed on the company infrastructure with SmartProfiler for ***Office 365 and Its services***. Detailed information about the scans can be found in the Technical Findings and other sections of this report.

The scans reflect a quick analysis and overall risk and compliance assessment program. The findings expressed through a Maturity Model construction provide a highlevel rating. This report is not meant to be a detailed control review. However, it is intended to provide an overall review of the aspects of the organization's risk assessment program in an all-up approach to determine whether it is aware of the risks and compliance issues revealed by **SmartProfiler**. SmartProfiler is capable of performing Risks and Compliance maintained by CIS Benchmark. CIS Microsoft 365 Foundations Benchmark provides prescriptive guidance for establishing a secure baseline configuration for Microsoft 365. Read more about CIS Benchmark for Office 365 foundation at https://www.cisecurity.org/benchmark/microsoft_365.

2. Organization Overview

During the creation of this report, the following summary information was gathered.

ORGANIZATION	
CUSTOMER NAME	ABC Corporation
CUSTOMER ADDRESS	51 SM Lane, ST, New, USA
CUSTOMER OPERATION BRANCHES	Canada, UK,USA
NUMBER OF EMPLOYEES	12900

3. Participants

During the creation of this report, the following summary information was gathered.

PARTICIPANT NAMES	COMPANY	PROJECT ROLE
NIRMAL K RATAWA	ABC Consulting	{enter Participant Project Role here}
{ENTER PARTICIPANT NAME HERE}	{enter Participant Company here}	{enter Participant Project Role here}
{ENTER PARTICIPANT NAME HERE}	ABC Consulting	{enter Participant Project Role here}

4. Recommendations

Organizations should be proactive in avoiding the risks and health issues associated with ***Office 365 and its services*** by establishing policies around securing and maintaining the IT environment. It is critical that an organization's plan include protocols governing cybersecurity and how it's managed relative to the amount of risk an organization is comfortable in assuming (since there is no such thing as zero risk).

Because the mitigation of cybersecurity risks and management of the threats is so challenging and can pose such a significant threat to an organization, IT security is a top-level strategic issue requiring executive leadership participation as stakeholders in the process.

- Senior Management must support and enforce establishment of Security Policies. Policies allow for standards to be mandated resulting in guidelines and procedures that will ultimately decrease risk to the organization.
- A Patch Management policy needs to be created and supported by upper level management to provide a more consistent monthly patching process for all ABC Corporation's Internal Networks. This will decrease risk within the organization.
- The IT department's use of a firewall, email encryption, anti-malware application and a Mobile Device Management system demonstrate a desire to secure and control the environment. However, significantly more technical controls and security awareness training are needed to combat the high level of risk within the organization and to prevent future security incidents and breaches.
- All of the security compliance and risk items must be reviewed carefully in the **Office 365 Compliance & Risks** section and actions to be taken accordingly.

5. Issues Services-Wise

The SmartProfiler software product was used to perform a complete health & security assessment of ***Office 365 Subscription*** of customer. The finiding helps you know the current health status and critical, high and medium issues that have been uncovered. The finding also provides recommendations to fix the issues. Though the report does not contain affected objects, it helps you know the overall health & security status of ***Office 365*** environment.

SERVICE/CATEGORY	ISSUES	PASSED	NON-COMPLIANT
Users	20	0	20
Email/Exchange Online	40	0	20
Accounts And Authentication	22	0	40
Configuration	8	0	22
Application Permissions	12	0	8
Data Management	8	0	8
Auditing	9	0	12

Storage	8	0	10
Mobile Device Management	10	0	10

6. Office 365 Subscription and SKU

SKU Name	SKU Status	Licenses in SKU

7. Office 365 Domains and Status

Domain name	Verification status	Status
SampleA.com	Verified	OK
SampleB.net	Verified	OK
SampleC.com	Verified	OK
SampleA.onmicrosoft.com	**Verified**	**OK**

8. Office 365 Domains and Services

DOMAIN NAME	SERVICES	STATUS
SAMPLEA.COM	EMAIL, OFFICECOMMUNICATIONSONLINE, INTUNE	OK
SAMPLEB.NET	EMAIL, OFFICECOMMUNICATIONSONLINE, INTUNE	OK
SAMPLEC.COM	EMAIL, OFFICECOMMUNICATIONSONLINE, INTUNE	OK
SAMPLEA.ONMICROSOFT.COM	**EMAIL, OFFICECOMMUNICATIONSONLINE**	**OK**

9. Office 365 Domain Passwords

DOMAIN NAME	DOMAIN TYPE	NOTIFICATION DAYS	VALIDITY PERIOD

10. Reported Items Per Test

The following table shows the items that have been reported Per Office 365 Test. The table might also need the Tests that have been pased and/or completed but doesn't include tests that have not been executed for some reasons.

Category	Test	Risk	Items
Users	Office 365 Users Password Never Expires Test	**High**	Total Office Users Password Never Expires Set:0

Users	Office 365 Users Not Changed Password Test	**High**	Total Office 365 Users Not Changed Their Passwords:50
Email/Exchange Online	Office 365 Inactive Mailbox Test	**High**	Total Inactive Mailboxes:2
Email/Exchange Online	Office 365 Deleted Mailbox Test	**High**	Total Deleted Mailboxes:0
Email/Exchange Online	Office 365 Mailbox Sync Test	**High**	Total Mailboxes In Sync Error:13
Email/Exchange Online	Office 365 Mailbox Hidden From Address List Test	**High**	Total Hidden Mailboxes:0
Email/Exchange Online	Exchange Online External Address Forwarding Test	**High**	Total Mailboxes Forwarding To External Domains:0
Email/Exchange Online	Exchange Online Litigation Hold Test	**High**	Total Mailboxes On Litigation Hold:0
Email/Exchange Online	Exchange Online SPAM Test	**High**	Total Inbound and Outbound SPAM Items:0
Email/Exchange Online	Exchange Online Mailbox Auditing Test	**High**	Total Mailboxes With No Mailboxes Auditing:0
Email/Exchange Online	Office 365 Exchange Online Modern Authentication Test	**High**	Exchange Online Modern Authentication Status:Enabled
Email/Exchange Online	Office 365 Exchange Online Privileged Access Management Test	**High**	Privileged Access Management Status:Not Enabled
Email/Exchange Online	Office 365 Exchange Online Admin Auditing Test	**High**	Admin Auditing Status:Disabled
Email/Exchange Online	Office 365 Exchange Online Admin Success and Failure Attempts	**High**	Total Failures for Online Admins:0
Email/Exchange Online	Office 365 Exchange Online External Access Admin Success and Failure Attempts	**High**	Total Failures for External Admins:0
Email/Exchange Online	Ensure the Common Attachment Types Filter is enabled	**High**	:EnableFileFilter:Not Enabled
Email/Exchange Online	Ensure Exchange Online Spam Policies are set correctly	**High**	Status:Not Enabled
Email/Exchange Online	Ensure mail transport rules do not forward email to external domains	**High**	Total Mails Forwarding Enabled:0
Email/Exchange Online	Ensure automatic forwarding options are disabled	**High**	Auto Forwarding Status:True
Email/Exchange Online	Ensure mail transport rules do not whitelist specific domains	**High**	Total Whitelist Domains:0
Email/Exchange Online	Ensure the Client Rules Forwarding Block is enabled	**High**	Client Rules Forwarding Block Status:Disabled
Email/Exchange Online	Ensure the Advanced Threat Protection Safe Links policy is enabled	**High**	NONE

Email/Exchange Online	Ensure the Advanced Threat Protection SafeAttachments policy is enabled	**High**	NONE
Email/Exchange Online	Ensure basic authentication for Exchange Online is disabled	**High**	Basic Authentication Status for Exchange Online:Disabled
Email/Exchange Online	Ensure that an anti-phishing policy has been created	**High**	Anti-Phishing Policy Status:Enabled
Email/Exchange Online	Ensure that DKIM is enabled for all Exchange Online Domains	**High**	Total Domains Missing DKIM :3
Email/Exchange Online	Ensure that SPF records are published for all Exchange Domains	**High**	Total Domains Missing SPF Records:4
Email/Exchange Online	Ensure DMARC Records for all Exchange Online domains are published	**High**	Total Domains Not Registered with DMARC Records:4
Email/Exchange Online	Ensure notifications for internal users sending malware is Enabled	**High**	Status:EnableInternalSenderAdminNotifications:Disabled
Email/Exchange Online	Ensure MailTips are enabled for end users	**High**	User MailTips Status:Not All MailTips Enabled
Email/Exchange Online	Ensure that LinkedIn contact synchronization is disabled	**High**	LinkedIn Contact Sync Status:Enabled
Email/Exchange Online	Ensure that Facebook contact synchronization is disabled	**High**	Facebook Contact Sync Status:Enabled
Accounts And Authentication	Office 365 User Roles Test	**High**	Total Office Groups having more than 10 Members:0
Accounts And Authentication	Ensure that between two and four global admins are designated	**High**	Total Global Admins:5
Accounts And Authentication	Ensure multifactor authentication is enabled for all users in all roles	**High**	Total Users with NO MFA Enabled:50
Accounts And Authentication	Office 365 Users Strong Password Requirements Test	**High**	Total Users With No Strong Password Requirements:0
Accounts And Authentication	Ensure multifactor authentication is enabled for all users in administrative roles	**High**	Total Office Administrators Not Enabled With MFA:2
Accounts And Authentication	Ensure self-service password reset is enabled	**High**	Self-Service Password Status:SSR Not Enabled
Accounts And Authentication	Ensure that password protection is enabled for Active Directory	**High**	NONE
Accounts And Authentication	Ensure modern authentication for Exchange Online is enabled	**High**	Modern Authentication for Exchange Online Status:Enabled
Accounts And Authentication	Ensure modern authentication for Teams Online is enabled	**High**	Modern Authentication for Teams Online:Enabled

