Microsoft Office 365 Assessment

Microsoft 365

By Smart Profiler

Version 6.2

ABC Consulting Services

Assessment date: {date of assessment}

Phone: {consulting firm Telephone}

Direct: {Direct phone}

Email: {Email Address}

Project: {enter project name here}

Effective Date: {enter project effective date here}
Customer: {enter customer name here}
Microsoft 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 ***Microsoft 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 Microsoft 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	{enter customer name here}
CUSTOMER ADDRESS	{enter customer address here}
CUSTOMER OPERATION BRANCHES	{enter customer operation branches here}
NUMBER OF EMPLOYEES	{enter number of employees here}

3. Participants

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

PARTICIPANT NAMES	COMPANY	PROJECT ROLE
{ENTER PARTICIPANT NAME HERE}	{enter Participant Company here}	{enter Participant Project Role here}
{ENTER PARTICIPANT NAME HERE}	{enter Participant Company here}	{enter Participant Project Role here}
{ENTER PARTICIPANT NAME HERE}	{enter Participant Company here}	{enter Participant Project Role here}

4. Recommendations

Organizations should be proactive in avoiding the risks and health issues associated with ***Microsoft 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 {enter customer name here}'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 **Microsoft 365 Compliance & Risks** section and actions to be taken accordingly.

5. Microsoft 365 Domain Passwords Policies

DOMAIN NAME	DOMAIN TYPE	NOTIFICATION DAYS	VALIDITY PERIOD
ITRISKSCAN.COM	MANAGED	14	2147483647
DYNAMICPACKS.NET	MANAGED	14	2147483647
ITRISKSCANNER.COM	MANAGED	14	2147483647
DYNAMICPACKSNET.ONMICROSOFT.COM	**MANAGED**	**14**	**2147483647**

6. CIS Assessment Status Table

The following table shows the status for each CIS Assessment performed.

CIS PDF Section	Profile Type	CIS Test	Assessment Type	Set Correctly?
M365 Admin Center-Users 1.1.1	E3 Level 1	Ensure Administrative accounts are separate and cloud-only	Automated	**Passed**
M365 Admin Center-Users 1.1.2	E3 Level 1	Ensure two emergency access accounts have been defined	Manual	**Passed**

M365 Admin Center-Users 1.1.3	E3 Level 1	Ensure that between two and four global admins are designated	Automated	**Passed**
M365 Admin Center-Users 1.1.4	E3 Level 1	Ensure Guest Users are reviewed at least biweekly	Automated	Failed
M365 Admin Center-Teams and Groups 1.2.1	E3 Level 2	Ensure that only organizationally managed-approved public groups exist	Automated	Failed
M365 Admin Center-Teams and Groups 1.2.2	E3 Level 1	Ensure sign-in to shared mailboxes is blocked	Automated	Failed
M365 Admin Center-Settings 1.3.1	E3 Level 1	Ensure the Password expiration policy is set to Set passwords to never expire (recommended)	Automated	**Passed**
M365 Admin Center-Settings 1.3.2	E3 Level 1	Ensure Idle session timeout is set to 3 hours (or less) for unmanaged devices	Manual	**Passed**
M365 Admin Center-Settings 1.3.3	E3 Level 2	Ensure calendar details sharing with external users is disabled	Automated	Failed
M365 Admin Center-Settings 1.3.4	E3 Level 1	Ensure User owned apps and services is restricted	Manual	**Passed**
M365 Admin Center-Settings 1.3.5	E3 Level 1	Ensure internal phishing protection for Forms is enabled	Manual	**Passed**
M365 Admin Center-Settings 1.3.6	E5 Level 2	Ensure the customer lockbox feature is enabled	Automated	Failed
M365 Admin Center-Settings 1.3.7	E3 Level 2	Ensure third-party storage services are restricted in Microsoft 365 on the web	Automated	Failed
M365 Admin Center-Settings 1.3.8	E3 Level 2	Ensure that Sways cannot be shared with people outside of your organization	Manual	**Passed**

Microsoft 365 Defender-Email and Collaboration 2.1.1	E5 Level 2	Ensure Safe Links for Office Applications is Enabled	Automated	Failed
Microsoft 365 Defender-Email and Collaboration 2.1.2	E3 Level 1	Ensure the Common Attachment Types Filter is enabled	Automated	Failed
Microsoft 365 Defender-Email and Collaboration 2.1.3	E3 Level 1	Ensure notifications for internal users sending malware is Enabled	Automated	Failed
Microsoft 365 Defender-Email and Collaboration 2.1.4	E5 Level 2	Ensure Safe Attachments policy is enabled	Automated	**Passed**
Microsoft 365 Defender-Email and Collaboration 2.1.5	E5 Level 2	Ensure Safe Attachments for SharePoint-OneDrive-Microsoft Teams is Enabled	Automated	Failed
Microsoft 365 Defender-Email and Collaboration 2.1.6	E3 Level 1	Ensure Exchange Online Spam Policies are set correctly	Automated	Failed
Microsoft 365 Defender-Email and Collaboration 2.1.7	E5 Level 1	Ensure that an anti-phishing policy has been created	Automated	**Passed**
Microsoft 365 Defender-Email and Collaboration 2.1.8	E3 Level 1	Ensure that SPF records are published for all Exchange Domains	Automated	Failed

Microsoft 365 Defender-Email and Collaboration 2.1.9	E3 Level 1	Ensure that DKIM is enabled for all Exchange Online Domains	Automated	Failed
Microsoft 365 Defender-Email and Collaboration 2.1.10	E3 Level 1	Ensure DMARC Records for all Exchange Online domains are published	Automated	Failed
Microsoft 365 Defender-Email and Collaboration 2.1.11	E5 Level 1	Ensure the spoofed domains report is review weekly	Automated	Failed
Microsoft 365 Defender-Email and Collaboration 2.1.12	E3 Level 1	Ensure the Restricted entities report is reviewed weekly	Automated	**Passed**
Microsoft 365 Defender-Email and Collaboration 2.1.13	E3 Level 1	Ensure all security threats in the Threat protection status report are reviewed at least weekly	Automated	Failed
Microsoft 365 Defender-Audit 2.3.1	E3 Level 1	Ensure the Account Provisioning Activity report is reviewed at least weekly	Automated	**Passed**
Microsoft 365 Defender-Audit 2.3.2	E3 Level 1	Ensure non-global administrator role group assignments are reviewed at least weekly	Automated	**Passed**
Microsoft 365 Defender-Settings 2.4.1	E5 Level 1	Ensure Priority account protection is enabled and configured	Automated	Failed
Microsoft 365 Defender-Settings 2.4.2	E5 Level 1	Ensure Priority accounts have Strict protection presets applied	Automated	Failed
Microsoft 365 Defender-Settings 2.4.3	E5 Level 2	Ensure Microsoft Defender for Cloud Apps is Enabled	Automated	**Passed**

Microsoft Purview-Audit 3.1.1	E3 Level 1	Ensure Microsoft 365 audit log search is Enabled	Automated	**Passed**
Microsoft Purview-Audit 3.1.2	E3 Level 1	Ensure user role group changes are reviewed at least weekly	Automated	**Passed**
Microsoft Purview-Data Loss Protection 3.2.1	E3 Level 1	Ensure DLP policies are enabled	Automated	Failed
Microsoft Purview-Data Loss Protection 3.2.2	E5 Level 1	Ensure DLP policies are enabled for Microsoft Teams	Automated	Failed
Microsoft Purview-Information Protection 3.3.1	E3 Level 1	Ensure SharePoint Online Information Protection policies are set up and used	Automated	Failed
Microsoft Entra admin center-Identity-Overview 5.1.1.1	E3 Level 1	Ensure Security Defaults is disabled on Azure Active Directory	Automated	**Passed**
Microsoft Entra admin center-Identity-Users 5.1.2.1	E3 Level 1	Ensure Per-user MFA is disabled	Automated	**Passed**
Microsoft Entra admin center-Identity-Users 5.1.2.2	E3 Level 2	Ensure third party integrated applications are not allowed	Automated	Failed
Microsoft Entra admin center-Identity-Users 5.1.2.3	E3 Level 1	Ensure Restrict non-admin users from creating tenants is set to Yes	Automated	Failed
Microsoft Entra admin center-Identity-Users 5.1.2.4	E3 Level 1	Ensure Restrict access to the Azure AD administration portal is set to Yes	Automated	Failed

Microsoft Entra admin center-Identity-Users 5.1.2.5	E3 Level 2	Ensure the option to remain signed in is hidden	Automated	Failed
Microsoft Entra admin center-Identity-Users 5.1.2.6	E3 Level 2	Ensure LinkedIn account connections is disabled	Automated	Failed
Microsoft Entra admin center-Identity-Groups 5.1.3.1	E3 Level 1	Ensure a dynamic group for guest users is created	Automated	Failed
Microsoft Entra admin center-Identity-Applications 5.1.5.1	E3 Level 1	Ensure the Application Usage report is reviewed at least weekly	Automated	Failed
Microsoft Entra admin center-Identity-Applications 5.1.5.2	E3 Level 2	Ensure user consent to apps accessing company data on their behalf is not allowed	Automated	Failed
Microsoft Entra admin center-Identity-Applications 5.1.5.3	E3 Level 1	Ensure the admin consent workflow is enabled	Automated	Failed
Microsoft Entra admin center-Identity-External Identities 5.1.6.1	E3 Level 2	Ensure that collaboration invitations are sent to allowed domains only	Automated	Failed
Microsoft Entra admin center-Identity-Hybrid Management 5.1.8.1	E3 Level 1	Ensure that password hash sync is enabled for hybrid deployments	Automated	Failed
Microsoft Entra admin center-Protection-	E3 Level 1	Ensure multifactor authentication is enabled for all users in administrative roles	Automated	Failed

Conditional Access 5.2.2.1				
Microsoft Entra admin center- Protection- Conditional Access 5.2.2.2	E3 Level 1	Ensure multifactor authentication is enabled for all users	Automated	Failed
Microsoft Entra admin center- Protection- Conditional Access 5.2.2.3	E3 Level 1	Enable Conditional Access policies to block legacy authentication	Automated	Failed
Microsoft Entra admin center- Protection- Conditional Access 5.2.2.4	E3 Level 1	Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users	Automated	Failed
Microsoft Entra admin center- Protection- Conditional Access 5.2.2.5	E3 Level 2	Ensure Phishing-resistant MFA strength is required for Administrators	Automated	Failed
Microsoft Entra admin center- Protection- Conditional Access 5.2.2.6	E5 Level 2	Enable Azure AD Identity Protection user risk policies	Automated	Failed
Microsoft Entra admin center- Protection- Conditional Access 5.2.2.7	E5 Level 2	Enable Azure AD Identity Protection sign-in risk policies	Automated	Failed
Microsoft Entra admin center- Protection- Conditional Access 5.2.2.8	E3 Level 1	Ensure Microsoft Azure Management is limited to administrative roles	Automated	Failed
Microsoft Entra admin center- Protection-	E3 Level 1	Ensure Microsoft Authenticator is configured to protect against MFA fatigue	Automated	Failed

Authentication Methods 5.2.3.1				
Microsoft Entra admin center-Protection-Authentication Methods 5.2.3.2	E3 Level 1	Ensure custom banned passwords lists are used	Automated	Failed
Microsoft Entra admin center-Protection-Authentication Methods 5.2.3.3	E3 Level 1	Ensure that password protection is enabled for Active Directory	Manual	**Passed**
Microsoft Entra admin center-Protection-Password Reset 5.2.4.1	E3 Level 1	Ensure Self service password reset enabled is set to All	Automated	**Passed**
Microsoft Entra admin center-Protection-Password Reset 5.2.4.2	E3 Level 1	Ensure the self-service password reset activity report is reviewed at least weekly	Automated	**Passed**
Microsoft Entra admin center-Protection-Risk Activities 5.2.6.1	E3 Level 1	Ensure the Azure AD Risky sign-ins report is reviewed at least weekly	Automated	**Passed**
Microsoft Entra admin center-Identity Governance 5.3.1	E5 Level 2	Ensure Privileged Identity Management is used to manage roles	Automated	**Passed**
Microsoft Entra admin center-Identity Governance 5.3.2	E5 Level 2	Ensure Access reviews for Guest Users are configured	Manual	**Passed**
Microsoft Entra admin center-Identity	E5 Level 1	Ensure Access reviews for high privileged Azure AD roles are configured	Manual	**Passed**

Governance 5.3.3				
Microsoft Exchange admin center-Audit 6.1.1	E3 Level 1	Ensure AuditDisabled organizationally is set to False	Automated	**Passed**
Microsoft Exchange admin center-Audit 6.1.2	E3 Level 1	Ensure mailbox auditing for E3 users is Enabled	Automated	**Passed**
Microsoft Exchange admin center-Audit 6.1.3	E5 Level 1	Ensure mailbox auditing for E5 users is Enabled	Automated	**Passed**
Microsoft Exchange admin center-Audit 6.1.4	E3 Level 1	Ensure AuditBypassEnabled is not enabled on mailboxes	Automated	Failed
Microsoft Exchange admin center-Mailflow 6.2.1	E3 Level 1	Ensure all forms of mail forwarding are blocked and-or disabled	Automated	**Passed**
Microsoft Exchange admin center-Mailflow 6.2.2	E3 Level 1	Ensure mail transport rules do not whitelist specific domains	Automated	**Passed**
Microsoft Exchange admin center-Mailflow 6.2.3	E3 Level 1	Ensure Tagging is enabled for External Emails	Automated	Failed
Microsoft Exchange admin center-Mailflow NA	E3 Level 1	Ensure Tagging does not allow specific domains	Automated	**Passed**
Microsoft Exchange admin center-Roles 6.3.1	E3 Level 2	Ensure users installing Outlook add-ins is not allowed	Automated	Failed
Microsoft Exchange admin	E3 Level 1	Ensure mail forwarding rules are reviewed at least weekly	Automated	**Passed**

center-Reports 6.4.1				
Microsoft Exchange admin center-Settings 6.5.1	E3 Level 1	Ensure modern authentication for Exchange Online is enabled	Automated	**Passed**
Microsoft Exchange admin center-Settings 6.5.2	E3 Level 2	Ensure MailTips are enabled for end users	Automated	Failed
Microsoft Exchange admin center-Settings 6.5.3	E3 Level 2	Ensure external storage providers available in Outlook on the Web are restricted	Automated	Failed
Microsoft SharePoint Admin Center-Policies 7.2.1	E3 Level 1	Ensure modern authentication for SharePoint applications is required	Automated	Failed
Microsoft SharePoint Admin Center-Policies 7.2.2	E3 Level 1	Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled	Automated	**Passed**
Microsoft SharePoint Admin Center-Policies 7.2.3	E3 Level 1	Ensure external content sharing is restricted	Automated	Failed
Microsoft SharePoint Admin Center-Policies 7.2.4	E3 Level 2	Ensure OneDrive content sharing is restricted	Automated	**Passed**
Microsoft SharePoint Admin Center-Policies 7.2.5	E3 Level 2	Ensure that SharePoint guest users cannot share items they dont own	Automated	Failed
Microsoft SharePoint Admin Center-Policies 7.2.7	E3 Level 1	Ensure link sharing is restricted in SharePoint and OneDrive	Automated	**Passed**
Microsoft SharePoint	E3 Level 2	Ensure external sharing is restricted by security group	Automated	**Passed**

Admin Center-Policies 7.2.8				
Microsoft SharePoint Admin Center-Policies 7.2.9	E3 Level 1	Ensure expiration time for external sharing links is set	Automated	**Passed**
Microsoft SharePoint Admin Center-Policies 7.2.10	E3 Level 1	Ensure reauthentication with verification code is restricted	Automated	**Passed**
Microsoft SharePoint Admin Center-Settings 7.3.1	E5 Level 2	Ensure Microsoft 365 SharePoint infected files are disallowed for download	Automated	Failed
Microsoft SharePoint Admin Center-Settings 7.3.2	E3 Level 2	Block OneDrive for Business sync from unmanaged devices	Automated	Failed
Microsoft SharePoint Admin Center-Settings 7.3.3	E3 Level 1	Ensure custom script execution is restricted on personal sites	Automated	Failed
Microsoft SharePoint Admin Center-Settings 7.3.4	E3 Level 1	Ensure custom script execution is restricted on site collections	Automated	**Passed**
Microsoft Teams Admin Center-Teams 8.1.1	E3 Level 2	Ensure external file sharing in Teams is enabled for only approved cloud storage services	Automated	Failed
Microsoft Teams Admin Center-Teams 8.1.2	E3 Level 1	Ensure users cant send emails to a channel email address	Automated	**Passed**
Microsoft Teams Admin Center-Users 8.2.1	E3 Level 2	Ensure external access is restricted in the Teams admin center	Automated	**Passed**
Microsoft Teams Admin	E3 Level 1	Ensure app permission policies are configured	Automated	Failed

Center-Teams Apps 8.4.1				
Microsoft Teams Admin Center-Meetings 8.5.1	E3 Level 2	Ensure anonymous users cant join a meeting	Automated	**Passed**
Microsoft Teams Admin Center-Meetings 8.5.2	E3 Level 1	Ensure anonymous users and dial-in callers cant start a meeting	Automated	**Passed**
Microsoft Teams Admin Center-Meetings 8.5.3	E3 Level 1	Ensure only people in my org can bypass the lobby	Automated	**Passed**
Microsoft Teams Admin Center-Meetings 8.5.4	E3 Level 1	Ensure users dialing in cant bypass the lobby	Automated	**Passed**
Microsoft Teams Admin Center-Meetings 8.5.5	E3 Level 1	Ensure meeting chat does not allow anonymous users	Automated	**Passed**
Microsoft Teams Admin Center-Meetings 8.5.6	E3 Level 1	Ensure only organizers and co-organizers can present	Automated	**Passed**
Microsoft Teams Admin Center-Meetings 8.5.7	E3 Level 1	Ensure external participants cant give or request control	Automated	**Passed**
Microsoft Teams Admin Center-Messaging 8.6.1	E3 Level 1	Ensure users can report security concerns in Teams	Automated	**Passed**
Microsoft Fabric-Tenant Settings 9.1.1	E3 Level 1	Ensure guest user access is restricted	Automated	Failed
Microsoft Fabric-Tenant Settings 9.1.2	E3 Level 1	Ensure external user invitations are restricted	Automated	Failed

Microsoft Fabric-Tenant Settings 9.1.3	E3 Level 1	Ensure guest access to content is restricted	Manual	**Passed**
Microsoft Fabric-Tenant Settings 9.1.4	E3 Level 1	Ensure Publish to web is restricted	Manual	**Passed**
Microsoft Fabric-Tenant Settings 9.1.5	E3 Level 2	Ensure Interact with and share R and Python visuals is Disabled	Manual	**Passed**
Microsoft Fabric-Tenant Settings 9.1.6	E3 Level 1	Ensure Allow users to apply sensitivity labels for content is Enabled	Automated	**Passed**
Microsoft Fabric-Tenant Settings 9.1.7	E3 Level 1	Ensure shareable links are restricted	Manual	**Passed**
Microsoft Fabric-Tenant Settings 9.1.8	E3 Level 1	Ensure enabling of external data sharing is restricted	Manual	**Passed**
Microsoft Fabric-Tenant Settings 9.1.9	**E3 Level 1**	**Ensure Block ResourceKey Authentication is Enabled**	**Manual**	**Passed**

7. Reported Items Per Test

The following table shows the items that have been reported Per Microsoft 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. Note that the table below might also include tests that belong to SmartProfiler Version 1.0.