Accounts And Authentication	Ensure modern authentication for SharePoint applications is required	**High**	Modern Authenitcation for SharePoint Online:Enabled
Accounts And Authentication	Ensure that Office 365 Passwords Are Not Set to Expire	**High**	Total Office Domains Not Configured With Password Policies:0
Accounts And Authentication	Enable Conditional Access policies to block legacy authentication	**High**	Total Conditional Access Policies:0
Accounts And Authentication	Ensure that password hash sync is enabled for hybrid deployments	**High**	Status:Password Has Sync:Not Enabled
Accounts And Authentication	Enable Azure AD Identity Protection sign-in risk policies	**High**	NONE
Accounts And Authentication	Enable Azure AD Identity Protection user risk policies	**High**	NONE
Accounts And Authentication	Use Just In Time privileged access to Office 365 roles	**High**	NONE
Accounts And Authentication	Ensure Security Defaults is disabled on Azure Active Directory	**High**	Status:Password Has Sync:Not Enabled
Accounts And Authentication	Ensure Administrative accounts are separate and cloud-only	**High**	Total Sync-In Admin Accounts:0
Accounts And Authentication	Ensure that only organizationally managed/approved public groups exist	**High**	NONE
Accounts And Authentication	Ensure that collaboration invitations are sent to allowed domains only	**High**	NONE
Accounts And Authentication	Ensure that LinkedIn contact synchronization is disabled	**High**	LinkedIn Contact Sync Status:Enabled
Accounts And Authentication	Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users	**High**	NONE
Accounts And Authentication	Ensure the option to remain signed in is hidden	**High**	NONE
Configuration	Office 365 Domain Authentication Config Test	**High**	NONE
Configuration	Office 365 Organization Auditing Test	**High**	Office 365 Organizationa Auditing Status:Enabled
Application Permissions	Ensure third party integrated applications are not allowed	**High**	NONE
Application Permissions	Ensure calendar details sharing with external users is disabled	**High**	Status:Enabled

Application Permissions	Ensure Safe Links for Office Applications is Enabled	**High**	Status:Not Enabled
Application Permissions	Ensure Safe Attachments for SharePoint-OneDrive-Microsoft Teams is Enabled	**High**	Status:Not Enabled
Application Permissions	Ensure Office 365 SharePoint infected files are disallowed for download	**High**	Status:Disabled
Application Permissions	Ensure user consent to apps accessing company data on their behalf is not allowed	**High**	Status:UsersPermissionToUserConsentToAppEnabled
Application Permissions	Ensure the admin consent workflow is enabled	**High**	NONE
Application Permissions	Ensure users installing Outlook add-ins is not allowed	**High**	NONE
Application Permissions	Ensure users installing Word-Excel-and PowerPoint add-ins is not allowed	**High**	NONE
Application Permissions	Ensure internal phishing protection for Microsoft Forms is enabled	**High**	NONE
Application Permissions	Ensure that Sways cannot be shared with people outside of your organization	**High**	NONE
Data Management	Ensure the customer lockbox feature is enabled	**High**	Status:Disabled
Data Management	Ensure SharePoint Online Information Protection policies are set up and used	**High**	NONE
Data Management	Ensure external domains are not allowed in Teams	**High**	NONE
Data Management	Ensure DLP policies are enabled	**High**	NONE
Data Management	Ensure DLP policies are enabled for Microsoft Teams	**High**	NONE
Data Management	Ensure that external users cannot share files folders and sites they do not own	**High**	Status:PreventExternalUsersFromResharing: Not Enabled
Data Management	Ensure external file sharing in Teams is enabled for only approved cloud storage services	**High**	NONE
Auditing	Ensure Microsoft 365 audit log search is Enabled	**High**	NONE
Auditing	Ensure mailbox auditing for all users is Enabled	**High**	NONE

Auditing	Ensure the Azure AD 'Risky sign-ins' report is reviewed at least weekly	**High**	NONE
Auditing	Ensure the Application Usage report is reviewed at least weekly	**High**	NONE
Auditing	Ensure the self-service password reset activity report is reviewed at least weekly	**High**	NONE
Auditing	Ensure user role group changes are reviewed at least weekly	**High**	NONE
Auditing	Ensure mail forwarding rules are reviewed at least weekly	**High**	NONE
Auditing	Ensure the Mailbox Access by Non-Owners Report is reviewed at least biweekly	**High**	NONE
Auditing	Ensure the Malware Detections report is reviewed at least weekly	**High**	NONE
Auditing	Ensure the Account Provisioning Activity report is reviewed at least weekly	**High**	NONE
Auditing	Ensure non-global administrator role group assignments are reviewed at least weekly	**High**	NONE
Auditing	Ensure the spoofed domains report is review weekly	**High**	NONE
Auditing	Ensure Microsoft Defender for Cloud Apps is Enabled	**High**	NONE
Auditing	Ensure the report of users who have had their email privileges restricted due to spamming is reviewed	**High**	NONE
Auditing	Ensure Guest Users are reviewed at least biweekly	**High**	NONE
Auditing	Ensure all security threats in the Threat protection status report are reviewed at least weekly	**High**	NONE
Storage	Ensure document sharing is being controlled by domains with whitelist or blacklist	**High**	NONE
Storage	Block OneDrive for Business sync from unmanaged devices	**High**	NONE
Storage	Ensure expiration time for external sharing links is set	**High**	NONE

Storage	Ensure external storage providers available in Outlook on the Web are restricted	**High**	NONE
Mobile Device Management	Ensure mobile device management policies are set to require advanced security configurations for Android Devices	**High**	NONE
Mobile Device Management	Ensure mobile device management policies are set to require advanced security configurations for iOS Devices	**High**	NONE
Mobile Device Management	Ensure that mobile device password reuse is prohibited for Android Devices	**High**	NONE
Mobile Device Management	Ensure that mobile device password reuse is prohibited for iOS Devices	**High**	NONE
Mobile Device Management	**Ensure that mobile devices are set to never expire passwords for Android Devices**	**High**	**NONE**

5. Compliance Status

Compliance Status section includes Tests the need attention ensuring Office 365 environment is in compliant with CIS Benchmark standards. The table also includes tests that have been passed but doesn't include not executed tests.

Category	Test	Risk	Compliance status
Users	Office 365 Users Password Never Expires Test	**High**	**NonCompliant**
Users	Office 365 Users Not Changed Password Test	**High**	**NonCompliant**
Email/Exchange Online	Office 365 Inactive Mailbox Test	**High**	**NonCompliant**
Email/Exchange Online	Office 365 Deleted Mailbox Test	**High**	**NonCompliant**
Email/Exchange Online	Office 365 Mailbox Sync Test	**High**	**NonCompliant**
Email/Exchange Online	Office 365 Mailbox Hidden From Address List Test	**High**	**NonCompliant**
Email/Exchange Online	Exchange Online External Address Forwarding Test	**High**	**NonCompliant**
Email/Exchange Online	Exchange Online Litigation Hold Test	**High**	**NonCompliant**
Email/Exchange Online	Exchange Online SPAM Test	**High**	**NonCompliant**
Email/Exchange Online	Exchange Online Mailbox Auditing Test	**High**	**NonCompliant**
Email/Exchange Online	Office 365 Exchange Online Modern Authentication Test	**High**	**NonCompliant**
Email/Exchange Online	Office 365 Exchange Online Privileged Access Management Test	**High**	**NonCompliant**
Email/Exchange Online	Office 365 Exchange Online Admin Auditing Test	**High**	**NonCompliant**
Email/Exchange Online	Office 365 Exchange Online Admin Success and Failure Attempts	**High**	**NonCompliant**

Email/Exchange Online	Office 365 Exchange Online External Access Admin Success and Failure Attempts	**High**	**NonCompliant**
Email/Exchange Online	Ensure the Common Attachment Types Filter is enabled	**High**	**NonCompliant**
Email/Exchange Online	Ensure Exchange Online Spam Policies are set correctly	**High**	**NonCompliant**
Email/Exchange Online	Ensure mail transport rules do not forward email to external domains	**High**	**NonCompliant**
Email/Exchange Online	Ensure automatic forwarding options are disabled	**High**	**NonCompliant**
Email/Exchange Online	Ensure mail transport rules do not whitelist specific domains	**High**	**NonCompliant**
Email/Exchange Online	Ensure the Client Rules Forwarding Block is enabled	**High**	**NonCompliant**
Email/Exchange Online	Ensure the Advanced Threat Protection Safe Links policy is enabled	**High**	**NonCompliant**
Email/Exchange Online	Ensure the Advanced Threat Protection SafeAttachments policy is enabled	**High**	**NonCompliant**
Email/Exchange Online	Ensure basic authentication for Exchange Online is disabled	**High**	**NonCompliant**
Email/Exchange Online	Ensure that an anti-phishing policy has been created	**High**	**NonCompliant**
Email/Exchange Online	Ensure that DKIM is enabled for all Exchange Online Domains	**High**	**NonCompliant**
Email/Exchange Online	Ensure that SPF records are published for all Exchange Domains	**High**	**NonCompliant**
Email/Exchange Online	Ensure DMARC Records for all Exchange Online domains are published	**High**	**NonCompliant**
Email/Exchange Online	Ensure notifications for internal users sending malware is Enabled	**High**	**NonCompliant**
Email/Exchange Online	Ensure MailTips are enabled for end users	**High**	**NonCompliant**
Email/Exchange Online	Ensure that LinkedIn contact synchronization is disabled	**High**	**NonCompliant**
Email/Exchange Online	Ensure that Facebook contact synchronization is disabled	**High**	**NonCompliant**
Accounts And Authentication	Office 365 User Roles Test	**High**	**NonCompliant**
Accounts And Authentication	Ensure that between two and four global admins are designated	**High**	**NonCompliant**
Accounts And Authentication	Ensure multifactor authentication is enabled for all users in all roles	**High**	**NonCompliant**
Accounts And Authentication	Office 365 Users Strong Password Requirements Test	**High**	**NonCompliant**
Accounts And Authentication	Ensure multifactor authentication is enabled for all users in administrative roles	**High**	**NonCompliant**
Accounts And Authentication	Ensure self-service password reset is enabled	**High**	**NonCompliant**
Accounts And Authentication	Ensure that password protection is enabled for Active Directory	**High**	**NonCompliant**

Accounts And Authentication	Ensure modern authentication for Exchange Online is enabled	**High**	**NonCompliant**
Accounts And Authentication	Ensure modern authentication for Teams Online is enabled	**High**	**NonCompliant**
Accounts And Authentication	Ensure modern authentication for SharePoint applications is required	**High**	**NonCompliant**
Accounts And Authentication	Ensure that Office 365 Passwords Are Not Set to Expire	**High**	**NonCompliant**
Accounts And Authentication	Enable Conditional Access policies to block legacy authentication	**High**	**NonCompliant**
Accounts And Authentication	Ensure that password hash sync is enabled for hybrid deployments	**High**	**NonCompliant**
Accounts And Authentication	Enable Azure AD Identity Protection sign-in risk policies	**High**	**NonCompliant**
Accounts And Authentication	Enable Azure AD Identity Protection user risk policies	**High**	**NonCompliant**
Accounts And Authentication	Use Just In Time privileged access to Office 365 roles	**High**	**NonCompliant**
Accounts And Authentication	Ensure Security Defaults is disabled on Azure Active Directory	**High**	**NonCompliant**
Accounts And Authentication	Ensure Administrative accounts are separate and cloud-only	**High**	**NonCompliant**
Accounts And Authentication	Ensure that only organizationally managed/approved public groups exist	**High**	**NonCompliant**
Accounts And Authentication	Ensure that collaboration invitations are sent to allowed domains only	**High**	**NonCompliant**
Accounts And Authentication	Ensure that LinkedIn contact synchronization is disabled	**High**	**NonCompliant**
Accounts And Authentication	Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users	**High**	**NonCompliant**
Accounts And Authentication	Ensure the option to remain signed in is hidden	**High**	**NonCompliant**
Configuration	Office 365 Domain Authentication Config Test	**High**	**NonCompliant**
Configuration	Office 365 Organization Auditing Test	**High**	**NonCompliant**
Application Permissions	Ensure third party integrated applications are not allowed	**High**	**NonCompliant**
Application Permissions	Ensure calendar details sharing with external users is disabled	**High**	**NonCompliant**

Application Permissions	Ensure Safe Links for Office Applications is Enabled	**High**	**NonCompliant**
Application Permissions	Ensure Safe Attachments for SharePoint-OneDrive-Microsoft Teams is Enabled	**High**	**NonCompliant**
Application Permissions	Ensure Office 365 SharePoint infected files are disallowed for download	**High**	**NonCompliant**
Application Permissions	Ensure user consent to apps accessing company data on their behalf is not allowed	**High**	**NonCompliant**
Application Permissions	Ensure the admin consent workflow is enabled	**High**	**NonCompliant**
Application Permissions	Ensure users installing Outlook add-ins is not allowed	**High**	**NonCompliant**
Application Permissions	Ensure users installing Word-Excel-and PowerPoint add-ins is not allowed	**High**	**NonCompliant**
Application Permissions	Ensure internal phishing protection for Microsoft Forms is enabled	**High**	**NonCompliant**
Application Permissions	Ensure that Sways cannot be shared with people outside of your organization	**High**	**NonCompliant**
Data Management	Ensure the customer lockbox feature is enabled	**High**	**NonCompliant**
Data Management	Ensure SharePoint Online Information Protection policies are set up and used	**High**	**NonCompliant**
Data Management	Ensure external domains are not allowed in Teams	**High**	**NonCompliant**
Data Management	Ensure DLP policies are enabled	**High**	**NonCompliant**
Data Management	Ensure DLP policies are enabled for Microsoft Teams	**High**	**NonCompliant**
Data Management	Ensure that external users cannot share files folders and sites they do not own	**High**	**NonCompliant**
Data Management	Ensure external file sharing in Teams is enabled for only approved cloud storage services	**High**	**NonCompliant**
Auditing	Ensure Microsoft 365 audit log search is Enabled	**High**	**NonCompliant**
Auditing	Ensure mailbox auditing for all users is Enabled	**High**	**NonCompliant**
Auditing	Ensure the Azure AD 'Risky sign-ins' report is reviewed at least weekly	**High**	**NonCompliant**
Auditing	Ensure the Application Usage report is reviewed at least weekly	**High**	**NonCompliant**
Auditing	Ensure the self-service password reset activity report is reviewed at least weekly	**High**	**NonCompliant**
Auditing	Ensure user role group changes are reviewed at least weekly	**High**	**NonCompliant**
Auditing	Ensure mail forwarding rules are reviewed at least weekly	**High**	**NonCompliant**
Auditing	Ensure the Mailbox Access by Non-Owners Report is reviewed at least biweekly	**High**	**NonCompliant**
Auditing	Ensure the Malware Detections report is reviewed at least weekly	**High**	**NonCompliant**
Auditing	Ensure the Account Provisioning Activity report is reviewed at least weekly	**High**	**NonCompliant**

Auditing	Ensure non-global administrator role group assignments are reviewed at least weekly	**High**	**NonCompliant**
Auditing	Ensure the spoofed domains report is review weekly	**High**	**NonCompliant**
Auditing	Ensure Microsoft Defender for Cloud Apps is Enabled	**High**	**NonCompliant**
Auditing	Ensure the report of users who have had their email privileges restricted due to spamming is reviewed	**High**	**NonCompliant**
Auditing	Ensure Guest Users are reviewed at least biweekly	**High**	**NonCompliant**
Auditing	Ensure all security threats in the Threat protection status report are reviewed at least weekly	**High**	**NonCompliant**
Storage	Ensure document sharing is being controlled by domains with whitelist or blacklist	**High**	**NonCompliant**
Storage	Block OneDrive for Business sync from unmanaged devices	**High**	**NonCompliant**
Storage	Ensure expiration time for external sharing links is set	**High**	**NonCompliant**
Storage	Ensure external storage providers available in Outlook on the Web are restricted	**High**	**NonCompliant**
Mobile Device Management	Ensure mobile device management policies are set to require advanced security configurations for Android Devices	**High**	**NonCompliant**
Mobile Device Management	Ensure mobile device management policies are set to require advanced security configurations for iOS Devices	**High**	**NonCompliant**
Mobile Device Management	Ensure that mobile device password reuse is prohibited for Android Devices	**High**	**NonCompliant**
Mobile Device Management	Ensure that mobile device password reuse is prohibited for iOS Devices	**High**	**NonCompliant**
Mobile Device Management	**Ensure that mobile devices are set to never expire passwords for Android Devices**	**High**	**NonCompliant**

5. Technical Findings By SmartProfiler

After carrying out a complete health assessment of the ***Microsoft Office 365 and its Services***, the following issues have been identified. These are the Action Items identified in this report. We recommend that these items are acted on with the highest priority for each focus area.