Category	Control	Profile Type	Test	Risk	Items
M365 Admin Center-Users	CIS v3.0	E3 Level 1	Ensure Administrative accounts are separate and cloud-only	**Passed**	Sync-In Admins: 0
M365 Admin Center-Users	CIS v3.0	E3 Level 1	Ensure that between two and four global admins are designated	**Passed**	Total Global Admins: 4
M365 Admin Center-Users	CIS v3.0	E3 Level 1	Ensure Guest Users are reviewed at least biweekly	**Medium**	Guest Accounts: 6

M365 Admin Center-Accounts and Authentication	SP v1.0		Ensure Azure Information Protection-AIP is enabled at Global Level	**High**	Status: Not Enabled
M365 Admin Center-Accounts and Authentication	SP v1.0		Ensure Microsoft 365 User Roles have less than 10 Admins	**Passed**	More than 10 Admins: 0
M365 Admin Center-Accounts and Authentication	SP v1.0		Ensure Microsoft 365 Users Have Strong Password Requirements Configured	**Passed**	Users With Weak Password Requirements: 0
M365 Admin Center-Accounts and Authentication	SP v1.0		Ensure self-service password reset is enabled	**Passed**	Status: Enabled
M365 Admin Center-Accounts and Authentication	SP v1.0		Ensure that Microsoft 365 Passwords Are Not Set to Expire	**Passed**	Missing Password Policies Domains: 0
M365 Admin Center-Accounts and Authentication	SP v1.0		Ensure modern authentication for Teams Online is enabled	**High**	Status: Not Enabled
M365 Admin Center-Accounts and Authentication	SP v1.0		Ensure Microsoft 365 Exchange Online Modern Authentication is Used	**Passed**	Status: Enabled
M365 Admin Center-Accounts and Authentication	SP v1.0		Ensure Microsoft 365 Exchange Online Privileged Access Management is Used	**High**	Status: Not Enabled
M365 Admin Center-Auditing	SP v1.0		Ensure Enterprise Applications Role Assignments are reviewed weekly	**High**	Apps Role Assignments: 7
M365 Admin Center-Teams and Groups	CIS v3.0	E3 Level 2	Ensure that only organizationally managed-approved public groups exist	**Medium**	Public Groups: 1

M365 Admin Center-Teams and Groups	CIS v3.0	E3 Level 1	Ensure sign-in to shared mailboxes is blocked	**Medium**	Sign-In Allowed for Total SharedMailbox: Not Sharedmailbox Found
M365 Admin Center-Settings	CIS v3.0	E3 Level 1	Ensure the Password expiration policy is set to Set passwords to never expire (recommended)	**Passed**	Missing Password Policies Domains: 0
M365 Admin Center-Settings	CIS v3.0	E3 Level 2	Ensure calendar details sharing with external users is disabled	**High**	Status: Enabled
M365 Admin Center-Settings	CIS v3.0	E5 Level 2	Ensure the customer lockbox feature is enabled	**Medium**	Status: Disabled
M365 Admin Center-Settings	CIS v3.0	E3 Level 2	Ensure third-party storage services are restricted in Microsoft 365 on the web	**High**	Status: Not Restricted
Microsoft 365 Defender-Email and Collaboration	CIS v3.0	E5 Level 2	Ensure Safe Links for Office Applications is Enabled	**High**	Status: Not Enabled
Microsoft 365 Defender-Email and Collaboration	CIS v3.0	E3 Level 1	Ensure the Common Attachment Types Filter is enabled	**High**	Status: Not Enabled
Microsoft 365 Defender-Email and Collaboration	CIS v3.0	E3 Level 1	Ensure notifications for internal users sending malware is Enabled	**High**	Status: Not Enabled
Microsoft 365 Defender-Email and Collaboration	CIS v3.0	E5 Level 2	Ensure Safe Attachments policy is enabled	**Passed**	Status: Not Enabled-Not Implemented
Microsoft 365 Defender-Email and Collaboration	CIS v3.0	E5 Level 2	Ensure Safe Attachments for SharePoint-OneDrive-Microsoft Teams is Enabled	**Medium**	Status: Not Enabled-Not Implemented
Microsoft 365 Defender-Email and Collaboration	CIS v3.0	E3 Level 1	Ensure Exchange Online Spam Policies are set correctly	**High**	Status: Not Enabled
Microsoft 365 Defender-Email	CIS v3.0	E5 Level 1	Ensure that an anti-phishing policy has been created	**Passed**	Status: Created

and Collaboration					
Microsoft 365 Defender-Email and Collaboration	CIS v3.0	E3 Level 1	Ensure that SPF records are published for all Exchange Domains	**Medium**	Domains Missing SPF Records: 4
Microsoft 365 Defender-Email and Collaboration	SP v1.0		Ensure No Domains with SPF Soft Fail are Configured	**Passed**	Status: Not Configured
Microsoft 365 Defender-Email and Collaboration	CIS v3.0	E3 Level 1	Ensure that DKIM is enabled for all Exchange Online Domains	**High**	Domains Missing DKIM: 3
Microsoft 365 Defender-Email and Collaboration	CIS v3.0	E3 Level 1	Ensure DMARC Records for all Exchange Online domains are published	**High**	Missing Domains for DMARC Records: 4
Microsoft 365 Defender-Email and Collaboration	CIS v3.0	E5 Level 1	Ensure the spoofed domains report is review weekly	**Medium**	Spoofed Domains: 10
Microsoft 365 Defender-Email and Collaboration	CIS v3.0	E3 Level 1	Ensure the Restricted entities report is reviewed weekly	**Passed**	Status: There are no Restricted users at present
Microsoft 365 Defender-Email and Collaboration	CIS v3.0	E3 Level 1	Ensure all security threats in the Threat protection status report are reviewed at least weekly	**High**	Status: Security Threats Found in Malware Report
Microsoft 365 Defender-Audit	CIS v3.0	E3 Level 1	Ensure the Account Provisioning Activity report is reviewed at least weekly	**Passed**	Account Provisioning Items: 0
Microsoft 365 Defender-Audit	CIS v3.0	E3 Level 1	Ensure non-global administrator role group assignments are reviewed at least weekly	**Passed**	Status: There are no non-admin Global Role assignments found in past 7 days
Microsoft 365 Defender-Settings	CIS v3.0	E5 Level 1	Ensure Priority account protection is enabled and configured	**High**	Priority Account Status: Not Enabled-Not Implemented

Microsoft 365 Defender-Settings	CIS v3.0	E5 Level 1	Ensure Priority accounts have Strict protection presets applied	**High**	Status: Not Enabled-Not Implemented
Microsoft 365 Defender-Settings	CIS v3.0	E5 Level 2	Ensure Microsoft Defender for Cloud Apps is Enabled	**Passed**	Status: Enabled
Microsoft Purview-Audit	CIS v3.0	E3 Level 1	Ensure Microsoft 365 audit log search is Enabled	**Passed**	Status: Enabled
Microsoft Purview-Audit	CIS v3.0	E3 Level 1	Ensure user role group changes are reviewed at least weekly	**Passed**	Status: There are no user role group changes found in past 7 days
Microsoft Purview-Data Loss Protection	CIS v3.0	E3 Level 1	Ensure DLP policies are enabled	**High**	Status: The DLP Policy is NOT Enabled
Microsoft Purview-Data Loss Protection	CIS v3.0	E5 Level 1	Ensure DLP policies are enabled for Microsoft Teams	**High**	Status: No DLP Policy Found
Microsoft Purview-Data Loss Protection	SP v1.0		Ensure DLP Policy is enabled for OneDrive	**High**	Status: Not Enabled
Microsoft Purview-Data Loss Protection	SP v1.0		Ensure DLP Policy is configured for SharePoint	**High**	Status: Not Enabled
Microsoft Purview-Data Loss Protection	SP v1.0		Ensure Custom Anti-Malware Policy is Present	**High**	Status: Not Defined
Microsoft Purview-Data Loss Protection	SP v1.0		Ensure Custom Anti-Phishing Policy is Present	**High**	Status: Not Defined
Microsoft Purview-Data Loss Protection	SP v1.0		Ensure Custom DLP Policies are Present	**High**	Status: Not Defined-Not Implemented
Microsoft Purview-Data Loss Protection	SP v1.0		Ensure Custom DLP Sensitive Information Types are Defined	**High**	Status: Not Defined-Not Implemented
Microsoft Purview-Information Protection	CIS v3.0	E3 Level 1	Ensure SharePoint Online Information Protection policies are set up and used	**High**	Status: Policies were published on 0 of the 8319 users

Microsoft Entra admin center-Identity-Overview	CIS v3.0	E3 Level 1	Ensure Security Defaults is disabled on Azure Active Directory	**Passed**	Status: Security Defaults are disabled.
Microsoft Entra admin center-Identity-Users	CIS v3.0	E3 Level 1	Ensure Per-user MFA is disabled	**Passed**	Total Per-User MFA Enabled: 0
Microsoft Entra admin center-Identity-Users	CIS v3.0	E3 Level 2	Ensure third party integrated applications are not allowed	**High**	Status: Allowed
Microsoft Entra admin center-Identity-Users	CIS v3.0	E3 Level 1	Ensure Restrict non-admin users from creating tenants is set to Yes	**High**	Permission Status: Enabled-Not Ok
Microsoft Entra admin center-Identity-Users	CIS v3.0	E3 Level 1	Ensure Restrict access to the Azure AD administration portal is set to Yes	**High**	Permission Status: No Policy Found
Microsoft Entra admin center-Identity-Users	CIS v3.0	E3 Level 2	Ensure the option to remain signed in is hidden	**Medium**	Status: No Branding Policies Found
Microsoft Entra admin center-Identity-Users	CIS v3.0	E3 Level 2	Ensure LinkedIn account connections is disabled	**High**	Status: Enabled
Microsoft Entra admin center-Identity-Groups	CIS v3.0	E3 Level 1	Ensure a dynamic group for guest users is created	**High**	Status: LinkedIn Account Connections is enabled
Microsoft Entra admin center-Identity-Applications	CIS v3.0	E3 Level 1	Ensure the Application Usage report is reviewed at least weekly	**Medium**	Azure Applications: 9
Microsoft Entra admin center-Identity-Applications	CIS v3.0	E3 Level 2	Ensure user consent to apps accessing company data on their behalf is not allowed	**Medium**	Status: Allowed
Microsoft Entra admin center-Identity-Applications	CIS v3.0	E3 Level 1	Ensure the admin consent workflow is enabled	**High**	Status: WARNING: Not Enabled for Graph App
Microsoft Entra admin center-	CIS v3.0	E3 Level 2	Ensure that collaboration invitations are sent to allowed domains only	**Medium**	Status: Enabled-No Policy Configured

Identity-External Identities					
Microsoft Entra admin center-Identity-Hybrid Management	CIS v3.0	E3 Level 1	Ensure that password hash sync is enabled for hybrid deployments	**Medium**	Status: On-Premises Sync is not enabled.
Microsoft Entra admin center-Protection-Conditional Access	CIS v3.0	E3 Level 1	Ensure multifactor authentication is enabled for all users in administrative roles	**High**	Admins Without MFA: You have 5 out of 5 users with administrative roles that aren?t registered and protected with MFA.
Microsoft Entra admin center-Protection-Conditional Access	CIS v3.0	E3 Level 1	Ensure multifactor authentication is enabled for all users	**High**	Status: Multifactor Authentication is not enabled for all users
Microsoft Entra admin center-Protection-Conditional Access	CIS v3.0	E3 Level 1	Enable Conditional Access policies to block legacy authentication	**High**	Block Legacy Authentication Status: You have 8327 of 8327 users that don’t have legacy authentication blocked.
Microsoft Entra admin center-Protection-Conditional Access	CIS v3.0	E3 Level 1	Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users	**High**	Status: Not Configured
Microsoft Entra admin center-Protection-Conditional Access	CIS v3.0	E3 Level 2	Ensure Phishing-resistant MFA strength is required for Administrators	**High**	Status: Phishing-resistant MFA policy is not configured for administrators
Microsoft Entra admin center-Protection-Conditional Access	CIS v3.0	E5 Level 2	Enable Azure AD Identity Protection user risk policies	**High**	Status: No Protection User Risk Policies found
Microsoft Entra admin center-Protection-	CIS v3.0	E5 Level 2	Enable Azure AD Identity Protection sign-in risk policies	**High**	Status: No Sign-In Risk Policies found

Conditional Access					
Microsoft Entra admin center-Protection-Conditional Access	CIS v3.0	E3 Level 1	Ensure Microsoft Azure Management is limited to administrative roles	**High**	Permission Status: No Policy Found
Microsoft Entra admin center-Protection-Authentication Methods	CIS v3.0	E3 Level 1	Ensure Microsoft Authenticator is configured to protect against MFA fatigue	**High**	Status: Microsoft Authenticator is disabled.
Microsoft Entra admin center-Protection-Authentication Methods	CIS v3.0	E3 Level 1	Ensure custom banned passwords lists are used	**High**	Status: Custom banned passwords setting is disabled.
Microsoft Entra admin center-Protection-Password Reset	CIS v3.0	E3 Level 1	Ensure Self service password reset enabled is set to All	**Passed**	Self-Service Password Status: You have 0 of 0 users who don't have self-service password reset enabled.
Microsoft Entra admin center-Protection-Password Reset	CIS v3.0	E3 Level 1	Ensure the self-service password reset activity report is reviewed at least weekly	**Passed**	Status: Changed Password Found via SSPR
Microsoft Entra admin center-Protection-Risk Activities	CIS v3.0	E3 Level 1	Ensure the Azure AD Risky sign-ins report is reviewed at least weekly	**Passed**	Status: No Risky user found
Microsoft Entra admin center-Identity Governance	SP v1.0		Use Just In Time privileged access to Microsoft 365 roles	**High**	Status: WARNING: JIT Not Enabled for Graph App
Microsoft Entra admin center-Identity Governance	CIS v3.0	E5 Level 2	Ensure Privileged Identity Management is used to manage roles	**Passed**	Status: No permanent active role assignments found.
Microsoft Exchange	CIS v3.0	E3 Level 1	Ensure AuditDisabled organizationally is set to False	**Passed**	Status: Enabled

admin center-Audit					
Microsoft Exchange admin center-Audit	CIS v3.0	E3 Level 1	Ensure mailbox auditing for E3 users is Enabled	**Passed**	Missing Mailbox Auditing: 0
Microsoft Exchange admin center-Audit	CIS v3.0	E5 Level 1	Ensure mailbox auditing for E5 users is Enabled	**Passed**	Missing Mailbox Auditing: 0
Microsoft Exchange admin center-Audit	CIS v3.0	E3 Level 1	Ensure AuditBypassEnabled is not enabled on mailboxes	**High**	Status: AuditBypass is enabled on some mailboxes
Microsoft Exchange admin center-Audit	SP v1.0		Ensure Microsoft 365 Exchange Online Admin Auditing Is Enabled	**Passed**	Status: Enabled
Microsoft Exchange admin center-Audit	SP v1.0		Ensure Microsoft 365 Exchange Online Unified Auditing Is Enabled	**Passed**	Status: Enabled
Microsoft Exchange admin center-Mailflow	CIS v3.0	E3 Level 1	Ensure all forms of mail forwarding are blocked and-or disabled	**Passed**	Mails Forwarding Rules Enabled: 0
Microsoft Exchange admin center-Mailflow	CIS v3.0	E3 Level 1	Ensure mail transport rules do not whitelist specific domains	**Passed**	Whitelist Domains: 0
Microsoft Exchange admin center-Mailflow	CIS v3.0	E3 Level 1	Ensure Tagging is enabled for External Emails	**High**	Status: Disabled
Microsoft Exchange admin center-Mailflow	CIS v3.0	E3 Level 1	Ensure Tagging does not allow specific domains	**Passed**	Tagging Allowed Domains: 0
Microsoft Exchange	SP v1.0		Ensure Transport Rules to Block Exchange Auto-Forwarding is configured	**High**	Status: Not Configured