5.1 Email/Exchange Online

Test	Severity/risk	Compliance status	Remark
Office 365 Inactive Mailbox Test	High	NonCompliant	**IMPACT:** Inactive Mailboxes were found in Office 365 Exchange Online. Inactive Mailboxes are assigned with licenses. **ACTION:** If these mailboxes are not used then unassign the license to save the cost.
Office 365 Deleted Mailbox Test	High	NonCompliant	**IMPACT:** Deleted Mailboxes were found in Office 365 Exchange Online.Refer issue details **ACTION:** Please check why these mailboxes were deleted or restore if any mailbox is important.
Office 365 Mailbox Sync Test	High	NonCompliant	**IMPACT:** Some mailboxes are not syncing. Refer issue details **ACTION:** Please review the list provided.
Office 365 Mailbox Hidden From Address List Test	High	NonCompliant	**IMPACT:** Some mailboxes are hidden from the address list.These mailboxes will not appear in the address list. **ACTION:** Please review the list provided.

Exchange Online External Address Forwarding Test	High	NonCompliant	**IMPACT:** Some Mailboxes are configured with External Forwarding. It is a security risk. Mailboxes must not be configured with forwarding to prevent data loss. **ACTION:** Please review the list and make sure to remove forwarding from these mailboxes.
Exchange Online Litigation Hold Test	High	NonCompliant	**IMPACT:** Some Mailboxes are in Litigation Hold.Refer issue details **ACTION:** Please review the list provided.
Exchange Online SPAM Test	High	NonCompliant	**IMPACT:** Found SPAM Items.It is a security risk. **ACTION:** Identify the SPAM domains and block them.
Exchange Online Mailbox Auditing Test	High	NonCompliant	**IMPACT:** Auditing is not enabled for mailboxes.Auditing is required for mailboxes in order to see changes that have been taking place. **ACTION:** Please review the list provided.
Office 365 Exchange Online Modern Authentication Test	High	NonCompliant	**IMPACT:** Modern Authentication is not enabled.Newer clients will not be able to use Modern Authentication feature of Office 365 causing multiple logon prompts. **ACTION:** It is recommended to enable Office 365 Modern Authentication Service.
Office 365 Exchange Online Privileged Access Management Test	High	NonCompliant	**IMPACT:** Office 365 Privileged Access Management is NOT enabled.Refer issue details **ACTION:** It is recommended to enable PAM in Office 365.
Office 365 Exchange Online Admin Auditing Test	High	NonCompliant	**IMPACT:** Office 365 Admin Auditing is disabled.It is a security risk and not compliance issue. **ACTION:** It is recommended to enable Admin Auditing so data can be audited such as when someone changes the permissions on a mailbox.

Office 365 Exchange Online Admin Success and Failure Attempts	**High**	**NonCompliant**	**IMPACT:** Found failure attemts from Admins when accessing Office 365 objects.It is a securit risk. **ACTION:** Please review the data and make sure the attempts did not cause any issues.
Office 365 Exchange Online External Access Admin Success and Failure Attempts	**High**	**NonCompliant**	**IMPACT:** Found failure attemts from External Admins when accessing Office 365 objects.It is a securit risk. **ACTION:** Please review the data and make sure the attempts did not cause any issues.
Ensure the Common Attachment Types Filter is enabled	**High**	**NonCompliant**	**IMPACT:** Common Attachment Filter is not enabled.Blocking common malicious file types should not cause an impact in modern computing environments. **ACTION:** The Common Attachment Types Filter lets a user block known and custom malicious file types from being attached to emails. Blocking known malicious file types can help prevent malware-infested files from infecting a host.
Ensure Exchange Online Spam Policies are set correctly	**High**	**NonCompliant**	IMPACT: **Exchange Online Spam Policies are not set correctly.Notification of users that have been blocked should not cause an impact to the user** ACTION: **In Microsoft 365 organizations with mailboxes in Exchange Online or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, email messages are automatically protected against spam (junk email) by EOP. Configure Exchange Online Spam Policies to copy emails and notify someone when a sender in your tenant has been blocked for sending spam emails. A blocked account is a good indication that the account in question has been breached and an attacker is using it to send spam emails to other people.**

5.2 Office 365 Users

Test	Severity/risk	Compliance status	Remark

Office 365 Users Licensing Test	High	NotApplicable	**IMPACT:** Some Office 365 Users are not licensed.Unlicensed users will not be able to use Office 365 Services. **ACTION:** It is recommended to assign Licenses to users.
Office 365 Users Deleted Test	High	NotApplicable	**IMPACT:** Some users found in Office 365 Recycle Bin.These user accounts get deleted from Office 365 Recycle Bin after sometime. **ACTION:** Please check if any of these accounts are needed and restore them from Office 365 Recycle Bin.
Office 365 Users Disabled Test	High	NotApplicable	**IMPACT:** Some users are disabled in Office 365.Disabled users cannot use Office 365 Services. **ACTION:** Please check if any of the user accounts need to be enabled to enable use of Office 365 Services.
Office 365 Users Reconciliation Test	High	NotApplicable	**IMPACT:** Some users require License Reconciliation.Users may not be able to use Office 365 Services. **ACTION:** Please check if these users need to be assigned a license again.
Office 365 Users Password Never Expires Test	High	NonCompliant	**IMPACT:** Some Office 365 Users have their Password set to NOT Expire. These users can remain with a single password and if the password is compromised anyone can access Office 365 Services. **ACTION:** Every user in Office 365 must change their password according to Password Policies.
Office 365 Users Sync Test	High	NotApplicable	**IMPACT:** Some users do not sync.Refer issue details **ACTION:** Please review the list.
Office 365 Users Provisioning Test	High	NotApplicable	**IMPACT:** Some Office 365 users have their Provisioning State to pending.Refer issue details **ACTION:** Please review the list and provision these users.

Office 365 Blocked Users Test	**High**	**NotApplicable**	**IMPACT:** Some Office 365 Users are blocked.Blocked Users will not be able to sign in to use Office 365 Services. **ACTION:** Please review the list and unblock these users if required.
Office 365 Users Not Changed Password Test	**High**	**NonCompliant**	**IMPACT:** Some Office 365 users have not been changing their passwords within 90 days.It is a security risk. Every user in Office 365 Users must change their passwords within 90 days. **ACTION:** Please identify these users and make sure they change their passwords.
Office 365 Users With Company Administrators Test	**High**	**NotApplicable**	**IMPACT:** More than Five company Administrators were found in Office 365.More users can have full control over Office 365 Services. **ACTION:** Please review the list and make sure only designated members are part of Company Administrator User Role.
Office 365 Users Deleted and Licensed Test	**High**	**NotApplicable**	**IMPACT:** Some users are deleted but have Office 365 Licenses associated.Office 365 Services are being charged for users that have licenses assigned and deleted. **ACTION:** Please review the list and unassign licenses from these users.
Office 365 Groups Without Members Test	**High**	**NotApplicable**	**IMPACT:** Some Office 365 Groups do not contain user members.If these Groups were created for some reasons then they should have members in it. **ACTION:** Please review the list of Grops provided by the test and add users or remove these groups.
Office 365 Groups Without Description Test	**High**	**NotApplicable**	**IMPACT: Some Office 365 Groups do not have description set.In a large Office 365 environment you may not be able to identify the groups.** **ACTION: Please review the list and assign a description to each Office 365 Group.**

5.3 Accounts And Authentication

Test	Severity/risk	Compliance status	Remark
Office 365 User Roles Test	High	NonCompliant	**IMPACT:** Some Office 365 User Roles contain more than 10 members.Refer issue details **ACTION:** Please review the list and make sure only designated members are part of Office 365 User Roles and it is not recommended to have more than 10 members in each role.
Ensure that between two and four global admins are designated	High	NonCompliant	**IMPACT:** There is only one Global Administrator assigned to the Global Administrator group.The potential impact associated with ensuring compliance with this requirement is dependent upon the current number of global administrators configured in the tenant. If there is only one global administrator in a tenant, an additional global administrator will need to be identified and configured. If there are more than four global administrators, a review of role requirements for current global administrators will be required to identify which of the users require global administrator access. **ACTION:** More than one global administrator should be designated so a single admin can be monitored and to provide redundancy should a single admin leave an organization. Additionally, there should be no more than four global admins set for any tenant. Ideally global administrators will have no licenses assigned to them.
Ensure multifactor authentication is enabled for all users in all roles	High	NonCompliant	**IMPACT:** Some users do not have multi-factor authentication. Please review the list and enable MFA for missing users.Implementation of multifactor authentication for all users will necessitate a change to user routine. All users will be required to enroll in multifactor authentication using phone, SMS, or an authentication application. After enrollment, use of multifactor authentication will be required for future authentication to the environment. **ACTION:** Enable multifactor authentication for all users in the Microsoft 365 tenant. Users will be prompted to authenticate with a second factor upon logging in to Microsoft 365