admin center-Mailflow				
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Do Not Bypass the Safe Attachments Filter is not configured	**Passed**	Status: Not Configured
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Do Not Bypass the Safe Links Feature is not configured	**Passed**	Status: Not Configured
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Exchange Modern Authentication is Enabled	**Passed**	Status: Enabled
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Transport Rules to Block Executable Attachments are configured	**Passed**	Status: Configured
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Malware Filter Policies Alert for Internal Users Sending Malware is configured	**Passed**	Status: Configured
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Transport Rules to Block Large Attachments are configured	**Passed**	Status: Configured
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Mailbox Auditing is Enabled at Tenant Level	**Passed**	Status: Enabled
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Mailboxes without Mailbox Auditing are not present	**Passed**	Mailboxes Without Auditing: 0
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Exchange Mailboxes with IMAP is not Enabled	**Passed**	Status: No Mailboxes with IMAP
Microsoft Exchange	SP v1.0	Ensure Exchange Online Mailboxes with SMTP Authentication is not Enabled	**High**	Status: Not Enabled

admin center-Mailflow				
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Safe Attachments is Enabled	**High**	Status: Not Configured - No ATP License
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Safe Links is Enabled	**High**	Status: Not Configured - No ATP License
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Safe Links Click-Through is Not Allowed	**High**	Status: Not Configured - No ATP License
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure Safe Links Flags Links in Real Time	**High**	Status: Not Configured - No ATP License
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure SMTP Authentication is disabled Globally	**High**	Status: Not Disabled
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure mail transport rules do not forward email to external domains	**Passed**	Mails Forwarding Rules Enabled: 0
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure automatic forwarding options are disabled	**High**	Status: Not Disabled
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure the Client Rules Forwarding Block is enabled	**High**	Status: Disabled
Microsoft Exchange admin center-Mailflow	SP v1.0	Ensure the Advanced Threat Protection Safe Links policy is enabled	**Passed**	Status: Not Enabled-Not Implemented
Microsoft Exchange	SP v1.0	Ensure the Advanced Threat Protection SafeAttachments policy is enabled	**Passed**	Status: Not Enabled-Not Implemented

admin center-Mailflow					
Microsoft Exchange admin center-Mailflow	SP v1.0		Ensure that an anti-phishing policy has been created	**Passed**	Status: Created
Microsoft Exchange admin center-Mailflow	SP v1.0		Ensure mailbox auditing for all users is Enabled	**Passed**	Missing Mailbox Auditing: 0
Microsoft Exchange admin center-Roles	CIS v3.0	E3 Level 2	Ensure users installing Outlook add-ins is not allowed	**High**	Status: Allowed to Install Outlook Add-in
Microsoft Exchange admin center-Reports	CIS v3.0	E3 Level 1	Ensure mail forwarding rules are reviewed at least weekly	**Passed**	Forwarding Rules To External Domains: 0
Microsoft Exchange admin center-Reports	SP v1.0		Ensure the Malware Detections report is reviewed at least weekly	**Passed**	Malware Report Items: 0
Microsoft Exchange admin center-Reports	SP v1.0		Ensure Microsoft 365 Deleted Mailboxes are identified and Verified	**Passed**	Deleted Mailboxes: 0
Microsoft Exchange admin center-Reports	SP v1.0		Ensure Microsoft 365 Hidden Mailboxes are Identified	**Passed**	Hidden Mailboxes: 0
Microsoft Exchange admin center-Reports	SP v1.0		Ensure Mailboxes External Address Forwarding is not configured	**Passed**	Mailboxes Forwarding To External Domains: 0
Microsoft Exchange admin center-Reports	SP v1.0		Ensure Exchange Online Mailboxes on Litigation Hold	**Passed**	Mailboxes On Litigation Hold: 0
Microsoft Exchange	SP v1.0		Ensure Exchange Online SPAM Domains are identified	**High**	Inbound and Outbound SPAM Items: 2

admin center-Reports					
Microsoft Exchange admin center-Reports	SP v1.0		Ensure Exchange Online Mailbox Auditing is enabled	**Passed**	Mailboxes Without Auditing: 0
Microsoft Exchange admin center-Reports	SP v1.0		Microsoft 365 Exchange Online Admin Success and Failure Attempts	**Passed**	Failures for Online Admins: 0
Microsoft Exchange admin center-Reports	SP v1.0		Microsoft 365 Exchange Online External Access Admin Success and Failure Attempts	**Passed**	Failures for External Admins: 0
Microsoft Exchange admin center-Settings	CIS v3.0	E3 Level 1	Ensure modern authentication for Exchange Online is enabled	**Passed**	Status: Enabled
Microsoft Exchange admin center-Settings	CIS v3.0	E3 Level 2	Ensure MailTips are enabled for end users	**Medium**	Status: Not All MailTips Enabled
Microsoft Exchange admin center-Settings	CIS v3.0	E3 Level 2	Ensure external storage providers available in Outlook on the Web are restricted	**Medium**	Status: Not Restricted
Microsoft Exchange admin center-Settings	SP v1.0		Ensure Email Security Checks are Bypassed Based on Sender Domain are not configured	**High**	Status: Configured
Microsoft Exchange admin center-Settings	SP v1.0		Ensure Email Security Checks are Bypassed Based on Sender IP are not configured	**High**	Status: Configured
Microsoft Exchange admin center-Settings	SP v1.0		Ensure No Exchange Mailboxes with FullAccess Delegates are present	**High**	Number of Mailboxes with FullAccess Delegates: 0
Microsoft Exchange	SP v1.0		Ensure No Exchange Mailboxes with SendAs Delegates are present	**High**	Number of Mailboxes with SendAs Delegates:

admin center-Settings					
Microsoft Exchange admin center-Settings	SP v1.0		Ensure No Exchange Mailboxes with SendOnBehalfOf Delegates are present	**High**	Number of Mailboxes with SendOnBehalfOf Delegates: 3266
Microsoft SharePoint Admin Center-Policies	CIS v3.0	E3 Level 1	Ensure modern authentication for SharePoint applications is required	**High**	Status: Disabled
Microsoft SharePoint Admin Center-Policies	CIS v3.0	E3 Level 1	Ensure external content sharing is restricted	**High**	Status: Enabled
Microsoft SharePoint Admin Center-Policies	CIS v3.0	E3 Level 2	Ensure that SharePoint guest users cannot share items they dont own	**High**	Status: Not Enabled
Microsoft SharePoint Admin Center-Policies	SP v1.0		Ensure document sharing is being controlled by domains with whitelist or blacklist	**Passed**	Status: Controlled
Microsoft SharePoint Admin Center-Policies	CIS v3.0	E3 Level 1	Ensure expiration time for external sharing links is set	**Passed**	Status: Expiration Time for Links Is Set to
Microsoft SharePoint Admin Center-Settings	CIS v3.0	E5 Level 2	Ensure Microsoft 365 SharePoint infected files are disallowed for download	**High**	Status: WARNING: Allowed
Microsoft SharePoint Admin Center-Settings	CIS v3.0	E3 Level 2	Block OneDrive for Business sync from unmanaged devices	**High**	Status: WARNING: Not Blocked
Microsoft SharePoint Admin Center-Settings	CIS v3.0	E3 Level 1	Ensure custom script execution is restricted on personal sites	**High**	Total Sites allowing custom script execution: 22
Microsoft SharePoint	SP v1.0		Ensure SharePoint sites are not enabled for both External and User Sharing	**High**	Status: Enabled

Admin Center-Settings					
Microsoft SharePoint Admin Center-Settings	SP v1.0		External user sharing-share by email-and guest link sharing are both disabled	**Passed**	Status: Disabled
Microsoft SharePoint Admin Center-Settings	SP v1.0		Ensure that external users cannot share files folders and sites they do not own	**High**	Status: Not Enabled
Microsoft SharePoint Admin Center-Settings	SP v1.0		SharePoint External Sharing is not Enabled at Global Level	Error	Status: Enabled : Sharing capability is .
Microsoft SharePoint Admin Center-Settings	SP v1.0		SharePoint External User Resharing is not Permitted	Error	Status: Not Permitted
Microsoft SharePoint Admin Center-Settings	SP v1.0		SharePoint Legacy Authentication is not Enabled	Error	Status: Disabled
Microsoft SharePoint Admin Center-Settings	SP v1.0		SharePoint Anyone Shared Links Never Expire is not configured	Error	Status: Expires
Microsoft SharePoint Admin Center-Settings	SP v1.0		SharePoint Online Modern Authentication is Enabled	Error	Status: Enabled
Microsoft SharePoint Admin Center-Settings	SP v1.0		Ensure Sign out inactive users in SharePoint Online is Configured	**High**	Sign-out Inactive Users Status: The setting is not **compliant**.
Microsoft Teams Admin Center-Teams	CIS v3.0	E3 Level 2	Ensure external file sharing in Teams is enabled for only approved cloud storage services	**High**	Status: Not Controlled
Microsoft Teams Admin Center-Teams	SP v1.0		Ensure End-to-end encryption for Microsoft Teams is enabled	**High**	Status: Disabled

Microsoft Teams Admin Center-Teams	SP v1.0		Ensure external domains are not allowed in Teams	**High**	Status: Allowed All Domains
Microsoft Teams Admin Center-Policies	SP v1.0		Ensure Microsoft Teams External Domain Communication Policies are configured	**Medium**	Domains Allowed Status: All Domains Allowed
Microsoft Teams Admin Center-Policies	SP v1.0		Ensure Microsoft Teams Users Allowed to Invite Anonymous Users is disabled	**High**	Status: Enabled
Microsoft Teams Admin Center-Policies	SP v1.0		Ensure Microsoft Teams Policies Allow Anonymous Members is disabled	**High**	Status: Enabled
Microsoft Teams Admin Center-Policies	SP v1.0		Ensure Microsoft Teams Consumer Communication Policies are configured	**High**	Status: Not Configured
Microsoft Teams Admin Center-Policies	SP v1.0		Ensure Microsoft Teams External Access Policies are configured	**Low**	Status: Configured
Microsoft Teams Admin Center-Policies	SP v1.0		Ensure Microsoft Teams Users Allowed to Preview Links in Messages is disabled	**High**	AllowUrlPreviews Configured in Total Teams Policies: 4
Microsoft Teams Admin Center-Policies	SP v1.0		Ensure Safe Links for Teams is Enabled	**High**	Status: Not Configured - No ATP License
Microsoft Teams Admin Center-Teams Apps	CIS v3.0	E3 Level 1	Ensure app permission policies are configured	**High**	Status: Either some or all settings are Not **compliant**
Microsoft Fabric-Tenant Settings	CIS v3.0	E3 Level 1	Ensure guest user access is restricted	**High**	Status: Not Restricted: 10dae51f-b6af-4016-8d66-8c2a99b929b3
Microsoft Fabric-Tenant Settings	CIS v3.0	E3 Level 1	Ensure external user invitations are restricted	**High**	Status: Not Restricted: everyone
Microsoft Fabric-Tenant Settings	CIS v3.0	E3 Level 1	Ensure Allow users to apply sensitivity labels for content is Enabled	**Passed**	Status: Allow users to apply sensitivity labels for content is enabled

Microsoft M365 Users-Users	SP v1.0	Ensure All Microsoft 365 Users are licensed	**Medium**	Users Not Licensed: 8311
Microsoft M365 Users-Users	SP v1.0	Ensure Deleted Microsoft 365 Users are Identified	**Passed**	Deleted Users: 0
Microsoft M365 Users-Users	SP v1.0	Ensure Disabled Microsoft 365 Users are Identified	**Passed**	Disabled Users: 4
Microsoft M365 Users-Users	SP v1.0	Ensure Microsoft 365 Users have no Reconciliation Errors	**Passed**	Users Reconciliation Errors: 0
Microsoft M365 Users-Users	SP v1.0	Ensure Microsoft 365 Users Password Expires	**Passed**	Password Never Expires Set: 0
Microsoft M365 Users-Users	SP v1.0	Ensure Microsoft 365 Users are Syncing and No Sync Errors	**Passed**	Users in Sync Errors: 0
Microsoft M365 Users-Users	SP v1.0	Ensure no Provisioning Errors for Microsoft 365 Users	**Passed**	Users Not Provisioned: 0
Microsoft M365 Users-Users	SP v1.0	Ensure Microsoft 365 Blocked Users are Identified	**Passed**	Microsoft 365 Users Blocked: 0
Microsoft M365 Users-Users	SP v1.0	Ensure Microsoft 365 Users Have Changed Passwords	**High**	Passwords unchanged since 90 days: 8330
Microsoft M365 Users-Users	SP v1.0	Ensure Microsoft 365 Company Administrators have less than 5 Admins	**Passed**	More Than 10 Company Administrators Status: 4
Microsoft M365 Users-Users	SP v1.0	Ensure Microsoft 365 Deleted and Licensed Users are Identified	**Passed**	Deleted Users Licensed: 0
Microsoft M365 Users-Users	SP v1.0	Ensure Microsoft 365 Groups Without Members are Identified	**Low**	Groups Without Members: 6
Microsoft Mobile Device	SP v1.0	Ensure mobile device management policies are set to require advanced	**High**	Status: MDM/InTune is not configured as not applicable

Management-MDM Policies		security configurations for Android Devices		
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure mobile device management policies are set to require advanced security configurations for iOS Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that mobile device password reuse is prohibited for Android Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that mobile device password reuse is prohibited for iOS Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that mobile devices are set to never expire passwords for Android Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that mobile devices are set to never expire passwords for iOS Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that users cannot connect from devices that are jail broken or rooted	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise for Android Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise for iOS Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that mobile devices require a minimum password length to prevent brute force attacks for Android Devices	**High**	Status: MDM/InTune is not configured as not applicable

Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that mobile devices require a minimum password length to prevent brute force attacks for iOS Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure devices lock after a period of inactivity to prevent unauthorized access for Android Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure devices lock after a period of inactivity to prevent unauthorized access for iOS Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data for Android Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data for iOS Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that mobile devices require complex passwords (Type = Alphanumeric) for Android Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that mobile devices require complex passwords (Type = Alphanumeric) for iOS Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that mobile devices require complex passwords (Simple Passwords = Blocked) for iOS Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure that devices connecting have AV and a local firewall enabled	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure mobile device management policies are required for email profiles	**High**	Status: MDM/InTune is not configured as not applicable

Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure mobile devices require the use of a password for Android Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft Mobile Device Management-MDM Policies	SP v1.0	Ensure mobile devices require the use of a password for iOS Devices	**High**	Status: MDM/InTune is not configured as not applicable
Microsoft M365 Dangerous Defaults	SP v1.0	Ensure Users can read all attributes in Azure AD is disabled	**Medium**	Permission Status: Enabled-Not Ok
Microsoft M365 Dangerous Defaults	SP v1.0	Ensure Users can create security groups is disabled	**High**	Status: Enabled-Not Ok
Microsoft M365 Dangerous Defaults	SP v1.0	Ensure Users are allowed to create and register applications is disabled	**High**	Permission Status: Enabled-Not Ok
Microsoft M365 Dangerous Defaults	SP v1.0	Ensure Users with a verified mail domain can join the tenant is disabled	**High**	Permission Status: Enabled-Not Ok
Microsoft M365 Dangerous Defaults	SP v1.0	Ensure Guests can invite other guests into the tenant is disabled	**High**	Permission Status: Enabled-Not Ok
Microsoft M365 Dangerous Defaults	SP v1.0	Ensure Users are allowed to create new Azure Active Directory Tenants is disabled	**High**	Permission Status: Enabled-Not Ok
Microsoft M365 Dangerous Defaults	SP v1.0	Ensure Policy exists to restrict non-administrator access to Azure Active Directory or Entra	**High**	Permission Status: No Policy Found
Microsoft M365 Configuration	SP v1.0	Ensure Microsoft 365 Licenses are consumed in SKUs	**High**	SKUs Not In Use: 2

Microsoft M365 Configuration	SP v1.0	Ensure All Microsoft 365 Domains Have been verified	**Passed**	Domains Verification Pending: 0
Microsoft M365 Configuration	SP v1.0	Ensure Microsoft 365 Domain Services Have Services Assigned	**Passed**	Domains Without Services: 0
Microsoft M365 Configuration	SP v1.0	Ensure Microsoft 365 Notification Email is configured	**Passed**	Notifications Email: Nirmal@DynamicPacks.net
Microsoft M365 Configuration	SP v1.0	Ensure Microsoft 365 Organization Level Mailbox Auditing is configured	**Passed**	Status: Enabled
Microsoft M365 Configuration	SP v1.0	Ensure Microsoft 365 Dir Sync Feature is Configured	**Medium**	Status: Disabled
Microsoft M365 Configuration	SP v1.0	Ensure Microsoft 365 Dir Sync Features Are Used	**Low**	Status: Not Enabled
Microsoft M365 Configuration	SP v1.0	Ensure No Microsoft 365 Dir Sync Property Conflicts	**Passed**	Total Objects In Property Conflict: 0
Microsoft M365 Configuration	SP v1.0	Ensure No Microsoft 365 Dir Sync Property Conflict with User Principal Name	**Passed**	Objects In UPN Conflicts: 0
Microsoft M365 Configuration	**SP v1.0**	**Ensure No Microsoft 365 Dir Sync Property Conflict with ProxyAddress**	**Passed**	**Objects in ProxyAddress Conflicts: 0**

8. Technical Findings by SmartProfiler

After carrying out a complete health assessment of the ***Microsoft Microsoft 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.