			services. The second factor is most commonly a text message to a registered mobile phone number where they type in an authorization code, or with a mobile application like Microsoft Authenticator.
Office 365 Users Strong Password Requirements Test	**High**	**NonCompliant**	**IMPACT:** Some Office 365 Users do not have Strong Password Requirements Set.Users can use Weak passwords which is a security risk. **ACTION:** Please use Set-MSOLUser Cmdlet and enable Strong Password Requirements for these users.
Ensure multifactor authentication is enabled for all users in administrative roles	**High**	**NonCompliant**	**IMPACT:** Some Admin Accounts are not MFA Enabled. Please review impact and enable.Implementation of multifactor authentication for all users in administrative roles will necessitate a change to user routine. All users in administrative roles will be required to enroll in multifactor authentication using phone, SMS, or an authentication application. After enrollment, use of multifactor authentication will be required for future access to the environment. **ACTION:** Enable multifactor authentication for all users who are members of administrative roles in Office 365 Tenant.
Ensure self-service password reset is enabled	**High**	**NonCompliant**	**IMPACT:** Self-Service Password Reset is not enabled for Tenant.The impact associated with this setting is that users will be required to provide additional contact information to enroll in self-service password reset. Additionally, minor user education may be required for users that are used to calling a help desk for assistance with password resets. As of August of 2020 combined registration is automatic for new tenants therefor users will not need to register for password reset separately from multi-factor authentication. **ACTION:** Users will no longer need to engage the helpdesk for password resets, and the password reset mechanism will automatically block common, easily guessable passwords. Combined registration should be enabled if not already, as of August of 2020 combined registration is automatic for new tenants therefore users will not need to register for password reset

			separately from multi-factor authentication.
Ensure that password protection is enabled for Active Directory	**High**	**NonCompliant**	**IMPACT:** Password Protection is not enabled.The potential impact associated with implementation of this setting is dependent upon the existing password policies in place in the environment. For environments that have strong password policies in place, the impact will be minimal. For organizations that do not have strong password policies in place, implementation of Azure Active Directory Password Protection may require users to change passwords, and adhere to more stringent requirements than they have been accustomed to. **ACTION:** Enable Azure Active Directory Password Protection to Active Directory to protect against the use of common passwords. Note: This recommendation applies to Hybrid deployments only, and will have no
Ensure modern authentication for Exchange Online is enabled	**High**	**NonCompliant**	**IMPACT:** Modern Authentication is not enabled for Exchange Online.Users of older email clients, such as Outlook 2013 and Outlook 2016, will no longer be able to authenticate to Exchange using Basic Authentication, which will necessitate migration to modern authentication practices. **ACTION:** Modern authentication in Microsoft 365 enables authentication features like multifactor authentication (MFA) using smart cards, certificate-based authentication (CBA), and third-party SAML identity providers. When you enable modern authentication in Exchange Online, Outlook 2016 and Outlook 2013 use modern authentication to log in to Microsoft 365 mailboxes. When you disable modern authentication in Exchange
Ensure modern authentication for Teams Online is enabled	**High**	**NonCompliant**	**IMPACT:** Teams Online is not configured to use Modern Authentication.When you use modern authentication with the Microsoft Teams Rooms application, Active Directory Authentication Library (ADAL) is used to connect to Microsoft Teams, Exchange, and Skype for Business. The modern authentication mechanism uses the resource owner password credentials authorization grant type in OAuth 2.0, which doesn't require any user intervention.

			ACTION: It is recommended to enable Modern Authentication for Teams.
Ensure modern authentication for SharePoint applications is required	**High**	**NonCompliant**	**IMPACT:** Basic Authentication is not enabled for SharePoint OnlineImplementation of modern authentication for SharePoint will require users to authenticate to SharePoint using modern authentication. This may cause a minor impact to typical user behavior. **ACTION:** Strong authentication controls, such as the use of multifactor authentication, may be circumvented if basic authentication is used by SharePoint applications. Requiring modern authentication for SharePoint applications ensures strong authentication mechanisms are used when establishing sessions between these applications, SharePoint, and connecting users.
Ensure that Office 365 Passwords Are Not Set to Expire	**High**	**NonCompliant**	**IMPACT:** Not all Office 365 Password Policies are configured for all domains.The primary impact associated with this change is ensuring that users understand the process for making or requesting a password change when required. **ACTION:** Microsoft cloud-only accounts have a pre-defined password policy that cannot be changed. The only items that can change are the number of days until a password expires and whether or not passwords expire at all.Organizations such as NIST and Microsoft have updated their password policy recommendations to not arbitrarily require users to change their passwords after a specific amount of time, unless there is evidence that the password is compromised or the user forgot it. They suggest this even for single factor (Password Only) use cases, with a reasoning that forcing arbitrary password changes on users make the passwords less secure. Other recommendations within this Benchmark suggest the use of MFA authentication for at least critical accounts (at minimum), which makes password expiration even less useful as well as password protection for Azure AD.

Enable Conditional Access policies to block legacy authentication	High	NonCompliant	**IMPACT:** No Conditional Access policies were found.Enabling this setting will prevent users from connecting with older versions of Office, ActiveSync or using protocols like IMAP, POP or SMTP and may require upgrades to older versions of Office, and use of mobile mail clients that support modern authentication. **ACTION:** Use Conditional Access to block legacy authentication protocols in Office 365. Legacy authentication protocols do not support multi-factor authentication. These protocols are often used by attackers because of this deficiency. Blocking legacy authentication makes it harder for attackers to gain access.
Ensure that password hash sync is enabled for hybrid deployments	High	NonCompliant	**IMPACT:** Password Sync is not enabled for hybrid deployments.Compliance or regulatory restrictions may exist, depending on the organization's business sector, that preclude hashed versions of passwords from being securely transmitted to cloud data centers. **ACTION:** Password hash synchronization is one of the sign-in methods used to accomplish hybrid identity synchronization. Azure AD Connect synchronizes a hash, of the hash, of a user's password from an on-premises Active Directory instance to a cloud-based Azure AD instance. Applicable only to Hybrid Deplouments. Password hash synchronization helps by reducing the number of passwords your users
Enable Azure AD Identity Protection sign-in risk policies	High	NonCompliant	**IMPACT:** Azure AD Identity Protection Sign-In Risk Policies are not configured.When the policy triggers, the user will need MFA to access the account. In the case of a user who hasn't registered MFA on their account, they would be blocked from accessing their account. It is therefore recommended that the MFA registration policy be configured for all users who are a part of the Sign-in Risk policy. **ACTION:** Azure Active Directory Identity Protection sign-in risk detects risks in real-time and offline. A risky sign-in is an indicator for a sign-in attempt that might not have been performed by the legitimate owner of a user account. Turning on the sign-in risk policy ensures

			that suspicious sign-ins are challenged for multi-factor authentication.
Enable Azure AD Identity Protection user risk policies	**High**	**NonCompliant**	IMPACT: **Azure AD User Risk Policies are not enabled.When the policy triggers, access to the account will either be blocked or the user would be required to use multi-factor authentication and change their password. Users who haven't registered MFA on their account will be blocked from accessing it. If account access is blocked, an admin would need to recover the account. It is therefore recommended that the MFA registration policy be configured for all users who are a part of the User Risk policy.** ACTION: **Azure Active Directory Identity Protection user risk policies detect the probability that a user account has been compromised. With the user risk policy turned on, Azure AD detects the probability that a user account**

5.4 Configuration

Test	Severity/risk	Compliance status	Remark
Office 365 License Consumption Test	**High**	**NotApplicable**	**IMPACT:** Some SKUs are not being used in Office 365.Office 365 Services are being charged for SKUs which are not in use. **ACTION:** Please review the SKU list and make sure users are licensed from unused SKUs.
Office 365 Domain Verification Test	**High**	**NotApplicable**	**IMPACT:** Some Office 365 Domains are not verfied.Unverified domains will not be able to participate in Office 365 Services. **ACTION:** Please review the list and verify each Office 365 domain.
Office 365 Domain Services Test	**High**	**NotApplicable**	**IMPACT:** Some Office Domains do not have Services assigned.Refer issue details **ACTION:** Please review the list provided.
Office 365 Subscription Status Test	**High**	**NotApplicable**	**IMPACT:** Some SKUs are not enabled.Disabled SKUs need to be

			renewed or else licenses will not be assigned to the users. **ACTION:** Please review the list provided.
Office 365 Domain Authentication Config Test	**High**	**NonCompliant**	**IMPACT:** **ACTION:**
Office 365 Notification Emails Test	**High**	**NotApplicable**	**IMPACT:** Technical Notification Emails are not configured in Office 365.You will not receive any technical email notification from Microsoft. **ACTION:** Please configure atleast one email to receive Technical Notifications from Microsoft.
Office 365 Organization Auditing Test	**High**	**NonCompliant**	**IMPACT:** Auditing is not enabled for organization.Refer issue details **ACTION:** Please check and enable Organization Auditing.
Office 365 Dir Config Test	**High**	**NotApplicable**	**IMPACT:** Office 365 Dir Sync is not enabled.If you have Federated Identity configured then Synchronization must be enabled. **ACTION:** Please review Dir Sync configuration.
Office 365 Dir Sync Features Test	**High**	**NotApplicable**	**IMPACT:** Some Dir Sync features are not enabled. Please checkSome Dir Sync Features are required to meet the compliance. **ACTION:** Please review the features list and make sure to enable the required features.
Office 365 Dir Sync Property Conflict Test	**High**	**NotApplicable**	**IMPACT:** Found Users with User conflict properties.Users may not be able to sync from Office 365 to On-Premises and vice-versa. **ACTION:** Please review the conflicting objects and take actions accordingly.
Office 365 Dir Sync Property Conflict with User Principal Name Test	**High**	**NotApplicable**	**IMPACT:** Found Users with User Principal Name conflicts.Users may not be able to sync from Office 365 to On-Premises and vice-versa.

			ACTION: Please review the conflicting objects and take actions accordingly.
Office 365 Dir Sync Property Conflict with ProxyAddress Test	**High**	**NotApplicable**	**IMPACT: Found Users with ProxyAddress conflicts.Users may not be able to utilize Office 365 Services.** **ACTION: Please review the conflicting objects and take actions accordingly.**

5.5 Application Permissions

Test	Severity/risk	Compliance status	Remark
Ensure third party integrated applications are not allowed	**High**	**NonCompliant**	**IMPACT:** Third party integrated applications are not allowed is not configured.Implementation of this change will impact both end users and administrators. End users will not be able to integrate third-party applications that they may wish to use. **ACTION:** Do not allow third party integrated applications to connect to your services. You should not allow third party integrated applications to connect to your services unless there is a very clear value and you have robust security controls in place. While there are legitimate uses, attackers can grant access from breached accounts to third party applications to exfiltrate data from your tenancy without having to maintain the
Ensure calendar details sharing with external users is disabled	**High**	**NonCompliant**	**IMPACT:** Calender Details Sharing with External Users is not disabled.This functionality is not widely used. As a result it is unlikely that implementation of this setting will cause an impact to most users. Users that do utilize this functionality are likely to experience a minor inconvenience when scheduling meetings. **ACTION:** You should not allow your users to share the full details of their calendars with external users. Attackers often spend time learning about your organization before launching an attack. Publicly available calendars can help attackers understand organizational relationships and determine when specific users may be more vulnerable

			to an attack, such as when they are traveling.
Ensure Safe Links for Office Applications is Enabled	**High**	**NonCompliant**	**IMPACT:** Safe Links for Office Applications is not enabled.User impact associated with this change is minor - users may experience a very short delay when clicking on URLs in Office documents before being directed to the requested site. Users should be informed of the change as, in the event a link is unsafe and blocked, they will receive a message that it has been blocked. **ACTION:** Enabling Safe Links policy for Office applications allows URL's that exist inside of Office documents and email applications opened by Office, Office Online and Office mobile to be processed against Defender for Office time-of-click verification and rewritten if required. Note: E5 Licensing includes a number of Built-in Protection policies. When auditing policies note which policy you are viewing, and keep in mind CIS recommendations often extend the Default or Build-in Policies provided by MS. In order to Pass the highest priority policy must match all settings recommended. Safe Links for Office applications extends phishing protection to documents and emails that contain hyperlinks, even after they have been delivered to a user.
Ensure Safe Attachments for SharePoint-OneDrive-Microsoft Teams is Enabled	**High**	**NonCompliant**	**IMPACT:** Safe Attachments for SharePoint-OneDrive-Teams is not enabled.Impact associated with Safe Attachments is minimal, and equivalent to impact associated with anti-virus scanners in an environment. **ACTION:** Safe Attachments for SharePoint, OneDrive, and Microsoft Teams scans these services for malicious files.
Ensure Office 365 SharePoint infected files are disallowed for download	**High**	**NonCompliant**	**IMPACT:** SharePoint Infected Files are disallowed for download is not enabled.The only potential impact associated with implementation of this setting is potential inconvenience associated with the small percentage of false positive detections that may occur. **ACTION:** By default SharePoint online allows files that Defender for Office 365 has detected as infected to be downloaded. Defender for Office 365 for

			SharePoint, OneDrive, and Microsoft Teams protects your
Ensure user consent to apps accessing company data on their behalf is not allowed	**High**	**NonCompliant**	**IMPACT:** Consent to Apps accessing company data on their behalf is not allowed is not configured.If user consent is disabled previous consent grants will still be honored but all future consent operations must be performed by an administrator. **ACTION:** By default, users can consent to applications accessing your organization's data, although only for some permissions. For example, by default a user can consent to allow an app to access their own mailbox or the Teams conversations for a team the user owns, but cannot consent to allow an app unattended access to read and write to all SharePoint sites in your organization. Do not allow users to grant consent to apps accessing company data on their behalf. Attackers commonly use custom applications to trick users into granting them access to company data.
Ensure the admin consent workflow is enabled	**High**	**NonCompliant**	**IMPACT:** Admin Consent workflow is not enabled.To approve requests a reviewer must be a global administrator cloud application administrator or application administrator. **ACTION:** Without an admin consent workflow (Preview), a user in a tenant where user consent is disabled will be blocked when they try to access any app that requires permissions to access organizational data. The user sees a generic error message that says they're unauthorized to access the app and they should ask their admin for help. The admin consent workflow (Preview) gives admins a secure way to grant access to
Ensure users installing Outlook add-ins is not allowed	**High**	**NonCompliant**	**IMPACT:** Outlook Add-Ins is allowed.Implementation of this change will impact both end users and administrators. End users will not be able to integrate third-party applications that they may wish to use. **ACTION:** By default, users can install add-ins in their Microsoft Outlook Desktop client, allowing data access within the client application. Do not allow users to install add-ins in Outlook. Attackers commonly use vulnerable and custom-built add-ins to access data in user applications. While allowing users

			to install add-ins by themselves does allow them to easily acquire useful add-ins that integrate with Microsoft applications, it can represent a risk if not used and monitored carefully. Disable future user's ability to install add-ins in Microsoft Outlook helps reduce your threat-surface and mitigate this risk.
Ensure users installing Word-Excel-and PowerPoint add-ins is not allowed	**High**	**NonCompliant**	**IMPACT:** Work-Excel-PowerPoint add-ins are not allowed is not configured.Implementation of this change will impact both end users and administrators. End users will not be able to install add-ins that they may want to install. **ACTION:** By default, users can install add-ins in their Microsoft Word, Excel, and PowerPoint applications, allowing data access within the application. Do not allow users to install add-ins in Word, Excel, or PowerPoint.
Ensure internal phishing protection for Microsoft Forms is enabled	**High**	**NonCompliant**	**IMPACT:** Internal Phishing Protection for Microsoft Forms is not enabled.If potential phishing was detected, the form will be temporarily blocked and cannot be distributed and response collection will not happen until it is unblocked by the administrator or keywords were removed by the creator. **ACTION:** Microsoft Forms can be used for phishing attacks by asking personal or sensitive information and collecting the results. Microsoft 365 has built-in protection that will proactively scan for phishing attempt in forms such personal information request. Enabling internal phishing protection for Microsoft Forms will prevent attackers using forms for phishing attacks by asking personal or other sensitive information and URLs.
Ensure that Sways cannot be shared with people outside of your organization	**High**	**NonCompliant**	**IMPACT: Sways Cannot be shared with people outside of your organization is not configured.Interactive reports, presentations, newsletters and other items created in Sway will not be shared outside the organization by users.** **ACTION: Disable external sharing of Sway items such as reports, newsletters, presentations etc that could contain sensitive information. Disable external sharing of Sway documents that can contain sensitive**

			information to prevent accidental or arbitrary data leak.

5.6 Data Management

Test	Severity/risk	Compliance status	Remark
Ensure the customer lockbox feature is enabled	**High**	**NonCompliant**	**IMPACT:** Customer Lockbox Feature is not enabled.The impact associated with this setting is a requirement to grant Microsoft access to the tenant environment prior to a Microsoft engineer accessing the environment for support or troubleshooting. **ACTION:** You should enable the Customer Lockbox feature. It requires Microsoft to get your approval for any datacenter operation that grants a Microsoft support engineer or other employee direct access to any of your data. For example, in some cases a Microsoft support engineer might need access to your Microsoft 365 content in order to help troubleshoot and fix an issue for you. Customer lockbox requests also have an
Ensure SharePoint Online Information Protection policies are set up and used	**High**	**NonCompliant**	**IMPACT:** SharePoint Online Information Protection Policies are not set up and used.Creation of data classification policies will not cause a significant impact to an **ACTION:**
Ensure external domains are not allowed in Teams	**High**	**NonCompliant**	**IMPACT:** External Domains are not allowed in Teams is not configured.Impact associated with this change is highly dependent upon current practices in the tenant. If users do not regularly communicate with external parties using Skype or Teams channels, then minimal impact is likely. However, if users do regularly utilize Teams and Skype for client communication, potentially significant impacts could occur, and users should be contacts, and if necessary, alternate mechanisms to continue this communication should be identified prior to disabling external access to Teams and Skype. **ACTION:** As of December 2021 the default for Teams external

			communication is set to 'People in my organization can communicate with Teams users whose accounts aren't managed by an organization.' This means that users can communicate with personal Microsoft accounts (e.g. Hotmail, Outlook etc.), which presents data loss / phishing / social engineering risks. You should not allow your users to communicate with Skype or Teams users outside your organization. While there are legitimate, productivity-improving scenarios for this, it also represents a potential security threat because those external users will be able to interact with your users over Skype for Business or Teams. Users are prone to data loss / phishing / social engineering attacks via Teams.
Ensure DLP policies are enabled	**High**	**NonCompliant**	**IMPACT:** DLP Policies are not enabled.Enabling a Teams DLP policy will allow sensitive data in Exchange Online and **ACTION:**
Ensure DLP policies are enabled for Microsoft Teams	**High**	**NonCompliant**	**IMPACT:** Enabling a Teams DLP policy will allow sensitive data in Teams channels or chat messages to be detected or blocked. **ACTION:**
Ensure that external users cannot share files folders and sites they do not own	**High**	**NonCompliant**	**IMPACT:** Impact associated with this change is highly dependent upon current practices. If users do not regularly share with external parties, then minimal impact is likely. **ACTION:** If users do regularly share with guests/externally minimum impacts could occur as those external users will be unable to 're-share' content.
Ensure external file sharing in Teams is enabled for only approved cloud storage services	**High**	**NonCompliant**	**IMPACT:** **ACTION:**