8.1 M365 Admin Center

Test	Status	Remark
Ensure Administrative accounts are separate and cloud-only	**Passed**	**IMPACT:** All Administrative Accounts are Cloud-Only. **ACTION:**

		Test Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/add-users?view=o365-worldwide:https://learn.microsoft.com/en-us/microsoft-365/enterprise/protect-your-global-administrator-accounts?view=o365-worldwide:https://learn.microsoft.com/en-us/azure/active-directory/roles/best-practices#9-use-cloud-native-accounts-for-azure-ad-roles:https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/whatis Default Value: N/A
Ensure two emergency access accounts have been defined	**NotExecuted**	**IMPACT:** Item does not meet all the requirements as per test. Emergency access or accounts are limited for emergency scenarios where normal administrative accounts are unavailable. They are not assigned to a specific user and will have a combination of physical and technical controls to prevent them from being accessed outside a true emergency. These emergencies could be due to several things, including: - Technical failures of a cellular provider or Microsoft related service such as MFA. - The last remaining Global Administrator account is inaccessible. Ensure two Emergency Access accounts have been defined. NOTE: Microsoft provides a number of recommendations for these accounts and how to configure them. For more information on this, please refer to the references section. The CIS Benchmark outlines the more critical things to consider. In various situations, an organization may require the use of a break glass account to gain emergency access. In the event of losing access to administrative functions, an organization may experience a significant loss in its ability to provide support, lose insight into its security posture, and potentially suffer financial losses. If care is not taken in properly implementing an emergency access account this could weaken security posture. Microsoft recommends excluding at least one of these accounts from all conditional access rules therefore passwords must have sufficient entropy and length to protect against random guesses. FIDO2 security keys may be used instead of a password for secure passwordless solution. **ACTION:** Step 1 - Create two emergency access accounts: 1. Navigate to Microsoft 365 admin center https://admin.microsoft.com 2. Expand Users > Active Users 3. Click Add user and create a new user with these criteria: - Name the account in a way that does NOT identify it with a particular person. - Assign the account to the default .onmicrosoft.com domain and not the organizations. - The password must be at least 16 characters and generated randomly. - Do not assign a license. - Assign the user the Global Administrator role. 4. Repeat the above steps for the second account. Step 2 - Exclude at least one account from conditional access policies: 1. Navigate Microsoft Entra admin center https://entra.microsoft.com/ 2. Expand Azure Active Directory > Protect & Secure > Conditional Access 3. Inspect the conditional access policies. 4. For each rule add an exclusion for at least one of the emergency access accounts. 5. Users > Exclude > Users and groups and select one emergency access account.

		Step 3 - Ensure the necessary procedures and policies are in place: - In order for accounts to be effectively used in a break glass situation the proper policies and procedures must be authorized and distributed by senior management. - FIDO2 Security Keys, if used, should be locked in a secure separate fireproof location. - Passwords should be at least 16 characters, randomly generated and MAY be separated in multiple pieces to be joined on emergency. NOTE: Microsoft documentation contains in-depth information on securing break glass accounts, please refer to the references section. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/roles/security-planning#stage-1-critical-items-to-do-right-now:https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access Default Value: Not defined.
Ensure that between two and four global admins are designated	**Passed**	**IMPACT:** Found more than two Global Administrators. **ACTION:** Test Reference: https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.directorymanagement/get-mgdirectoryrole?view=graph-powershell-1.0:https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#role-template-ids Default Value: No Default Value Found
Ensure Guest Users are reviewed at least biweekly	**Medium**	**IMPACT:** Found Guest accounts found. Auditing Process needs to be created and followed. There is no impact if the 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. Test Reference: No Link Found Default Value: No Default Value Found
Ensure Azure Information Protection-AIP is enabled at Global Level	**High**	**IMPACT:** Azure Information Protection is not enabled at global level. No Impact as AIP will be retired in April 2024. **ACTION:** No Impact as AIP will be retired in April 2024. Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 User Roles have less than 10 Admins	**Passed**	**IMPACT:** All Microsoft 365 Roles have 10 or less members. **ACTION:**

		Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Users Have Strong Password Requirements Configured	**Passed**	**IMPACT:** All Microsoft 365 users are enabled with Strong Password Requirements. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure self-service password reset is enabled	**Passed**	**IMPACT:** Self Service Password Reset is enabled for Tenant. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure that Microsoft 365 Passwords Are Not Set to Expire	**Passed**	**IMPACT:** Microsoft 365 Password Policies are configured for domains. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure modern authentication for Teams Online is enabled	**High**	**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. Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Exchange Online Modern Authentication is Used	**Passed**	**IMPACT:** Microsoft 365 Modern Authentication is enabled. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Exchange Online Privileged Access Management is Used	**High**	**IMPACT:** Microsoft 365 Privileged Access Management is NOT enabled. Refer issue details. **ACTION:** It is recommended to enable PAM in Microsoft 365. Test Reference: No Link Found Default Value: No Default Value Found

Ensure Enterprise Applications Role Assignments are reviewed weekly	**High**	**IMPACT:** Found role assignments were not found for enterprise applications. Applications have an attack surface for security breaches and must be monitored. While not targeted as often as user accounts, breaches can occur. Because applications often run without human intervention, the attacks may be harder to detect. **ACTION:** It is recommended that the Security administrator reviews the list of role assignments to each Enterprise Application and removes them if they are not needed. Test Reference: No Link Found Default Value: No Default Value Found
Ensure that only organizationally managed-approved public groups exist	**Medium**	**IMPACT:** Public Groups found in Microsoft 365 Tenant. If the recommendation is applied, group owners could receive more access requests than usual, especially regarding groups originally meant to be public. **ACTION:** Ensure that only organizationally managed and approved public groups exist. When a group has public privacy. users may access data related to this group. Administrators are notified when a user uses the Azure Portal. Requesting access to the group forces users to send a message to the group owner. But they still have immediate access to the group. Public in this case means public to the identities within the organization. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-self-service-management:https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide Default Value: Public when create from the Administration portal, private otherwise.
Ensure sign-in to shared mailboxes is blocked	**Medium**	IMPACT: Item does not meet all the requirements as per test. Shared mailboxes are used when multiple people need access to the same mailbox, such as a company information or support email address, reception desk, or other function that might be shared by multiple people. Users with permissions to the group mailbox can send as or send on behalf of the mailbox email address if the administrator has given that user permissions to do that. This is particularly useful for help and support mailboxes because users can send emails from or Shared mailboxes are created with a corresponding user account using a system generated password that is unknown at the time of creation. The recommended state is Sign in blocked for Shared mailboxes. The intent of the shared mailbox is the only allow delegated access from other mailboxes. An admin could reset the password, or an attacker could potentially gain access to the shared mailbox allowing the direct sign-in to the shared mailbox and subsequently the sending of email from a sender that does not have a unique identity. To prevent this, block sign-in for the account that is associated with the shared mailbox. ACTION: Block sign-in to shared mailboxes in the UI: 1. Navigate to Microsoft 365 admin center https://admin.microsoft.com/ 2. Click to expand Teams & groups and select Shared mailboxes. 3. Take note of all shared mailboxes. 4. Click to expand Users and select Active users.

		5. Select a shared mailbox account to open its properties pane and then select Block sign-in. 6. Check the box for Block this user from signing in. 7. Repeat for any additional shared mailboxes. Using PowerShell connect with 2 modules: 1. Connect using Connect-AzureAD. 2. To disable sign-in for a single account: Set-AzureADUser -ObjectId TestUser@example.com -AccountEnabled $false 3. Or, the following script will block sign-in to all Shared Mailboxes. 4. Connect using Connect-ExchangeOnline. $MBX = Get-EXOMailbox -RecipientTypeDetails SharedMailbox $MBX | ForEach {Set-AzureADUser -ObjectId $_.ExternalDirectoryObjectId -AccountEnabled $false} Test Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/email/about-shared-mailboxes?view=o365-worldwide:https://learn.microsoft.com/en-us/microsoft-365/admin/email/create-a-shared-mailbox?view=o365-worldwide#block-sign-in-for-the-shared-mailbox-account:https://learn.microsoft.com/en-us/microsoft-365/enterprise/block-user-accounts-with-microsoft-365-powershell?view=o365-worldwide#block-individual-user-accounts:https://learn.microsoft.com/en-us/powershell/module/azuread/set-azureaduser?view=azureadps-2.0 Default Value: AccountEnabled: True
Ensure the Password expiration policy is set to Set passwords to never expire (recommended)	**Passed**	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: https://pages.nist.gov/800-63-3/sp800-63b.html:https://www.cisecurity.org/white-papers/cis-password-policy-guide/:https://learn.microsoft.com/en-US/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide Default Value: If the property is not set, a default value of 90 days will be used
Ensure Idle session timeout is set to 3 hours (or less) for unmanaged devices	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. Idle session timeout allows the configuration of a setting which will timeout inactive users after a pre-determined amount of time. When a user reaches the set idle timeout session, they will get a notification that they are about to be signed out. They have to select to stay signed in or they will be automatically signed out of all Microsoft 365 web apps. Combined with a Conditional Access rule this will only impact unmanaged devices. A managed device is considered a device managed by Intune MDM. The following Microsoft 365 web apps are supported. - Outlook Web App - OneDrive for Business - SharePoint Online (SPO) - Office.com and other start pages - Office (Word, Excel, PowerPoint) on the web

		- Microsoft 365 Admin Center NOTE: Idle session timeout doesn't affect Microsoft 365 desktop and mobile apps. The recommended setting is 3 hours (or less) for unmanaged devices. Ending idle sessions through an automatic process can help protect sensitive company data and will add another layer of security for end users who work on unmanaged devices that can potentially be accessed by the public. Unauthorized individuals onsite or remotely can take advantage of systems left unattended over time. Automatic timing out of sessions makes this more difficult. If step 2 in the Audit/Remediation procedure is left out then there is no issue with this from a security standpoint. However, it will require users on trusted devices to sign in more frequently which could result in credential prompt fatigue. ACTION: To configure Idle session timeout: 1. Navigate to the Microsoft 365 admin center https://admin.microsoft.com/. 2. Click to expand Settings Select Org settings. 3. Click Security & Privacy tab. 4. Select Idle session timeout. 5. Check the box Turn on to set the period of inactivity for users to be signed off of Microsoft 365 web apps 6. Set a maximum value of 3 hours. 7. Click save. Step 2 - Ensure the Conditional Access policy is in place: 1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/ 2. Expand Azure Active Directory > Protect & secure > Conditional Access 3. Click New policy and give the policy a name. 4. Select Users > All users. 5. Select Cloud apps or actions > Select apps and select Office 365 6. Select Conditions > Client apps > Yes check only Browser unchecking all other boxes. 7. Select Sessions and check Use app enforced restrictions. 8. Set Enable policy to On and click Create. NOTE: To ensure that idle timeouts affect only unmanaged devices, both steps must be completed. Test Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/manage/idle-session-timeout-web-apps?view=o365-worldwide Default Value: Not configured. (Idle sessions will not timeout.)
Ensure calendar details sharing with external users is disabled	**High**	IMPACT: Calendar 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 have 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.

		Test Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/manage/share-calendars-with-external-users?view=o365-worldwide Default Value: Enabled (True)
Ensure User owned apps and services is restricted	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. 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. 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 users ability to install add-ins in Microsoft Word, Excel, or PowerPoint helps reduce your threat-surface and mitigate this risk. 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: To prohibit users installing Office Store add-ins and starting 365 trials: 1. Navigate to Microsoft 365 admin center https://admin.microsoft.com. 2. Click to expand Settings Select Org settings. 3. Under Services select User owned apps and services. 4. Uncheck Let users access the Office Store and Let users start trials on behalf of your organization. 5. Click Save. Test Reference: No Link Found Default Value: Let users access the Office Store is Checked Let users start trials on behalf of your organization is Checked
Ensure internal phishing protection for Forms is enabled	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. 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. 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: To enable internal phishing protection for Forms: 1. Navigate to Microsoft 365 admin center https://admin.microsoft.com. 2. Click to expand Settings then select Org settings. 3. Under Services select Microsoft Forms. 4. Click the checkbox labeled Add internal phishing protection under Phishing protection. 5. Click Save.

		Test Reference: https://learn.microsoft.com/en-US/microsoft-forms/administrator-settings-microsoft-forms:https://learn.microsoft.com/en-US/microsoft-forms/review-unblock-forms-users-detected-blocked-potential-phishing Default Value: Internal Phishing Protection is enabled.
Ensure the customer lockbox feature is enabled	**Medium**	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 Test Reference: https://learn.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview Default Value: Require approval for all data access requests - Unchecked CustomerLockboxEnabled - False
Ensure third-party storage services are restricted in Microsoft 365 on the web	**High**	IMPACT: Item does not meet all the requirements as per test. Third-party storage can be enabled for users in Microsoft 365, allowing them to store and share documents using services such as Dropbox, alongside OneDrive and team sites. Ensure Microsoft 365 on the web third-party storage services are restricted. By using external storage services an organization may increase the risk of data breaches and unauthorized access to confidential information. Additionally, third-party services may not adhere to the same security standards as the organization, making it difficult to maintain data privacy and security. The 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: To restrict Microsoft 365 on the web: 1. Navigate to Microsoft 365 admin center https://admin.microsoft.com 2. Go to Settings > Org Settings > Services > Microsoft 365 on the web 3. Uncheck Let users open files stored in third-party storage services in Microsoft 365 on the web Test Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/setup/set-up-file-storage-and-sharing?view=o365-worldwide#enable-or-disable-third-party-storage-services Default Value: Enabled - Users are able to open files stored in third-party storage services
Ensure that Sways cannot be shared with people outside of your organization	**NotExecuted**	**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 leaks. Test Reference: https://support.microsoft.com/en-us/office/administrator-settings-for-sway-d298e79b-b6ab-44c6-9239-aa312f5784d4 **Default Value: Let people in your organization share their sways with people outside your organization - Enabled**

8.2 Microsoft 365 Defender-Email and Collaboration

Test	Status	Remark
Ensure Safe Links for Office Applications is Enabled	**High**	**IMPACT:** Safe Links for Office Applications are 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. Test Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure?view=o365-worldwide:https://learn.microsoft.com/en-us/powershell/module/exchange/set-safelinkspolicy?view=exchange-ps:https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/preset-security-policies?view=o365-worldwide Default Value: No Default Value Found
Ensure the Common Attachment Types Filter is enabled	**High**	**IMPACT:** Common Attachment Filter is not enabled. Blocking common malicious file types should not have 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. Test Reference: https://learn.microsoft.com/en-us/powershell/module/exchange/get-malwarefilterpolicy?view=exchange-ps:https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-policies-configure?view=o365-worldwide Default Value: Always on
Ensure notifications for internal users sending malware is Enabled	**High**	**IMPACT:** Notifications for Internal Users Sending Malware is not enabled. Notification of account with potential issues should not cause an impact to the user. **ACTION:** Exchange Online Protection (EOP) is the cloud-based filtering service that protects your organization against spam, malware, and other email threats. EOP is

		included in all Microsoft 365 organizations with Exchange Online mailboxes. EOP uses flexible anti-malware policies for malware protection settings. These policies Test Reference: No Link Found Default Value: EnableInternalSenderAdminNotifications : False InternalSenderAdminAddress : $null
Ensure Safe Attachments policy is enabled	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:** Test Reference: No Link Found Default Value: disabled
Ensure Safe Attachments for SharePoint-OneDrive-Microsoft Teams is Enabled	**Medium**	**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. Test Reference: No Link Found Default Value: No Default Value Found
Ensure Exchange Online Spam Policies are set correctly	**High**	**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. Test Reference: No Link Found Default Value: BccSuspiciousOutboundAdditionalRecipients : {} BccSuspiciousOutboundMail : False NotifyOutboundSpamRecipients : {} NotifyOutboundSpam : False
Ensure that an anti-phishing policy has been created	**Passed**	**IMPACT:** Anti-Phishing Policy has been created. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure that SPF records are published for all Exchange Domains	**Medium**	**IMPACT:** SPF Records are not published for all domains. There should be minimal impact of setting up SPF records. However, organizations should ensure proper SPF record setup as email could be flagged as spam if SPF is not setup appropriately.

		ACTION: For each domain that is configured in Exchange, a corresponding Sender Policy Framework (SPF) record should be created. SPF records allow Exchange Online Protection and other mail systems know where messages from your domains are allowed to originate. This information can be used to by that system to determine how to treat the message based on if it is being spoofed or is valid. Test Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-spf-configure?view=o365-worldwide Default Value: No Default Value Found
Ensure No Domains with SPF Soft Fail are Configured	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:** Test Reference: https //serverfault.com/questions/355511/is-using-softfail-over-fail-in-the-spf-record-considered-best-practice Default Value: No Default Value Found
Ensure that DKIM is enabled for all Exchange Online Domains	**High**	**IMPACT:** DKIM is not enabled for all exchange domains. There should be no impact of setting up DKIM however organizations should ensure appropriate setup to ensure continuous mail-flow. **ACTION:** You should use DKIM in addition to SPF and DMARC to help prevent spoofers from sending messages that look like they are coming from your domain. By enabling DKIM with Microsoft 365, messages that are sent from Exchange Online will be cryptographically signed. This will allow the receiving email system to validate that the messages were generated by a server that the organization authorized and not being spoofed. Test Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-dkim-configure?view=o365-worldwide Default Value: No Default Value Found
Ensure DMARC Records for all Exchange Online domains are published	**High**	**IMPACT:** DMARC Records for all Exchange Domains are not published. There should be no impact of setting up DMARC however organizations should ensure appropriate setup to ensure continuous mail-flow. **ACTION:** Publish Domain-Based Message Authentication, Reporting and Conformance (DMARC) records for each Exchange Online Accepted Domain. Domain-based Message Authentication, Reporting and Conformance (DMARC) work with Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to authenticate mail senders and ensure that destination email systems trust messages sent from your domain. Test Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-dmarc-configure?view=o365-worldwide Default Value: No Default Value Found
Ensure the spoofed domains report is review weekly	**Medium**	**IMPACT:** Found Spoofed domains. Please review the list and act 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 Microsoft 365 Enterprise E5 or separately as part of Defender for Microsoft 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. Test Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-spoof-intelligence?view=o365-worldwide:https://learn.microsoft.com/en-us/powershell/module/exchange/get-spoofintelligenceinsight?view=exchange-ps Default Value: No Default Value Found
Ensure the Restricted entities report is reviewed weekly	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:** Test Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/responding-to-a-compromised-email-account?view=o365-worldwide:https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam?view=o365-worldwide:https://learn.microsoft.com/en-us/powershell/module/exchange/get-blockedsenderaddress?view=exchange-ps Default Value: No Default Value Found
Ensure all security threats in the Threat protection status report are reviewed at least weekly	**High**	**IMPACT:** All Security Threats are not reviewed by Microsoft 365 Engineer weekly. **You should review all the security threats in the Threat protection status report at least weekly. This report shows specific instances of Microsoft blocking a malware attachment from reaching your users, phishing being blocked, impersonation attempts, etc.** **ACTION:** While this report isn't strictly actionable, reviewing it will give you a sense of the overall volume of various security threats targeting your users, which may prompt you to adopt more aggressive threat mitigations. **Test Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email-security?view=o365-worldwide** **Default Value: No Default Value Found**