5.7 Auditing

Test	Severity/risk	Compliance status	Remark

Ensure Microsoft 365 audit log search is Enabled	High	NonCompliant	**IMPACT:** Microsoft 365 Audit Log Search is not enabled.Auditing Process needs to be created and followed. **ACTION:** When audit log search in the Microsoft Purview compliance portal is enabled, user and admin activity from your organization is recorded in the audit log and retained for 90 days. However, your organization might be using a third-party security information and event management (SIEM) application to access your auditing data. In that case, a global admin can turn off audit log search in Microsoft 365. Enabling Microsoft Purview audit log search helps Office 365 back office teams to investigate activities for regular security operational or forensic purposes.
Ensure mailbox auditing for all users is Enabled	High	NonCompliant	**IMPACT:** Found some mailboxes found without auditing enabled.Auditing Process needs to be created and followed. **ACTION:** By turning on mailbox auditing, Microsoft 365 back office teams can track logons to a mailbox as well as what actions are taken while the user is logged on. After you turn on mailbox audit logging for a mailbox, you can search the audit log for mailbox activity. Additionally, when mailbox audit logging is turned on, some actions performed by administrators, delegates, and owners are logged by default. Starting in January 2019, Microsoft is turning on mailbox audit logging by default for all organizations.
Ensure the Azure AD 'Risky sign-ins' report is reviewed at least weekly	High	NonCompliant	**IMPACT:** Azure AD Risky Sign Ins auditing is not in place.Auditing Process needs to be created and followed. **ACTION:** This report contains records of accounts that have had activity that could indicate they are compromised. Reviewing this report on a regular basis allows for identification and remediation of compromised accounts.
Ensure the Application Usage report is reviewed at least weekly	High	NonCompliant	**IMPACT:** Application usage report review is not in place.Auditing Process needs to be created and followed. **ACTION:** The Application Usage report includes a usage summary for all Software as a Service (SaaS) applications

			that are integrated with your directory. Review the list of app registrations on a regular basis to look for risky apps that users have enabled that could cause data spillage or accidental elevation of privilege. Attackers can often get access to data illicitly through third-party SaaS applications. To verify the report is being reviewed at least weekly, confirm that the necessary procedures are in place and being followed.
Ensure the self-service password reset activity report is reviewed at least weekly	**High**	**NonCompliant**	**IMPACT:** Auditng is not in place and report is not being reviewed.Auditing Process needs to be created and followed. **ACTION:** The Microsoft 365 platforms allow a user to reset their password in the event they forget it. The self-service password reset activity report logs each time a user successfully resets their password this way. You should review the self-service password reset activity report at least weekly. An attacker will commonly compromise an account, then change the password to something they control and can manage. To verify the report is being reviewed at least weekly, confirm that the necessary procedures are in place and being followed
Ensure user role group changes are reviewed at least weekly	**High**	**NonCompliant**	**IMPACT:** Auditing Process is not created and followed.By performing regular reviews the Administrators assigning rights to users will need to inevitably provide justification for those changes to security auditors. Documentation that includes detailed policies, procedures, and change requests will need to be considered in order to keep a secure organization functioning within its planned operational level. **ACTION:** Role-Based Access Control allows for permissions to be assigned to users based on their roles within an organization. It is more manageable form of access control that is less prone to errors. These user roles can be audited inside of Microsoft Purview to provide a security auditor insight into user privilege change.
Ensure mail forwarding rules are reviewed at least weekly	**High**	**NonCompliant**	**IMPACT:** Auditing Process is not created and followed.Auditing Process needs to be created and followed.

			ACTION: The Exchange Online environment can be configured in a way that allows for automatic forwarding of e-mail. This can be done using Transport Rules in the Admin Center, Auto Forwarding per mailbox, and client-based rules in Outlook. Administrators and users both are given several methods to automatically and quickly send e-mails outside of your organization. Reviewing mail forwarding rules will provide the Messaging Administrator insight into possible attempts to exfiltrate data from the organization. Weekly review helps create a recognition of baseline, legitimate activity of users. This will aid in helping identify the more malicious activity of bad actors when/if they choose to use this side-channel.
Ensure the Mailbox Access by Non-Owners Report is reviewed at least biweekly	**High**	**NonCompliant**	**IMPACT:** Auditing Process needs to be created and followed. **ACTION:**
Ensure the Malware Detections report is reviewed at least weekly	**High**	**NonCompliant**	**IMPACT:** Auditing Process needs to be created and followed. **ACTION:**
Ensure the Account Provisioning Activity report is reviewed at least weekly	**High**	**NonCompliant**	**IMPACT:** Auditng Process is not created and followed.Auditing Process needs to be created and followed. **ACTION:** The Account Provisioning Activity report details any account provisioning that was attempted by an external application. If you don't usually use a third party provider to manage accounts, any entry on the list is likely illicit. If you do, this is a great way to monitor transaction volumes and look for new or unusual third-party applications that are managing users. If you see something unusual, contact the provider to determine if the action is legitimate.
Ensure non-global administrator role group assignments are reviewed at least weekly	**High**	**NonCompliant**	**IMPACT:** Auditing Process is not created and followed.Auditing Process needs to be created and followed. **ACTION:** You should review non-global administrator role group assignments at least every week. While these roles are less powerful than a global admin, they do grant special privileges that can be

			used illicitly. If you see something unusual, contact the user to confirm it is a legitimate need.
Ensure the spoofed domains report is review weekly	**High**	**NonCompliant**	**IMPACT:** Found Spoofed domains. Please review the list and take action accordingly.Auditing Process needs to be created and followed. **ACTION:** Use spoof intelligence in the Security Center on the Anti-spam settings page to review all senders who are spoofing either domains that are part of your organization or spoofing external domains. Spoof intelligence is available as part of Office 365 Enterprise E5 or separately as part of Defender for Office 365 and as of October 2018 Exchange Online Protection (EOP). Bad actors spoof domains to trick users into conducting actions they normally would not or should not via phishing emails. Running this report will inform the message administrators of current activities, and the phishing techniques used by bad actors. This information can be used to inform end users and plan against future campaigns.
Ensure Microsoft Defender for Cloud Apps is Enabled	**High**	**NonCompliant**	**IMPACT:** **ACTION:**
Ensure the report of users who have had their email privileges restricted due to spamming is reviewed	**High**	**NonCompliant**	**IMPACT:** Auditing Process is not created and followed.Auditing Process needs to be created and followed. **ACTION:** Microsoft 365 Defender reviews of Restricted Entities will provide a list of user accounts restricted from sending e-mail. If a user exceeds one of the outbound sending limits as specified in the service limits or in outbound spam policies, the user is restricted from sending email, but they can still receive email. Users who are found on the restricted users list have a high probability of having been compromised. Review of this list will allow an organization to remediate these user accounts, and then unblock them.
Ensure Guest Users are reviewed at least biweekly	**High**	**NonCompliant**	IMPACT: **Found Guest accounts found.Auditing Process needs to be created and followed. There is no impact if auditing process is created and followed.**

			ACTION: **Guest users can be set up for those users not in your tenant to still be granted access to resources. It is important to maintain visibility for what guest users are established in the tenant. Periodic review of guest users ensures proper access to resources in your tenant. To verify the report is being reviewed at least biweekly, confirm that the necessary procedures are in place and being followed.**