8.3 Microsoft Purview

Test	Status	Remark
Ensure Microsoft 365 audit log search is Enabled	**Passed**	**IMPACT:** Microsoft 365 Audit Log Search is enabled. **ACTION:** Test Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-log-enable-disable?view=o365-worldwide:https://learn.microsoft.com/en-us/powershell/module/exchange/set-adminauditlogconfig?view=exchange-ps Default Value: No Default Value Found
Ensure user role group changes are reviewed at least weekly	**Passed**	**IMPACT:** Auditing Process is created and followed. **ACTION:**

		Test Reference: https://learn.microsoft.com/en-us/powershell/module/exchange/search-unifiedauditlog?view=exchange-ps Default Value: No Default Value Found
Ensure DLP policies are enabled	**High**	**IMPACT:** DLP Policies are not enabled. Enabling a Teams DLP policy will allow sensitive data in Exchange Online and SharePoint Online to be detected or blocked. Always ensure to follow appropriate procedures in regard to testing and implementation of DLP policies based on your organizational standards. **ACTION:** Enabling Data Loss Prevention (DLP) policies allow Exchange Online and SharePoint Online content to be scanned for specific types of data like social security numbers, credit card numbers, or passwords. Test Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide Default Value: No Default Value Found
Ensure DLP policies are enabled for Microsoft Teams	**High**	**IMPACT:** DLP Policies are not enabled for Microsoft Teams. Enabling a Teams DLP policy will allow sensitive data in Teams channels or chat messages to be detected or blocked. **ACTION:** Enabling Data Loss Prevention (DLP) policies for Microsoft Teams, blocks sensitive content when shared in teams or channels. Content to be scanned for specific types of data like social security numbers, credit card numbers, or passwords. Enabling DLP policies alerts users and administrators that specific types of data should not be exposed, helping to protect the data from accidental exposure. Test Reference: https://learn.microsoft.com/en-us/powershell/exchange/connect-to-scc-powershell?view=exchange-ps:https://learn.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2?view=exchange-ps#turn-on-basic-authentication-in-winrm:https://learn.microsoft.com/en-us/powershell/module/exchange/connect-ippssession?view=exchange-ps Default Value: Enabled (On)
Ensure DLP Policy is enabled for OneDrive	**High**	**IMPACT:** DLP for OneDrive is not enabled. Data Loss Prevention (DLP) capabilities protect your data where it is stored, when it is moved, and when it is shared. **ACTION:** It is recommended to enable DLP for OneDrive. Test Reference: No Link Found Default Value: No Default Value Found
Ensure DLP Policy is configured for SharePoint	**High**	**IMPACT:** DLP Policy for SharePoint is not enabled. As businesses continue to digitize their operations, data protection has become a top priority. Microsoft SharePoint Online, a cloud-based collaboration and document management solution, offers a built-in Data Loss Prevention (DLP) solution to help safeguard sensitive information. DLP in SharePoint Online is important because it helps organizations protect their sensitive information from being shared with unauthorized parties. This is especially critical in industries that are highly regulated, such as healthcare and finance. **ACTION:** It is recommended to enable DLP Policy for SharePoint.

		Test Reference: No Link Found Default Value: No Default Value Found
Ensure Custom Anti-Malware Policy is Present	**High**	**IMPACT:** Item does not meet all the requirements as per test. It is possible to create custom anti-malware policies in Exchange Online to provide additional protection against threats that may be received via email. No anti-malware policy besides the Microsoft Default Anti-Malware Policy was detected in the O365 Tenant. Although the default anti-malware policy can provide some protection, each organization should consider creating an anti-malware policy that is customized to suit the nature of their day-to-day activities. **ACTION:** Follow the 'Configure anti-malware policies in Exchange Online Protection' guide below for a full introduction to creating a custom anti-malware policy. It is possible to create an anti-malware policy and enable it through the Exchange administration center or via Exchange Online PowerShell using the Set-MalwareFilterPolicy or New-MalwareFilterPolicy commands. Test Reference: No Link Found Default Value: No Default Value Found
Ensure Custom Anti-Phishing Policy is Present	**High**	**IMPACT:** Item does not meet all the requirements as per test. It is possible to create custom Anti-Phishing Policies in Exchange Online to provide additional protection against threats that may be received via email. No Anti-Phishing Policy besides the Microsoft Default Anti-Phishing Policy was detected in the O365 tenant. Although the default Anti-Phishing Policy can provide some protection, each organization should consider creating an Anti-Phishing Policy that is customized to suit the nature of their day-to-day activities. **ACTION:** Follow the 'Anti-Phishing Policies in Microsoft 365' article below to begin constructing a custom Anti-Phishing Policy. Test Reference: No Link Found Default Value: No Default Value Found
Ensure Custom DLP Policies are Present	**High**	**IMPACT:** Item does not meet all the requirements as per test. Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who should not have it. Default configurations may not meet the business needs, or compliance requirements of the organization. Custom policies can be configured to address any gaps that default settings do not remediate. **ACTION:** Determine if a custom DLP policy is beneficial for the Tenant, identify any gaps between desired end state and default policy configurations, and implement any new policies as needed. Test Reference: https //docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide Default Value: No Default Value Found
Ensure Custom DLP Sensitive Information Types are Defined	**High**	**IMPACT:** Item does not meet all the requirements as per test. Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. Default configurations may not meet the business needs, or compliance requirements of the

		organization. Custom-defined information types may be configured to mitigate any gaps that default settings do not address. **ACTION:** Determine if there is a need for custom DLP Sensitive Information types and add as needed. Test Reference: https //docs.microsoft.com/en-us/microsoft-365/compliance/create-a-custom-sensitive-information-type-in-scc-powershell?view=o365-worldwide Default Value: No Default Value Found
Ensure SharePoint Online Information Protection policies are set up and used	**High**	**IMPACT:** SharePoint Online Information Protection Policies are not set up and used. **The creation of data classification policies is unlikely to have a significant not impact on an organization. However, maintaining long-term adherence to policies may require ongoing training and compliance efforts across the organization. Therefore, organizations should include training and compliance planning as part of the data classification policy creation process.** **ACTION:** To set up SharePoint Online Information Protection: 1. Navigate to Microsoft Purview compliance portal https://compliance.microsoft.com. 2. Under Solutions select Information protection. 3. Click on the Label policies tab. **4. Click Create a label to crea**te a label. 5. Select the label and click on the Publish label. 6. Fill out the forms to create the policy. **Test Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-overview?view=o365-worldwide#top-sensitivity-labels**-applied-to-content **Default Value: No Default Value Found**

8.4 Microsoft Entra admin center

Test	Status	Remark
Ensure Security Defaults is disabled on Azure Active Directory	**Passed**	**IMPACT:** Security Defaults is disabled in Azure AD. **ACTION:** Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults:https://techcommunity.microsoft.com/t5/azure-active-directory-identity/introducing-security-defaults/ba-p/1061414 Default Value: Enabled.
Ensure Per-user MFA is disabled	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:** Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates#convert-users-from-per-user-mfa-to-conditional-access:https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide#use-conditional-access-policies:https://learn.microsoft.com/en-us/azure/active-

		directory/authentication/howto-mfa-userstates#convert-per-user-mfa-enabled-and-enforced-users-to-disabled Default Value: Disabled
Ensure third party integrated applications are not allowed	**High**	**IMPACT:** Third party integrated applications are not allowed and 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 Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added Default Value: Yes (Users can register applications.)
Ensure Restrict non-admin users from creating tenants is set to Yes	**High**	**IMPACT:** Item does not meet all the requirements as per test. Non-privileged users can create tenants in the Azure AD and Entra administration portal under Manage tenant. The creation of a tenant is recorded in the Audit log as category DirectoryManagement and activity Create Company. Anyone who creates a tenant becomes the Global Administrator of that tenant. The newly created tenant doesn't inherit any settings or configurations. Restricting tenant creation prevents unauthorized or uncontrolled deployment of resources and ensures that the organization retains control over its infrastructure. User generation of shadow IT could lead to multiple, disjointed environments that can make it difficult for IT to manage and secure the organizations data, especially if other users in the organization began using these tenants for business purposes under the misunderstanding that they were secured by the organizations security team. Non-admin users will need to contact I.T. if they have a valid reason to create a tenant. **ACTION:** Restrict access to the Azure AD portal: 1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/ 2. Click to expand Identity> Users > User settings. 3. Set Restrict non-admin users from creating tenants to Yes then Save. To remediate using PowerShell: 1. Connect to Microsoft Graph using Connect-MgGraph -Scopes 2. Run the following commands. # Create hashtable and update the auth policy $params = @{ AllowedToCreateTenants = $false } Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions $params Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions#restrict-member-users-default-permissions Default Value: No - Non-administrators can create tenants. AllowedToCreateTenants is True

Ensure Restrict access to the Azure AD administration portal is set to Yes	High	**IMPACT:** Item does not meet all the requirements as per test. Restrict non-privileged users from signing into the Azure Active Directory portal. Note: This recommendation only affects access to the Azure AD web portal. It does not prevent privileged users from using other methods such as Rest API or PowerShell to obtain information. Those channels are addressed elsewhere in this document. The Azure AD administrative (AAD) portal contains sensitive data and permission settings, which are still enforced based on the users role. However, an end user may inadvertently change properties or account settings that could result in increased administrative overhead. Additionally, a compromised end user account could be used by a malicious attacker as a means to gather additional information and escalate an attack. Note: Users will still be able to sign into Azure Active directory admin center but will be unable to see directory information. **ACTION:** Ensure access to the Azure AD portal is restricted: 1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/ 2. Click to expand Identity> Users > User settings. 3. Set Restrict access to Microsoft Entra ID administration portal to Yes then Save. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions#restrict-member-users-default-permissions Default Value: No - Non-administrators can access the Azure AD administration portal.
Ensure the option to remain signed in is hidden	Medium	**IMPACT:** Option to remain signed in is not hidden and needs to be configured. Please see impact. Allowing users to select this option presents risk, especially in the event that the user signs into their account on a publicly accessible computer/web browser. In this case it would be trivial for an unauthorized person to gain access to any associated cloud data from that account. Once this setting is hidden users will no longer be prompted upon sign-in with the message Stay signed in. This may mean users will be forced to sign in more frequently. **ACTION:** The option for the user to Stay signed in or the Keep me signed in option will prompt a user after a successful login, when the user selects this option a persistent refresh token is created. Typically, this lasts for 90 days and does not prompt for sign-in or Multi-Factor. Test Reference: No Link Found Default Value: Users may select stay signed in
Ensure LinkedIn account connections is disabled	High	**IMPACT:** Item does not meet all the requirements as per test. LinkedIn account connections allow users to connect their Microsoft work or school account with LinkedIn. After a user connects their accounts, information and highlights from LinkedIn are available in some Microsoft apps and services. Disabling LinkedIn integration prevents potential phishing attacks and risk scenarios where an external party could accidentally disclose sensitive information. Users will not be able to sync contacts or use LinkedIn integration. **ACTION:** To disable LinkedIn account connections:

		1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/. 2. Click to expand Identity > Users select User settings. 3. Under LinkedIn account connections select No. 4. Click Save. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/linkedin-integration:https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/linkedin-user-consent Default Value: LinkedIn integration is enabled by default.
Ensure a dynamic group for guest users is created	**High**	**IMPACT:** Item does not meet all the requirements as per test. A dynamic group is a dynamic configuration of security group membership for Azure Active Directory. Administrators can set rules to populate groups that are created in Azure AD based on user attributes (such as userType, department, or country/region). Members can be automatically added to or removed from a security group based on their attributes. The recommended state is to create a dynamic group that includes guest accounts. Dynamic groups allow for an automated method to assign group membership. Guest user accounts will be automatically added to this group and through this existing conditional access rules, access controls and other security measures will ensure that new guest accounts are restricted in the same manner as existing guest accounts. **ACTION:** Create a dynamic guest group: 1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/. 2. Click to expand Identity > Groups select All groups. 3. Select New group and assign the following values: - Group type: Security - Azure AD Roles can be assigned: No - Membership type: Dynamic User 4. Select Add dynamic query. 5. Above the Rule syntax text box, select Edit. 6. Place the following expression in the box: (user.userType -eq) 7. Select OK and Save Using PowerShell: 1. Connect to Microsoft Graph using Connect-MgGraph -Scopes 2. In the script below edit DisplayName and MailNickname as needed and run: $params = @{ DisplayName = MailNickname = MailEnabled = $false SecurityEnabled = $true GroupTypes =

		MembershipRule = (user.userType -eq) MembershipRuleProcessingState = } New-MgGroup @params Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-create-rule:https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership:https://learn.microsoft.com/en-us/azure/active-directory/external-identities/use-dynamic-groups Default Value: Undefined
Ensure the Application Usage report is reviewed at least weekly	**Medium**	**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. Test Reference: No Link Found Default Value: No Default Value Found
Ensure user consent to apps accessing company data on their behalf is not allowed	**Medium**	**IMPACT:** Consent to Apps accessing company data on their behalf is not allowed and 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. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent?tabs=azure-portal&pivots=portal Default Value: UI - Allow user consent for apps
Ensure the admin consent workflow is enabled	**High**	**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 Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow

		Default Value: - Users can request admin consent to apps they are unable to consent to: No - Selected users to review admin consent requests: None - Selected users will receive email notifications for requests: Yes - Selected users will receive request expiration reminders: Yes - Consent request expires after (days): 30
Ensure that collaboration invitations are sent to allowed domains only	**Medium**	**IMPACT:** Collaboration Invitations are not sent to allowed domains only. This could make harder collaboration if the setting is not quickly updated when a new domain is identified as allowed. **ACTION:** Users should be able to send collaboration invitations to allowed domains only. By specifying allowed domains for collaborations, external user companies are explicitly identified. Also, this prevents internal users from inviting unknown external users such as personal accounts and gives them access to resources. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/external-identities/allow-deny-list:https://learn.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b Default Value: Allow invitations to be sent to any domain (most inclusive)
Ensure that password hash sync is enabled for hybrid deployments	**Medium**	**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 Deployments. Password hash synchronization helps by reducing the number of passwords your users will need to remember. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs:https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#user-linked-detections:https://www.microsoft.com/en-us/download/details.aspx?id=47594 Default Value: - Azure AD Connect sync disabled by default - Password Hash Sync is Microsofts recommended setting for new deployments
Ensure multifactor authentication is enabled for all users in administrative roles	**High**	**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 Microsoft 365 Tenant. Test Reference: https://learn.microsoft.com/en-us/graph/api/resources/security-api-overview?view=graph-rest-beta Default Value: No Default Value Found

Ensure multifactor authentication is enabled for all users	**High**	IMPACT: Item does not meet all the requirements as per test. 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. Multifactor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multifactor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multifactor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk. 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. NOTE: Organizations that have difficulty enforcing MFA globally due lack of the budget to provide company owned mobile devices to every user, or equally are unable to force end users to use their personal devices due to regulations, unions, or policy have another option. FIDO2 Security keys may be used as a stand in for this recommendation. They are more secure, phishing resistant, and are affordable for an organization to issue to every end user. ACTION: To enable multifactor authentication for all users: 1. Navigate to the Microsoft Entra admin center https://entra.microsoft.com. 2. Click expand Protection > Conditional Access select Policies. 3. Click New policy. 4. Go to Assignments > Users and groups > Include > select All users (and do not exclude any user). 5. Select Cloud apps or actions > All cloud apps (and don't exclude any apps). 6. Access Controls > Grant > Require multi-factor authentication (and nothing else). 7. Leave all other conditions blank. 8. Make sure the policy is Enabled/On. 9. Create. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa:https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa:https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.reports/update-mgreportauthenticationmethoduserregistrationdetail?view=graph-powershell-1.0#-isadmin Default Value: Disabled
Enable Conditional Access policies to block legacy authentication	**High**	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 Microsoft 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.

		Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online:https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-microsoft-365-or-office-365:https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online Default Value: Basic authentication is disabled by default as of January 2023.
Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users	**High**	IMPACT: Item does not meet all the requirements as per test. In complex deployments, organizations might have a need to restrict authentication sessions. Conditional Access policies allow for the targeting of specific user accounts. Some scenarios might include: - Resource access from an unmanaged or shared device - Access to sensitive information from an external network - High-privileged users - Business-critical applications. Ensure Sign-in frequency does not exceed 4 hours for E3 tenants, or 24 hours for E5 tenants using Privileged Identity Management. Ensure Persistent browser session is set to Never persist. NOTE: This CA policy can be added to the previous CA policy in this benchmark Forcing a time out for MFA will help ensure that sessions are not kept alive for an indefinite period of time, ensuring that browser sessions are not persistent will help in prevention of drive-by attacks in web browsers, this also prevents creation and saving of session cookies leaving nothing for an attacker to take. Users with Administrative roles will be prompted at the frequency set for MFA. ACTION: To configure Sign-in frequency and browser sessions persistence for administrative users: 1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/. 2. Click to expand Protection > Conditional Access Select Policies. 3. Click New policy 4. Click Users and groups 5. Under Include select -Select users and groups- and then select -Directory roles-. 6. At a minimum, select the roles in the section below. 7. Go to Cloud apps or actions > Cloud apps > Include > select All cloud apps (and don't exclude any apps). 8. Under Access controls > Grant > select Grant access > check Require multi-factor authentication (and nothing else). 9. Under Session select Sign-in frequency and set to at most 4 hours for E3 tenants. E5 tenants with PIM can be set to a maximum value of 24 hours. 10. Check Persistent browser session then select Never persistent in the drop-down menu. 11. For Enable Policy select On and click Save At minimum these directory roles should be included for MFA: - Application administrator - Authentication administrator - Billing administrator - Cloud application administrator

		- Conditional Access administrator - Exchange administrator - Global administrator - Global reader - Helpdesk administrator - Password administrator - Privileged authentication administrator - Privileged role administrator - Security administrator - SharePoint administrator - User administrator Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime Default Value: The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days.
Ensure Phishing-resistant MFA strength is required for Administrators	**High**	IMPACT: Item does not meet all the requirements as per test. Authentication strength is a Conditional Access control that allows administrators to specify which combination of authentication methods can be used to access a resource. For example, they can make only phishing-resistant authentication methods available to access a sensitive resource. But to access a non-sensitive resource, they can allow less secure multifactor authentication (MFA) combinations, such as password + SMS. Microsoft has 3 built-in authentication strengths. MFA strength, password less MFA strength, and Phishing-resistant MFA strength. Ensure administrator roles are using a CA policy with Phishing-resistant MFA strength. Administrators can then enroll using one of 3 methods: - FIDO2 Security Key - Windows Hello for Business - Certificate-based authentication (Multi-Factor) NOTE: Additional steps to configure methods such as FIDO2 keys are not covered here but can be found in related MS articles in the references section. The Conditional Access policy only ensures 1 of the 3 methods is used. WARNING: Administrators should be pre-registered for a strong authentication mechanism before this Conditional Access Policy is enforced. Additionally, as stated elsewhere in the CIS Benchmark a break-glass administrator account should be excluded from this policy to ensure unfettered access in the case of an emergency. Sophisticated attacks targeting MFA are more prevalent as the use of it becomes more widespread. These 3 methods are considered phishing-resistant as they remove passwords from the login workflow. It also ensures that public/private key exchange can only happen between the devices and a registered provider which prevents login to fake or phishing websites. If administrators are not pre-registered for a strong authentication method prior to a conditional access policy is created, then a condition could occur where a user can not register for strong authentication because they don't meet the conditional access policy requirements and therefore are prevented from signing in. ACTION: To create a phishing-resistant MFA CA policy for users in administrative roles: 1. Navigate to the Microsoft Entra admin center https://entra.microsoft.com. 2. Click expand Protection > Conditional Access select Policies.

		3. Click New policy. 4. Go to Users > Users and groups > Include > Select users and groups > Directory roles 5. Add at least the Directory roles listed after these steps. 6. Select Cloud apps or actions > All cloud apps (and don't exclude any apps). 7. Grant > Grant Access with Require authentication strength (Preview): Phishing-resistant MFA 8. Click Select 9. Set Enable policy to Report-only and click Create At minimum these directory roles should be included for the policy: - Application administrator - Authentication administrator - Billing administrator - Cloud application administrator - Conditional Access administrator - Exchange administrator - Global administrator - Global reader - Helpdesk administrator - Password administrator - Privileged authentication administrator - Privileged role administrator - Security administrator - SharePoint administrator - User administrator WARNING: Ensure administrators are pre-registered with strong authentication before enforcing the policy. After which the policy must be set to On. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless#fido2-security-keys:https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key:https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths:https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy Default Value: No Default Value Found
Enable Azure AD Identity Protection user risk policies	**High**	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 has risky sign-in. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-risk-feedback:https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks Default Value: No Default Value Found

Enable Azure AD Identity Protection sign-in risk policies	**High**	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. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-risk-feedback:https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks Default Value: No Default Value Found
Ensure Microsoft Azure Management is limited to administrative roles	**High**	IMPACT: Item does not meet all the requirements as per test. The Microsoft Azure Management application governs various Azure services and can be secured through the implementation of a Conditional Access policy. This policy can restrict specific user accounts from accessing the related portals and applications. When Conditional Access policy is targeted to the Microsoft Azure Management application, within the Conditional Access policy app picker the policy will be enforced for tokens issued to application IDs of a set of services closely bound to the portal. - Azure Resource Manager - Azure portal, which also covers the Microsoft Entra admin center - Azure Data Lake - Application Insights API - Log Analytics API Microsoft Azure Management should be restricted to specific pre-determined administrative roles. NOTE: Blocking Microsoft Azure Management will prevent non-privileged users from signing into most portals other than Microsoft 365 Defender and Microsoft Purview. Blocking sign-in to Azure Management applications and portals enhances security of sensitive data by restricting access to privileged users. This mitigates potential exposure due to administrative errors or software vulnerabilities, as well as acting as a defense in depth measure against security breaches. PIM functionality will be impacted unless non-privileged users are first assigned to a permanent group or role that is excluded from this policy. When attempting to checkout a role in the Entra ID PIM area they will receive the message Because the policy is applied to the Azure management portal and API, services, or clients with an Azure API service dependency, can indirectly be impacted: Classic deployment model APIs Azure PowerShell Azure CLI Azure DevOps Azure Data Factory portal Azure Event Hubs Azure Service Bus Azure SQL Database

		SQL Managed Instance Azure Synapse Visual Studio subscriptions administrator portal Microsoft IoT Central ACTION: To enable Microsoft Azure Management restrictions: 1. Navigate to the Microsoft Entra admin center https://entra.microsoft.com. 2. Click expand Protection > Conditional Access select Policies. 3. Click New Policy and then name the policy. 4. Select Users > Include > All Users 5. Select Users > Exclude > Directory roles and select only administrative roles. See audit section for more information. 6. Select Cloud apps or actions > Select apps > Select then click the box next to Microsoft Azure Management. 7. Click Select. 8. Select Grant > Block access and click Select. 9. Ensure Enable Policy is On then click Create. WARNING: Exclude Global Administrator at a minimum to avoid being locked out. Report-only is a good option to use when testing any Conditional Access policy for the first time. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps Default Value: No - Non-administrators can access the Azure AD administration portal.
Ensure Microsoft Authenticator is configured to protect against MFA fatigue	**High**	IMPACT: Item does not meet all the requirements as per test. Microsoft has released additional settings to enhance the configuration of the Microsoft Authenticator application. These settings provide additional information and context to users who receive MFA passwordless and push requests, such as geographic location the request came from, the requesting application and requiring a number match. Ensure the following are Enabled. - Require number matching for push notifications - Show application name in push and passwordless notifications - Show geographic location in push and passwordless notifications NOTE: On February 27, 2023, Microsoft started enforcing number matching tenant-wide for all users using Microsoft Authenticator. As the use of strong authentication has become more widespread, attackers have started to exploit the tendency of users to experience. This occurs when users are repeatedly asked to provide additional forms of identification, leading them to eventually approve requests without fully verifying the source. To counteract this, number matching can be employed to ensure the security of the authentication process. With this method, users are prompted to confirm a number displayed on their original device and enter it into the device being used for MFA. Additionally, other information such as geolocation and application details are displayed to enhance the end users awareness. Among these 3 options, number matching provides the strongest net security gain. Additional interaction will be required by end users using number matching as opposed to simply pressing for login attempts. ACTION: To configure Microsoft Authenticator to protect against MFA fatigue:

		1. Navigate to the Microsoft Entra admin center https://entra.microsoft.com. 2. Click to expand Protection > Authentication methods select Policies. 3. Select Microsoft Authenticator 4. Under Enable and Target ensure the setting is set to Enable. 5. Select Configure 6. Set the following Microsoft Authenticator settings: - Require number matching for push notifications Status is set to Enabled, Target All users - Show application name in push and passwordless notifications is set to Enabled, Target All users - Show geographic location in push and passwordless notifications is set to Enabled, Target All users Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-default-enablement:https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/defend-your-users-from-mfa-fatigue-attacks/ba-p/2365677:https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match Default Value: Microsoft-managed
Ensure custom banned passwords lists are used	**High**	IMPACT: Item does not meet all the requirements as per test. With Azure AD Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. To support business and security needs, custom banned password lists can be defined. When users change or reset their passwords, these banned password lists are checked to enforce the use of strong passwords. A custom banned password list should include some of the following examples: - Brand names - Product names - Locations, such as company headquarters - Company-specific internal terms - Abbreviations that have specific company meaning Creating a new password can be difficult regardless of ones technical background. It is common to look around ones environment for suggestions when building a password, however, this may include picking words specific to the organization as inspiration for a password. An adversary may employ what is called a mangler to create permutations of these specific words in an attempt to crack passwords or hashes making it easier to reach their goal. If a custom banned password list includes too many common dictionary words, or short words that are part of compound words, then perfectly secure passwords may be blocked. The organization should consider a balance between security and usability when creating a list. ACTION: Create a custom banned password list: 1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/ 2. Click to expand Protection > Authentication methods 3. Select Password protection 4. Set Enforce custom list to Yes 5. In Custom banned password list create a list using suggestions outlined in this document. 6. Click Save

		NOTE: Below is a list of examples that can be used as a starting place. The references section contains more suggestions. - Brand names - Product names - Locations, such as company headquarters - Company-specific internal terms - Abbreviations that have specific company meaning Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#custom-banned-password-list:https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection Default Value: No Default Value Found
Ensure that password protection is enabled for Active Directory	**NotExecuted**	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 Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations Default Value: Enable - Yes Mode - Audit
Ensure Self service password reset enabled is set to All	**Passed**	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/let-users-reset-passwords?view=o365-worldwide:https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr:https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-registration-mfa-sspr-combined Default Value: No Default Value Found
Ensure the self-service password reset activity report is reviewed at least weekly	**Passed**	IMPACT: Auditing is in place and report is being reviewed. ACTION: Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-reporting:https://learn.microsoft.com/en-us/azure/active-directory/authentication/troubleshoot-sspr Default Value: No Default Value Found

Ensure the Azure AD Risky sign-ins report is reviewed at least weekly	**Passed**	IMPACT: Auditing is in place and report is being reviewed. ACTION: Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock Default Value: No Default Value Found
Use Just In Time privileged access to Microsoft 365 roles	**High**	IMPACT: Just In Time Access is not enabled for Microsoft 365 Roles. Implementation of Just in Time privileged access is likely to necessitate changes to administrator routine. Administrators will only be granted access to administrative roles when required. When administrators request role activation, they will need to document the reason for requiring role access, anticipated time required to have the access, and to reauthenticate to enable role access. ACTION: Azure Active Directory Privileged Identity Management can be used to audit roles, allow just in time activation of roles and allow for periodic role attestation. Organizations should remove permanent members from privileged Microsoft 365 roles and instead make them eligible, through a JIT activation workflow. Organizations want to minimize the number of people who have access to secure information or resources, because that reduces the chance of a malicious actor getting that access, or an authorized user inadvertently impacting a sensitive resource. However, users still need to carry out privileged operations in Azure AD and Microsoft 365. Organizations can give users just-in-time (JIT) privileged access to roles. Test Reference: https://learn.microsoft.com/en-us/purview/privileged-access-management Default Value: No Default Value Found
Ensure Privileged Identity Management is used to manage roles	**Passed**	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review:https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview Default Value: By default access reviews are not configured.
Ensure Access reviews for Guest Users are configured	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. Access reviews enable administrators to establish an efficient automated process for reviewing group memberships, access to enterprise applications, and role assignments. These reviews can be scheduled to recur regularly, with flexible options for delegating the task of reviewing membership to different members of the organization. Ensure Access reviews for Guest Users are configured to be performed no less frequently than monthly. Access to groups and applications for guests can change over time. If a guest users access to a particular folder goes unnoticed, they may unintentionally gain access to sensitive data if a member adds new files or data to the folder or application. Access reviews can help reduce the risks associated with outdated assignments by requiring a member of the organization to conduct the reviews. Furthermore, these reviews can enable a fail-closed mechanism to remove access to the subject if the reviewer does not respond to the review.

		Access reviews that are ignored may cause guest users to lose access to resources temporarily. ACTION: Create an access review for Guest Users: 1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/ 2. Click to expand Identity Governance and select Access reviews 3. Click New access review. 4. Select what to review choose Teams + Groups. 5. Review Scope set to All Microsoft 365 groups with guest users, do not exclude groups. 6. Scope set to Guest users only then click Next: Reviews. 7. Select reviewer as an appropriate user that is NOT the guest user themselves. 8. Duration (in days) at most 3. 9. Review recurrence is Monthly or more frequent. 10. End is set to Never, then click Next: Settings. 11. Check Auto apply results to resource. 12. Set If reviewers don't respond to Remove access. 13. Check the following: Justification required, E-mail notifications, Reminders. 14. Click Next: Review + Create and finally click Create. Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review:https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview Default Value: By default access reviews are not configured.
Ensure Access reviews for high privileged Azure AD roles are configured	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. **Access reviews enable administrators to establish an efficient automated process for reviewing group memberships, access to enterprise applications, and role assignments. These reviews can be scheduled** to recur regularly, with flexible options for delegating the task of reviewing membership to different members of the organization. **Ensure Access reviews for high privileged Azure AD roles are done no less frequently than weekly. These reviews should inc**lude at a minimum the roles listed below: - Global Administrator - Exchange Administrator - SharePoint Administrator - Teams Administrator - Security Administrator NOTE: An access review is created for each role selected after completing the process. **Regular review of critical high privileged roles in Azure AD will help identify role drift, or potential malicious activity. This will enable the practice and application of where even non-privileged users like security auditors can be assigned to review as**signed roles in an organization. Furthermore, if configured these reviews can enable a fail-closed mechanism to remove access to the subject if the reviewer does not respond to the review. **ACTION:** Create an access review for high privileged roles: 1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/ 2. Click to expand Identity Governance and select Privileged Identity Management 3. Select Azure AD Roles under Manage

		4. Select Access reviews and click New access review. 5. Provide a name and description. 6. Frequency set to Weekly or more frequent. 7. Duration (in days) is set to at most 3. 8. End set to Never. **9. Role select these roles: Global Administrator,Exchange Administra**tor,SharePoint Administrator,Teams Administrator,Security Administrator 9. Assignment type set to All active and eligible assignments. 10. Reviewers set to Selected user(s) or group(s) **11. Select reviewers are member(s) responsible for this type of review**. 12. Auto apply results to resource set to Enable 13. If reviewers don't respond is set to No change 14. Show recommendations set to Enable 15. Require reason or approval set to Enable 16. Mail notifications set to Enable 17. Reminders set to Enable **18.** Click Start to save the review. **NOTE: Reviewers will have the ability to revoke roles should be trusted individuals who understand the impact of the access reviews. The principle of separation of duties should be considered so that no one administrator i**s reviewing their own access levels. **Test Reference: https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review:https://learn.microsoft.com/en-us/azure/active-directory/gover**nance/access-reviews-overview **Default Value: By default access reviews are not configured.**

8.5 Microsoft Exchange admin center

Test	Status	Remark
Ensure AuditDisabled organizationally is set to False	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:** Test Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-mailboxes?view=o365-worldwide:https://learn.microsoft.com/en-us/powershell/module/exchange/set-organizationconfig?view=exchange-ps#-auditdisabled Default Value: FALSE
Ensure mailbox auditing for E3 users is Enabled	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:** Test Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-mailboxes?view=o365-worldwide Default Value: AuditEnabled: True for all mailboxes except below: - Resource Mailboxes - Public Folder Mailboxes - DiscoverySearch Mailbox

		AuditAdmin: ApplyRecord, Create, HardDelete, MoveToDeletedItems, SendAs, SendOnBehalf, SoftDelete, Update, UpdateCalendarDelegation, UpdateFolderPermissions, UpdateInboxRules **AuditDelegate:** ApplyRecord, Create, HardDelete, MoveToDeletedItems, SendAs, SendOnBehalf, SoftDelete, Update, UpdateFolderPermissions, UpdateInboxRules **AuditOwner:** ApplyRecord, HardDelete, MoveToDeletedItems, SoftDelete, Update, UpdateCalendarDelegation, UpdateFolderPermissions, UpdateInboxRules
Ensure mailbox auditing for E5 users is Enabled	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:** Test Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-mailboxes?view=o365-worldwide Default Value: AuditEnabled: True for all mailboxes except below: - Resource Mailboxes - Public Folder Mailboxes - DiscoverySearch Mailbox **AuditAdmin:** ApplyRecord, Create, HardDelete, MailItemsAccessed, MoveToDeletedItems, Send, SendAs, SendOnBehalf, SoftDelete, Update, UpdateCalendarDelegation, UpdateFolderPermissions, UpdateInboxRules **AuditDelegate:** ApplyRecord, Create, HardDelete, MailItemsAccessed, MoveToDeletedItems, SendAs, SendOnBehalf, SoftDelete, Update, UpdateFolderPermissions, UpdateInboxRules **AuditOwner:** ApplyRecord, HardDelete, MailItemsAccessed, MoveToDeletedItems, Send, SoftDelete, Update, UpdateCalendarDelegation, UpdateFolderPermissions, UpdateInboxRules
Ensure AuditBypassEnabled is not enabled on mailboxes	**High**	**IMPACT:** Item does not meet all the requirements as per test. When configuring a user or computer account to bypass mailbox audit logging, the system will not record any access or actions performed by the said user or computer account on any mailbox. Administratively this was introduced to reduce the volume of entries in the mailbox audit logs on trusted user or computer accounts. Ensure AuditBypassEnabled is not enabled on accounts without a written exception. If a mailbox audit bypass association is added for an account, the account can access any mailbox in the organization to which it has been assigned access permissions, without generating any mailbox audit logging entries for such access or recording any actions taken, such as message deletions. Enabling this parameter, whether intentionally or unintentionally, could allow insiders or malicious actors to conceal their activity on specific mailboxes. Ensuring proper logging of user actions and mailbox operations in the audit log will enable comprehensive incident response and forensics. None - this is the default behavior.