5.8 Storage

Test	Severity/risk	Compliance status	Remark
Ensure document sharing is being controlled by domains with whitelist or blacklist	**High**	**NonCompliant**	**IMPACT:** Document Sharing control for domains is not configured.Enabling this feature will prevent users from sharing documents with domains outside of the organization unless allowed. **ACTION:** You should control sharing of documents to external domains by either blocking domains or only allowing sharing with specific named domains. Enabling this feature will prevent users from sharing documents with domains outside of the organization unless allowed. Attackers will often attempt to expose sensitive information to external entities through sharing, and restricting the domains that your users can share documents with will reduce that surface area.
Block OneDrive for Business sync from unmanaged devices	**High**	**NonCompliant**	**IMPACT:** OneDrive For Business Sync from unmanaged Devices is not blocked.Enabling this feature will prevent users from using the OneDrive for Business Sync client on devices that are not joined to the domains that were defined. Enabling this feature will prevent users from using the OneDrive for Business Sync client on devices that are not joined to the domains that were defined. **ACTION:** Unmanaged devices pose a risk, since their security cannot be verified through existing security policies, brokers or endpoint protection. Allowing users to sync data to these devices takes that data out of the control of the organization. This increases the risk of the data either being intentionally or accidentally

			leaked. Note: This setting is only applicable to Active Directory domains when operating in a hybrid configuration. It does not apply to Azure AD domains. If you have devices which are only Azure AD joined, consider using a Conditional Access Policy instead.
Ensure expiration time for external sharing links is set	**High**	**NonCompliant**	**IMPACT:** Expiration time for External Sharing Links is not set.Enabling this feature will ensure that link expire within the defined number of days. This will have an effect on links that were previously not set with an expiration. **ACTION:** The external sharing features of Microsoft SharePoint let users in your organization share content with people outside the organization (such as partners, vendors, clients, or customers). External sharing in SharePoint is part of secure collaboration with Microsoft 365. An attacker can compromise a user account for a short period of time, send anonymous sharing links to an external account, then take their time accessing the data. They can also compromise external accounts and steal the anonymous sharing links sent to those external entities well after the data has been shared. Restricting how long the links are valid can reduce the window of opportunity for attackers.
Ensure external storage providers available in Outlook on the Web are restricted	**High**	**NonCompliant**	**IMPACT: External Storage Providers in Outlook on the Web are not restricted.Impact associated with this change is highly dependent upon current practices in the tenant. If users do not use other storage providers, then minimal impact is likely. However, if users do regularly utilize providers outside of the tenant this will affect their ability to continue to do so.** **ACTION: You should restrict storage providers that are integrated with Outlook on the Web. If users do regularly utilize providers outside of the tenant this will affect their ability to continue to do so. By default additional storage providers are allowed in Outlook on the Web (such as Box, Dropbox, Facebook, Google Drive, OneDrive Personal, etc.). This could lead to information leakage and additional risk of infection from organizational non-trusted storage providers. Restricting this will inherently reduce risk as it will narrow.**

5.9 Mobile Device Management

Test	Severity/risk	Compliance status	Remark
Ensure mobile device management policies are set to require advanced security configurations for Android Devices	High	NonCompliant	**IMPACT:** Mobile device management policies are not set to require advanced security configurations.The impact associated with this change is dependent upon the settings specified in the mobile device configuration profile. **ACTION:** You should configure your mobile device management policies to require advanced security configurations. If you do not require this, users will be able to connect from devices that are vulnerable to basic exploits, leading to potential breaches of accounts and data. Managing mobile devices in your organization helps provide a basic level of security to protect against attacks from these platforms. For example ensure that the device is up to date on patches or is not rooted. These configurations open those devices to vulnerabilities that are addressed in patched versions of the mobile OS.
Ensure mobile device management policies are set to require advanced security configurations for iOS Devices	High	NonCompliant	**IMPACT:** Mobile device management policies are not set to require advanced security configurations.The impact associated with this change is dependent upon the settings specified in the mobile device configuration profile. **ACTION:** You should configure your mobile device management policies to require advanced security configurations. If you do not require this, users will be able to connect from devices that are vulnerable to basic exploits, leading to potential breaches of accounts and data. Managing mobile devices in your organization, helps provide a basic level of security to protect against attacks from these platforms. For example ensure that the device is up to date on patches or is not rooted. These configurations open those devices to vulnerabilities that are addressed in patched versions of the mobile OS.

Ensure that mobile device password reuse is prohibited for Android Devices	**High**	**NonCompliant**	**IMPACT:** Mobile device password reuse is not prohibited or configured.This change will have a moderate user impact. **ACTION:** You should not allow your users to reuse the same password on their mobile devices. Devices without this protection are vulnerable to being accessed by attackers who can then steal account credentials, data, or install malware on the device. Choosing unique and unused passwords every time a password changes on mobile devices lessens the likelihood that the password can be guessed by an attacker.
Ensure that mobile device password reuse is prohibited for iOS Devices	**High**	**NonCompliant**	**IMPACT:** Mobile device password reuse is not prohibited or configured. This change will have a moderate user impact. **ACTION:** You should not allow your users to reuse the same password on their mobile devices. Devices without this protection are vulnerable to being accessed by attackers who can then steal account credentials, data, or install malware on the device. Choosing unique and unused passwords every time a password changes on mobile devices lessens the likelihood that the password can be guessed by an attacker.
Ensure that mobile devices are set to never expire passwords for Android Devices	**High**	**NonCompliant**	**IMPACT:** Mobile devices are set to never expire passwords is not configured. This setting should not cause a noticeable impact to users. **ACTION:** Ensure that users passwords on their mobile devices, never expire. While this is not the most intuitive recommendation, research has found that when periodic password resets are enforced, passwords become weaker as users tend to pick something weaker and then use a pattern of it for rotation. If a user creates a
Ensure that mobile devices are set to never expire passwords for iOS Devices	**High**	**NonCompliant**	**IMPACT:** Mobile devices are set to never expire passwords is not configured.This setting should not cause a noticeable impact to users. **ACTION:** Ensure that users passwords on their mobile devices, never expire. While this is not the most intuitive recommendation, research has found that when periodic password resets are

			enforced, passwords become weaker as users tend to pick something weaker and then use a pattern of it for rotation. If a user creates a
Ensure that users cannot connect from devices that are jail broken or rooted	**High**	**NonCompliant**	**IMPACT:** Ensure that users cannot connect from devices that are jail broken or rooted is not configured.Impact should be minimal however, in the event that a device is Jailbroken or running a developer build of a mobile Operating System it will be blocked from connecting. **ACTION:** You should not allow your users to use to connect with mobile devices that have been jail broken or rooted. These devices have had basic protections disabled to run software that is often malicious and could very easily lead to an account or data breach.
Ensure mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise for Android Devices	**High**	**NonCompliant**	**IMPACT:** Ensure mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise is not configured.This setting has no impact, unless a user mistypes their password multiple times and causes their device to wipe. In that case, it will have a high user impact. **ACTION:** Require mobile devices to wipe on multiple sign-in failures. Devices without this protection are vulnerable to being accessed physically by attackers who can then steal account credentials, data, or install malware on the device.
Ensure mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise for iOS Devices	**High**	**NonCompliant**	**IMPACT:** Ensure mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise is not configured.This setting has no impact, unless a user mistypes their password multiple times and causes their device to wipe. In that case, it will have a high user impact. **ACTION:** Require mobile devices to wipe on multiple sign-in failures. Devices without this protection are vulnerable to being accessed physically by attackers who can then steal account credentials, data, or install malware on the device.
Ensure that mobile devices require a minimum password length to prevent brute force attacks for Android Devices	**High**	**NonCompliant**	**IMPACT:** Ensure that mobile devices require a minimum password length to prevent brute force attacks is not configured.This change has potentially high user impact depending on the

			willingness and awareness of the end-user. **ACTION:** You should require your users to use a minimum password length of at least six characters to unlock their mobile devices. Devices without this protection are vulnerable to being accessed physically by attackers
Ensure that mobile devices require a minimum password length to prevent brute force attacks for iOS Devices	**High**	**NonCompliant**	**IMPACT:** Ensure that mobile devices require a minimum password length to prevent brute force attacks is not configured.This change has potentially high user impact depending on the willingness and awareness of the end-user. **ACTION:** You should require your users to use a minimum password length of at least six characters to unlock their mobile devices. Devices without this protection are vulnerable to being accessed physically by attackers
Ensure devices lock after a period of inactivity to prevent unauthorized access for Android Devices	**High**	**NonCompliant**	**IMPACT:** Ensure devices lock after a period of inactivity to prevent unauthorized access is not configured.This setting has a low impact on users. **ACTION:** You should require your users to configure their mobile devices to lock on inactivity. Attackers can steal unlocked devices and access data and account information.
Ensure devices lock after a period of inactivity to prevent unauthorized access for iOS Devices	**High**	**NonCompliant**	**IMPACT:** Ensure devices lock after a period of inactivity to prevent unauthorized access is not configured.This setting has a low impact on users. **ACTION:** You should require your users to configure their mobile devices to lock on inactivity. Attackers can steal unlocked devices and access data and account information.
Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data for Android Devices	**High**	**NonCompliant**	**IMPACT:** Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data is not configured.This setting should have no user impact, provided the device supports the feature. **ACTION:** You should require your users to use encryption on their mobile

			devices. Unencrypted devices can be stolen and their data extracted by an attacker very easily.
Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data for iOS Devices	**High**	**NonCompliant**	IMPACT: **Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data is not configured.This setting should have no user impact, provided the device supports the feature.** ACTION: **You should require your users to use encryption on their mobile devices. Unencrypted devices can be stolen, and their data extracted by an attacker very easily.**

APPENDIX-1: Passed/Completed Tests

After carrying out a complete health assessment of the ***Office 365 Environment***, the following Tests have been **passed**/completed sucessfully and no issues were found.

Category	Test	Risk	Finding

APPENDIX-2: Not Executed Tests

The following table lists the Tests that were not executed or error in executing

Test	CATEGORY