		ACTION: Disable Audit Bypass on all mailboxes using PowerShell:
		
		1. Connect to Exchange Online using Connect-ExchangeOnline.
		2. The following example PowerShell script will disable AuditBypass for all mailboxes which currently have it enabled:
		
		# Get mailboxes with AuditBypassEnabled set to $true
		$MBXAudit = Get-MailboxAuditBypassAssociation -ResultSize unlimited | Where-Object { $_.AuditBypassEnabled -eq $true }
		
		foreach ($mailbox in $MBXAudit) {
		$mailboxName = $mailbox.Name
		Set-MailboxAuditBypassAssociation -Identity $mailboxName -AuditBypassEnabled $false
		Write-Host -ForegroundColor Green
		}
		
		Test Reference: https://learn.microsoft.com/en-us/powershell/module/exchange/get-mailboxauditbypassassociation?view=exchange-ps
		Default Value: AuditBypassEnabled False

Ensure Microsoft 365 Exchange Online Admin Auditing Is Enabled	**Passed**	**IMPACT:** Microsoft 365 Admin Auditing is enabled. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Exchange Online Unified Auditing Is Enabled	**Passed**	**IMPACT:** Microsoft 365 Unified Auditing is enabled. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure all forms of mail forwarding are blocked and-or disabled	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:** Test Reference: https://learn.microsoft.com/en-us/exchange/policy-and-compliance/mail-flow-rules/mail-flow-rule-procedures?view=exchserver-2019:https://techcommunity.microsoft.com/t5/exchange-team-blog/all-you-need-to-know-about-automatic-email-forwarding-in/ba-p/2074888#:~:text=%20%20%20Automatic%20forwarding%20option%20%20,%:https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/outbound-spam-policies-external-email-forwarding?view=o365-worldwide Default Value: No Default Value Found

Ensure mail transport rules do not whitelist specific domains	**Passed**	**IMPACT:** Mail Transport rules are configured not to forward to specific domains. **ACTION:** Test Reference: https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/configuration-best-practices:https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules Default Value: No Default Value Found
Ensure Tagging is enabled for External Emails	**High**	**IMPACT:** Tagging is not enabled for external emails. Since most scam emails originate from external sources, its better to create awareness among users before opening the external emails. With the External email tagging feature, an External tag can be added to the external emails. It helps Outlook users handle those emails with extra attention. **ACTION:** It is recommended to enable tagging for all external emails. Please use Set-ExternalInOutlook ?Enabled $true to enable tagging. Test Reference: https://techcommunity.microsoft.com/t5/exchange-team-blog/native-external-sender-callouts-on-email-in-outlook/ba-p/2250098:https://learn.microsoft.com/en-us/powershell/module/exchange/set-externalinoutlook?view=exchange-ps Default Value: Disabled (False)
Ensure Tagging does not allow specific domains	**Passed**	**IMPACT:** Tagging does not allow specific domains. **ACTION:** Test Reference: https://techcommunity.microsoft.com/t5/exchange-team-blog/native-external-sender-callouts-on-email-in-outlook/ba-p/2250098:https://learn.microsoft.com/en-us/powershell/module/exchange/set-externalinoutlook?view=exchange-ps Default Value: Disabled (False)
Ensure Transport Rules to Block Exchange Auto-Forwarding is configured	**High**	**IMPACT:** Item does not meet all the requirements as per test. No Exchange Online Transport Rules are in place to block email auto-forwarding. Cyber adversaries often configure compromised Office 365 accounts to forward emails to external persons. It is therefore advisable to configure an Exchange transport rule that blocks auto-forwarded emails. **ACTION:** Navigate to the Mail Flow; Rules screen in the Exchange Admin Center. Add a rule that applies when the message is auto-forwarded and takes the action of blocking the message. An article in the References section also describes this process. There are additional steps below that detail how to stop email forwarding. Test Reference: No Link Found Default Value: No Default Value Found
Ensure Do Not Bypass the Safe Attachments Filter is not configured	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:**

		Test Reference: https //www.undocumented-features.com/2018/05/10/atp-safe-attachments-safe-links-and-anti-phishing-policies-or-all-the-policies-you-can-shake-a-stick-at/#Bypass_Safe_Attachments_Processing Default Value: No Default Value Found
Ensure Do Not Bypass the Safe Links Feature is not configured	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:** Test Reference: https //www.undocumented-features.com/2018/05/10/atp-safe-attachments-safe-links-and-anti-phishing-policies-or-all-the-policies-you-can-shake-a-stick-at/#Bypass_Safe_Attachments_Processing Default Value: No Default Value Found
Ensure Exchange Modern Authentication is Enabled	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:** Test Reference: https //docs.microsoft.com/en-us/powershell/module/exchange/set-organizationconfig?view=exchange-ps Default Value: No Default Value Found
Ensure Transport Rules to Block Executable Attachments are configured	**Passed**	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: https //docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/manage-mail-flow-rules Default Value: No Default Value Found
Ensure Dangerous Attachment Extensions are Filtered is configured	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. Email is a primary vector of exploitation. It is common for attackers to send malicious file attachments designed to mimic legitimate business files. A list of historically malicious extensions that should be blocked/filtered from O365 emails is checked against the Tenant's malware filters to determine if these file types are being blocked. The file extensions listed herein are on this list of dangerous file extensions, but no O365 Malware Filter Policy is configured to filter them. Creating filters for these file types may decrease the risk of malware spreading within the organization through phishing or lateral phishing. The common malicious attachments defined in O365 at the time this document was authored are xll, wll, rtf, reg, ws, wsf, vb, wsc, wsh, msh, msh1, msh2, mshxml, msh1xml, msh2xml, ps1, ps1xml, ps2, ps2xml, psc1, psc2, pif, msi, gadget, application, com, cpl, msc, hta, msp, bat, cmd, js, jse, scf, lnk, inf, dotm, xlsm, xltm, xlam, pptm, potm, ppam, ppsm, sldm. ACTION: This feature is accessible in the Security portal of the O365 Admin Center. Click through to Threat management; Policy; Anti-malware, and either edit the Default policy to include the above extensions, or create a custom policy to filter these extensions. Additionally, if other known dangerous attachment types are added to this exceptions list, they may be quickly filtered. However it is recommended to create a new policy to accomplish this as it is a more ideal long-term solution. Before doing this, consider polling key stakeholders in the organization or using available data to determine whether any of these file types are commonly exchanged via email within the organization. The complete list of additional file types may be added using the listed PowerShell commands.

		Test Reference: https //docs.microsoft.com/en-us/powershell/module/exchange/set-malwarefilterpolicy?view=exchange-ps Default Value: No Default Value Found
Ensure Malware Filter Policies Alert for Internal Users Sending Malware is configured	**Passed**	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: https //docs.microsoft.com/en-us/powershell/module/exchange/set-malwarefilterpolicy?view=exchange-ps Default Value: No Default Value Found
Ensure Transport Rules to Block Large Attachments are configured	**Passed**	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: https //docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/common-attachment-blocking-scenarios Default Value: No Default Value Found
Ensure Mailbox Auditing is Enabled at Tenant Level	**Passed**	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: https //docs.microsoft.com/en-us/powershell/module/exchange/set-organizationconfig?view=exchange-ps Default Value: No Default Value Found
Ensure Mailboxes without Mailbox Auditing are not present	**Passed**	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: https //docs.microsoft.com/en-us/powershell/module/exchange/set-mailbox?view=exchange-ps Default Value: No Default Value Found
Ensure Exchange Mailboxes with IMAP is not Enabled	**Passed**	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: https //www.ic3.gov/Media/Y2020/PSA200406 Default Value: No Default Value Found
Ensure Exchange Mailboxes with POP is not Enabled	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. The Exchange Online mailboxes listed above have POP enabled. POP is a method of accessing an Exchange Online mailbox. Cyber adversaries have used POP as a workaround for subtly conducting password spraying attacks or other credential-related attacks, because POP is a form of legacy authentication generally not subject to the restraints of Multi-Factor Authentication and other modern

		authentication safeguards. For these reasons it is recommended that POP be disabled where possible. ACTION: This finding refers to individual mailboxes that have POP enabled. For these mailboxes, POP authentication can be disabled using the Set-CASMailbox commandlet as follows Set-CASMailbox -Identity [MailboxName] -PopEnabled $false where the -Identity flag is the user's email address. A list of affected email addresses is included in this report. Key stakeholders should be polled prior to making this change, as there is a chance POP is used within the organization for legacy applications or service accounts. Test Reference: https //www.ic3.gov/Media/Y2020/PSA200406 Default Value: No Default Value Found
Ensure Exchange Online Mailboxes with SMTP Authentication is not Enabled	**High**	IMPACT: Item does not meet all the requirements as per test. The Exchange Online mailboxes listed above have SMTP Authentication enabled. SMTP Authentication is a method of authenticating to an Exchange Online mailbox. Cyber adversaries have used SMTP authentication as a workaround for subtly conducting password spraying attacks or other credential-related attacks, because SMTP authentication is a form of legacy authentication generally not subject to the restraints of Multi-Factor Authentication and other modern authentication safeguards. For these reasons it is recommended that SMTP Authentication be disabled where possible. ACTION: SMTP can be globally disabled using Exchange Online PowerShell using the Set-TransportConfig command, such as Set-TransportConfig -SmtpClientAuthenticationDisabled $true. However, this finding refers to individual mailboxes that have SMTP enabled. For these mailboxes, SMTP authentication can be disabled using the Set-CASMailbox commandlet as follows Set-CASMailbox -Identity [MailboxName] -SmtpClientAuthenticationDisabled $true where the -Identity flag is the user's email address. A list of affected email addresses is included in this report. Test Reference: https //www.ic3.gov/Media/Y2020/PSA200406 Default Value: No Default Value Found
Ensure Common Malicious Attachment Extensions are Filtered	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. O365 includes a list of common malicious file attachment extensions that should be blocked/filtered from O365 emails. The file extensions listed herein are on this list of common malicious file extensions, but no O365 Malware Filter Policy is configured to filter them. Enabling common malicious attachment filtering may decrease the risk of malware spreading within the organization through phishing or lateral phishing. The common malicious attachments defined in O365 at the time this document was authored are ace, ani, app, docm, exe, jar, reg, scr, vbe, vbs. ACTION: This feature is accessible in the Security portal of the O365 Admin Center. Click through to Threat management; Policy; Anti-malware and toggle the Common Attachment Types Filter to 'On'. Additionally, other known dangerous attachment types may be quickly filtered by adding them to this policy's list, although creating a new policy to do this would be a more ideal long-term solution. Before doing this, consider polling key stakeholders in the organization or using available data to determine whether any of these file types are commonly exchanged via email within the organization. Test Reference: https //docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide#anti-malware-policies

		Default Value: No Default Value Found
Ensure Safe Attachments is Enabled	**High**	IMPACT: Item does not meet all the requirements as per test. The Microsoft Office 365 Safe Attachments feature is not enabled. Safe Attachments is a Microsoft feature that uses behavioral analysis and detonation in a virtual environment to add another layer of defense against malware on top of existing Exchange Online anti-malware policies. It is recommended to enable this feature. This finding may also indicate that the O365 license tier does not enable ATP features. ACTION: Safe Attachments can be configured by navigating to the Threat Management portal in the Office 365 Security and Compliance center. The first reference below is a detailed guide to configuring ATP Safe Attachments. Test Reference: https //docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-safe-attachments-policies?view=o365-worldwide Default Value: No Default Value Found
Ensure Safe Links is Enabled	**High**	IMPACT: Item does not meet all the requirements as per test. Safe Links is a feature of O365 that enables real-time detection of malicious links in incoming Exchange emails and other Office 365 applications, such as Microsoft Teams. Safe Links is not enabled in the O365 tenant. This may be because the organization does not have the appropriate license level to use the feature, or because it has been disabled. This lowers the amount of built-in protection O365 offers the organization against phishing and other attacks. ACTION: Safe Links can be configured by navigating to the Threat Management portal in the Office 365 Security and Compliance center. The first guide below is a quick introduction to enabling Safe Links while the second is a detailed reference. Test Reference: https //docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links?view=o365-worldwide Default Value: No Default Value Found
Ensure Safe Links Click-Through is Not Allowed	**High**	IMPACT: Item does not meet all the requirements as per test. Advanced Threat Protection Safe Links (ATP Safe Links) is an Office 365 feature that enables the detection of suspicious links used in attacks delivered via Exchange Email and Teams, such as phishing attacks. ATP Safe Links is configured to allow users to click through a link flagged as unsafe if they choose. It is recommended to disable this ability, as users will often click through to potentially unsafe links if they are given the choice, partially negating the benefit of Safe Links. ACTION: Use the Set-SafeLinksPolicy function in the Exchange Online PowerShell module as follows Set-SafeLinksPolicy -AllowClickThrough $false. Test Reference: https //docs.microsoft.com/en-us/powershell/module/exchange/set-safelinkspolicy?view=exchange-ps Default Value: No Default Value Found
Ensure Safe Links Flags Links in Real Time	**High**	IMPACT: Item does not meet all the requirements as per test. Safe Links is an Office 365 feature that enables the detection of suspicious links used in attacks delivered via Exchange Email and Teams, such as phishing attacks. ATP Safe Links can be configured to flag dangerous links in email and guarantee that the email will not be delivered until the Safe Links scanning is complete. This is the ideal Safe Links setting. However, this setting is currently disabled, which

		means it is possible for emails to be delivered before Safe Links protections have been applied. It is also possible that this inspector finding was generated because ATP Safe Links is not enabled or the organization does not have an appropriate O365 license tier to use ATP Safe Links features, in which case the remediation described below would not apply. ACTION: Use the Set-SafeLinksPolicy function in the Exchange Online PowerShell module as follows Set-SafeLinksPolicy -DeliverMessageAfterScan $false. Test Reference: https //docs.microsoft.com/en-us/powershell/module/exchange/set-safelinkspolicy?view=exchange-ps Default Value: No Default Value Found
Ensure SMTP Authentication is disabled Globally	**High**	IMPACT: Item does not meet all the requirements as per test. SMTP Authentication is a method of authenticating to an Exchange Online mailbox to deliver email. Cyber adversaries have used SMTP authentication as a workaround for subtly conducting password spraying attacks or other credential-related attacks and bypassing Multi-Factor Authentication protection because legacy authentication methods such as SMTP do not support MFA. There are two ways of disabling SMTP, globally and granularly on a per-user-mailbox level. It is recommended that SMTP Authentication be globally disabled if possible. Note that this may disrupt the functionality of legacy or other applications that require it for continued operations., ACTION: Use the Exchange Online administration module for PowerShell to execute the listed PowerShell command. Note that SMTP authentication for individual mailboxes may still need to be located and disabled using the Set-CASMailbox command with the -SmtpClientAuthenticationDisabled script., Test Reference: https //docs.microsoft.com/en-us/powershell/module/exchange/set-casmailbox?view=exchange-ps Default Value: No Default Value Found
Ensure mail transport rules do not forward email to external domains	**Passed**	IMPACT: Mail Transport Rules are configured correctly not to forward to external domains. ACTION: Test Reference: https //image.communications.cyber.nj.gov/lib/fe3e15707564047c7c1270/m/2/FBI+PIN+-+11.25.2020.pdf Default Value: No Default Value Found
Ensure automatic forwarding options are disabled	**High**	IMPACT: Care should be taken before implementation to ensure there is no business need for case- by-case auto-forwarding. ACTION: Disabling auto-forwarding to remote domains will affect all users in an organization. Test Reference: https //image.communications.cyber.nj.gov/lib/fe3e15707564047c7c1270/m/2/FBI+PIN+-+11.25.2020.pdf Default Value: No Default Value Found

Ensure the Client Rules Forwarding Block is enabled	**High**	IMPACT: Client Rules Forwarding is not blocked. Care should be taken before implementation to ensure there is no business need for case- by-case auto-forwarding. Disabling auto-forwarding to remote domains will affect all users in an organization. ACTION: You should set your Exchange Online mail transport rules to not forward email to domains outside of your organization. Automatic forwarding to prevent users from auto-forwarding mail via Outlook or Outlook on the web should also be disabled. Alongside this Client Rules Forwarding Block, which prevents the use of any client-side rules that forward email to an external domain, should also be enabled. Test Reference: No Link Found Default Value: No Default Value Found
Ensure the Advanced Threat Protection Safe Links policy is enabled	**Passed**	IMPACT: Advanced Threat Protection Safe Links Policy is enabled. ACTION: Test Reference: https //docs.microsoft.com/en-us/powershell/module/exchange/set-safelinkspolicy?view=exchange-ps Default Value: No Default Value Found
Ensure the Advanced Threat Protection SafeAttachments policy is enabled	**Passed**	IMPACT: Safe Attachment Policy is enabled. ACTION: Test Reference: https //docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-safe-attachments-policies?view=o365-worldwide Default Value: No Default Value Found
Ensure that an anti-phishing policy has been created	**Passed**	IMPACT: Anti-Phishing Policy has been created. ACTION: Test Reference: https //docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-mdo-anti-phishing-policies?view=o365-worldwide Default Value: No Default Value Found
Ensure mailbox auditing for all users is Enabled	**Passed**	IMPACT: No mailboxes found without auditing. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
Ensure users installing Outlook add-ins is not allowed	**High**	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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/add-ins-for-outlook/specify-who-can-install-and-manage-add-ins?source=recommendations:https://learn.microsoft.com/en-us/exchange/permissions-exo/role-assignment-policies Default Value: UI - My Custom Apps, My Marketplace Apps, and My ReadWriteMailboxApps are checked PowerShell - My Custom Apps My Marketplace Apps and My ReadWriteMailboxApps are assigned
Ensure mail forwarding rules are reviewed at least weekly	**Passed**	IMPACT: Auditing Process is created and followed. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
Ensure the Mailbox Access by Non-Owners Report is reviewed at least biweekly	**NotExecuted**	IMPACT: Auditing Process needs to be created and followed. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
Ensure the Malware Detections report is reviewed at least weekly	**Passed**	IMPACT: Test has passed. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
Ensure the report of users who have had their email privileges restricted due to spamming is reviewed	**NotExecuted**	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. Test Reference: No Link Found Default Value: No Default Value Found

Ensure Microsoft 365 Deleted Mailboxes are identified and Verified	**Passed**	IMPACT: No deleted Mailboxes were found. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Hidden Mailboxes are Identified	**Passed**	IMPACT: No mailbox found with hidden flag. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
Ensure Mailboxes External Address Forwarding is not configured	**Passed**	IMPACT: No Mailboxes are configured with the Forwarding. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
Ensure Exchange Online Mailboxes on Litigation Hold	**Passed**	IMPACT: No Mailboxes are on litigation hold. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
Ensure Exchange Online SPAM Domains are identified	**High**	IMPACT: Found SPAM Items. It is a security risk. ACTION: Identify the SPAM domains and block them. Test Reference: No Link Found Default Value: No Default Value Found
Ensure Exchange Online Mailbox Auditing is enabled	**Passed**	IMPACT: Auditing is enabled for Exchange Online Mailboxes. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
Microsoft 365 Exchange Online Admin Success and Failure Attempts	**Passed**	IMPACT: No Failure Attempts were found. ACTION: Test Reference: No Link Found

		Default Value: No Default Value Found
Microsoft 365 Exchange Online External Access Admin Success and Failure Attempts	**Passed**	IMPACT: No Failure Attempts were found from external Admins. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
Ensure modern authentication for Exchange Online is enabled	**Passed**	IMPACT: **Modern Authentication is enabled for Exchange Online.** ACTION: Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/enable-or-disable-modern-authentication-in-exchange-online **Default Value: TRUE**

8.6 Microsoft SharePoint Admin Center

Test	Status	Remark
Ensure modern authentication for SharePoint applications is required	**High**	**IMPACT:** Basic Authentication is not enabled for SharePoint Online. Implementation 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. Test Reference: https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps Default Value: True (Apps that don't use modern authentication are allowed)
Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled	**NotExecuted**	**IMPACT:** Item does not meet all the requirements as per test. Azure AD B2B provides authentication and management of guests. Authentication happens via one-time passcode when they don't already have a work or school account or a Microsoft account. Integration with SharePoint and OneDrive allows for more granular control of how guest user accounts are managed in the organizations AAD, unifying a similar guest experience already deployed in other Microsoft 365 services such as Teams. Note: Global Reader role currently cannot access SharePoint using PowerShell. External users assigned guest accounts will be subject to Azure AD access policies, such as multi-factor authentication. This provides a way to manage guest identities and control access to SharePoint and OneDrive resources. Without this integration, files can be shared without account registration, making it more challenging to audit and manage who has access to the organizations data. Azure B2B collaboration is used with other Azure services so should not be new or unusual. Microsoft also has made the experience seamless when turning on integration on SharePoint sites that already have active files shared with guest users. The referenced Microsoft article on the subject has more details on this.

		ACTION: To remediate using PowerShell: 1. Connect to SharePoint Online using Connect-SPOService 2. Run the following command: Set-SPOTenant -EnableAzureADB2BIntegration $true Test Reference: https://learn.microsoft.com/en-us/sharepoint/sharepoint-azureb2b-integration#enabling-the-integration:https://learn.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b:https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps Default Value: FALSE
Ensure external content sharing is restricted	**High**	**IMPACT:** Item does not meet all the requirements as per test. The external sharing settings govern sharing for the organization overall. Each site has its own sharing setting that can be set independently, though it must be at the same or more restrictive setting as the organization. The new and existing guests option requires people who have received invitations to sign in with their work or school account (if their organization uses Microsoft 365) or a Microsoft account, or to provide a code to verify their identity. Users can share with guests already in your organizations directory, and they can send invitations to people who will be added to the directory if they sign in. The recommended state is New and existing guests or less permissive. Forcing guest authentication on the organizations tenant enables the implementation of controls and oversight over external file sharing. When a guest is registered with the organization, they now have an identity which can be accounted for. This identity can also have other restrictions applied to it through group membership and conditional access rules. When using Azure AD B2B integration, Azure AD external collaboration settings, such as guest invite settings and collaboration restrictions apply. **ACTION:** To remediate using the UI: 1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint 2. Click to expand Policies > Sharing. 3. Locate the External sharing section. 4. Under SharePoint, move the slider bar to New and existing guests or a less permissive level. - OneDrive will also be moved to the same level and can never be more permissive than SharePoint. To remediate using PowerShell: 1. Connect to SharePoint Online service using Connect-SPOService. 2. Run the following cmdlet to establish the minimum recommended state: Set-SPOTenant -SharingCapability ExternalUserSharingOnly Note: Other acceptable values for this parameter that are more restrictive include: Disabled and ExistingExternalUserSharingOnly.

		Test Reference: https://learn.microsoft.com/en-US/sharepoint/turn-external-sharing-on-or-off?WT.mc_id=365AdminCSH_spo:https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps Default Value: Anyone (ExternalUserAndGuestSharing)
Ensure OneDrive content sharing is restricted	**NotExecuted**	**IMPACT:** Item does not meet all the requirements as per test. This setting governs the global permissiveness of OneDrive content sharing in the organization. OneDrive content sharing can be restricted independent of SharePoint but can never be more permissive than the level established with SharePoint. The recommended state is Only people in your organization. OneDrive, designed for end-user cloud storage, inherently provides less oversight and control compared to SharePoint, which often involves additional content overseers or site administrators. This autonomy can lead to potential risks such as inadvertent sharing of privileged information by end users. Restricting external OneDrive sharing will require users to transfer content to SharePoint folders first which have those tighter controls. Users will be required to take additional steps to share OneDrive content or use other official channels. **ACTION:** To remediate using the UI: 1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint 2. Click to expand Policies > Sharing. 3. Locate the External sharing section. 4. Under OneDrive, set the slider bar to Only people in your organization. To remediate using PowerShell: 1. Connect to SharePoint Online service using Connect-SPOService. 2. Run the following cmdlet: Set-SPOTenant -OneDriveSharingCapability Disabled Test Reference: No Link Found Default Value: Anyone (ExternalUserAndGuestSharing)
Ensure that SharePoint guest users cannot share items they dont own	**High**	**IMPACT:** Item does not meet all the requirements as per test. SharePoint gives users the ability to share files, folders, and site collections. Internal users can share with external collaborators, and with the right permissions could share to other external parties. Sharing and collaboration are key; however, file, folder, or site collection owners should have the authority over what external users get shared with to prevent unauthorized disclosures of information. The 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. However, if users do regularly share with guests/externally, minimum impacts could occur as those external users will be unable to re-share content. **ACTION:** To remediate using the UI:

		1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint 2. Click to expand Policies then select Sharing. 3. Expand More external sharing settings, uncheck Allow guests to share items they don't own. 4. Click Save. To remediate using PowerShell: 1. Connect to SharePoint Online service using Connect-SPOService. 2. Run the following SharePoint Online PowerShell command: Set-SPOTenant -PreventExternalUsersFromResharing $True Test Reference: https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off:https://learn.microsoft.com/en-us/sharepoint/external-sharing-overview Default Value: Checked (False)
Ensure document sharing is being controlled by domains with whitelist or blacklist	**Passed**	**IMPACT:** Document Sharing control for domains is configured. **ACTION:** Test Reference: No Link Found Default Value: Limit external sharing by domain is unchecked SharingDomainRestrictionMode: None SharingDomainRestrictionMode: <Undefined>
Ensure link sharing is restricted in SharePoint and OneDrive	**NotExecuted**	**IMPACT:** Item does not meet all the requirements as per test. This setting sets the default link type that a user will see when sharing content in OneDrive or SharePoint. It does not restrict or exclude any other options. The recommended state is Specific people (only the people the user specifies) By defaulting to specific people, the user will first need to consider whether or not the content being shared should be accessible by the entire organization versus select individuals. This aids in reinforcing the concept of least privilege. **ACTION:** To audit using the UI: 1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint 2. Click to expand Policies > Sharing. 3. Scroll to Filer and folder links. 4. Set Choose the type of link thats selected by default when users share files and folders in SharePoint and OneDrive to Specific people (only the people the user specifies) To remediate using PowerShell: 1. Connect to SharePoint Online using Connect-SPOService. 2. Run the following PowerShell command: Set-SPOTenant -DefaultSharingLinkType Direct

		Test Reference: https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps Default Value: Only people in your organization (Internal)
Ensure external sharing is restricted by security group	**NotExecuted**	**IMPACT:** Item does not meet all the requirements as per test. External sharing of content can be restricted to specific security groups. This setting is global, applies to sharing in both SharePoint and OneDrive and cannot be set at the site level in SharePoint. The recommended state is Enabled or Checked. Note: Users in these security groups must be allowed to invite guests in the Azure Active Directory guest invite settings in Microsoft Entra. Identity > External Identities > External collaboration settings Organizations wishing to create tighter security controls for external sharing can set this to enforce role-based access control by using security groups already defined in Microsoft Entra. OneDrive will also be governed by this and there is no granular control at the SharePoint site level. **ACTION:** To remediate using the UI: 1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint 2. Click to expand Policies > Sharing. 3. Scroll to and expand More external sharing settings. 4. Set the following: - Check Allow only users in specific security groups to share externally - Define Manage security groups in accordance with company procedure. Test Reference: https://learn.microsoft.com/en-us/sharepoint/manage-security-groups Default Value: Unchecked/Undefined
Ensure expiration time for external sharing links is set	**Passed**	**IMPACT:** Expiration time for External Sharing Links is set. **ACTION:** Test Reference: https://learn.microsoft.com/en-US/sharepoint/turn-external-sharing-on-or-off?WT.mc_id=365AdminCSH_spo#change-the-organization-level-external-sharing-setting:https://learn.microsoft.com/en-us/microsoft-365/community/sharepoint-security-a-team-effort Default Value: ExternalUserExpirationRequired $false ExternalUserExpireInDays 60 days
Ensure reauthentication with verification code is restricted	**NotExecuted**	**IMPACT:** Item does not meet all the requirements as per test. This setting configures if guests who use a verification code to access the site or links are required to reauthenticate after a set number of days. The recommended state is 15 or less. By increasing the frequency of times guests need to reauthenticate this ensures guest user access to data is not prolonged beyond an acceptable amount of time.

		Guests who use Microsoft 365 in their organization can sign in using their work or school account to access the site or document. After the one-time passcode for verification has been entered for the first time, guests will authenticate with their work or school account and have a guest account created in the hosts organization. Note: If OneDrive and SharePoint integration with Azure AD B2B is enabled as per the CIS Benchmark the one-time-passcode experience will be replaced. Please visit [Secure external sharing in SharePoint - SharePoint in Microsoft 365 | Microsoft Learn](https://learn.microsoft.com/en-US/sharepoint/what-s-new-in-sharing-in-targeted-release?WT.mc_id=365AdminCSH_spo) for more information. **ACTION:** To remediate using the UI: 1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint 2. Click to expand Policies > Sharing. 3. Scroll to and expand More external sharing settings. 4. Set People who use a verification code must reauthenticate after this many days to 15 or less. To remediate using PowerShell: 1. Connect to SharePoint Online service using Connect-SPOService. 2. Run the following cmdlet: Set-SPOTenant -EmailAttestationRequired $true -EmailAttestationReAuthDays 15 Test Reference: https://learn.microsoft.com/en-US/sharepoint/what-s-new-in-sharing-in-targeted-release?WT.mc_id=365AdminCSH_spo:https://learn.microsoft.com/en-US/sharepoint/turn-external-sharing-on-or-off?WT.mc_id=365AdminCSH_spo#change-the-organization-level-external-sharing-setting:https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode Default Value: EmailAttestationRequired : False EmailAttestationReAuthDays : 30
Ensure Microsoft 365 SharePoint infected files are disallowed for download	**High**	**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 Microsoft 365 has detected as infected to be downloaded. Defender for Microsoft 365 for SharePoint, OneDrive, and Microsoft Teams protects your Test Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-configure?view=o365-worldwide:https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection-for-spo-odfb-teams-about?view=o365-worldwide:https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#global-reader Default Value: FALSE

Block OneDrive for Business sync from unmanaged devices	**High**	**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. Test Reference: https://learn.microsoft.com/en-US/sharepoint/allow-syncing-only-on-specific-domains?WT.mc_id=365AdminCSH_spo:https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenantsyncclientrestriction?view=sharepoint-ps Default Value: By default there are no restrictions applied to the syncing of OneDrive. TenantRestrictionEnabled : False AllowedDomainList : {}
Ensure custom script execution is restricted on personal sites	**High**	**IMPACT:** Item does not meet all the requirements as per test. This setting controls custom script execution on OneDrive or user-created sites. Custom scripts can allow users to change the look, feel and behavior of sites and pages. Every script that runs in a SharePoint page (whether its an HTML page in a document library or a JavaScript in a Script Editor Web Part) always runs in the context of the user visiting the page and the SharePoint application. This means: - Scripts have access to everything the user has access to. - Scripts can access content across several Microsoft 365 services and even beyond with Microsoft Graph integration. The recommended state is Prevent users from running custom script on personal sites and Prevent users from running custom script on self-service created sites. Custom scripts could contain malicious instructions unknown to the user or administrator. When users are allowed to run custom script, the organization can no longer enforce governance, scope the capabilities of inserted code, block specific parts of code, or block all custom code that has been deployed. If scripting is allowed the following things cannot be audited: - What code has been inserted - Where the code has been inserted - Who inserted the code Note: Microsoft recommends using the [SharePoint Framework](https://learn.microsoft.com/en-us/sharepoint/dev/spfx/sharepoint-framework-overview) instead of custom scripts. None - this is the default behavior. **ACTION:** To remediate using the UI: 1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint 2. Select Settings.

		3. At the bottom of the page click the classic settings page hyperlink. 4. Scroll to locate the Custom Script section. On the right set the following: - Select Prevent users from running custom script on personal sites. - Select Prevent users from running custom script on self-service created sites. Test Reference: https://learn.microsoft.com/en-us/sharepoint/allow-or-prevent-custom-script:https://learn.microsoft.com/en-us/sharepoint/security-considerations-of-allowing-custom-script:https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-sposite?view=sharepoint-ps Default Value: Selected Prevent users from running custom script on personal sites Selected Prevent users from running custom script on self-service created sites
Ensure custom script execution is restricted on site collections	**NotExecuted**	**IMPACT:** Item does not meet all the requirements as per test. This setting controls custom script execution on a particulate site (previously called). Custom scripts can allow users to change the look, feel and behavior of sites and pages. Every script that runs in a SharePoint page (whether its an HTML page in a document library or a JavaScript in a Script Editor Web Part) always runs in the context of the user visiting the page and the SharePoint application. This means: - Scripts have access to everything the user has access to. - Scripts can access content across several Microsoft 365 services and even beyond with Microsoft Graph integration. The recommended state is DenyAddAndCustomizePages set to $true. Custom scripts could contain malicious instructions unknown to the user or administrator. When users are allowed to run custom script, the organization can no longer enforce governance, scope the capabilities of inserted code, block specific parts of code, or block all custom code that has been deployed. If scripting is allowed the following things cannot be audited: - What code has been inserted - Where the code has been inserted - Who inserted the code Note: Microsoft recommends using the [SharePoint Framework](https://learn.microsoft.com/en-us/sharepoint/dev/spfx/sharepoint-framework-overview) instead of custom scripts. None - this is the default behavior. **ACTION:** To remediate using PowerShell: 1. Connect to SharePoint Online using Connect-SPOService. 2. Edit the below and run for each site as needeed: Set-SPOSite -Identity <SiteUrl> -DenyAddAndCustomizePages $true Note: The property DenyAddAndCustomizePages cannot be set on the MySite host, which is displayed with a URL like https://tenant id-my.sharepoint.com/ Test Reference: https://learn.microsoft.com/en-us/sharepoint/allow-or-prevent-custom-script:https://learn.microsoft.com/en-us/sharepoint/security-considerations-of-allowing-custom-script:https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-sposite?view=sharepoint-ps

		Default Value: DenyAddAndCustomizePages $true or Enabled
Ensure SharePoint sites are not enabled for both External and User Sharing	**High**	IMPACT: SharePoint Sites are enabled for both External and User Sharing. If you have confidential information that can be shared with external users. ACTION: Recommended action is to disable SharePoint sites for both external and user sharing. Test Reference: No Link Found Default Value: No Default Value Found
External user sharing-share by email-and guest link sharing are both disabled	**Passed**	IMPACT: External User sharing - sharing by email - is disabled. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
Ensure that external users cannot share files folders and sites they do not own	**High**	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. Test Reference: No Link Found Default Value: No Default Value Found
SharePoint External Sharing is not Enabled at Global Level	Error	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
SharePoint External User Resharing is not Permitted	Error	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
SharePoint Legacy Authentication is not Enabled	Error	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: No Link Found Default Value: No Default Value Found

SharePoint Anyone Shared Links Never Expire is not configured	Error	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
SharePoint Online Modern Authentication is Enabled	Error	IMPACT: Item has met all the requirements as per test. ACTION: Test Reference: No Link Found Default Value: No Default Value Found
Ensure Sign out inactive users in SharePoint Online is Configured	**High**	**IMPACT:** Item does not meet all the requirements as per test. **Idle session sign-out lets you specify a time at which users are warned and are later signed out of Microsoft 365 after a period of browser inactivity in SharePoint and OneDrive.** **ACTION: This policy is one of several you can use with SharePoint and OneDrive to balance security and user productivity and help keep your data safe, regardless of where users access the data from, what device they're working on, and how secure their network con**nection is. Test Reference: No Link Found **Default Value: No Default Value Found**

8.7 Microsoft Teams Admin Center

Test	Status	Remark
Ensure external file sharing in Teams is enabled for only approved cloud storage services	**High**	**IMPACT:** External File Sharing in Teams is enabled. The 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:** Microsoft Teams enables collaboration via file sharing. This file sharing is conducted within Teams, using SharePoint Online, by default; however, third-party cloud services are allowed as well. Ensuring that only authorized cloud storage providers are accessible from Teams will help to dissuade the use of non-approved storage providers. Test Reference: https://learn.microsoft.com/en-us/microsoft-365/enterprise/manage-skype-for-business-online-with-microsoft-365-powershell?view=o365-worldwide Default Value: AllowDropBox : True AllowBox : True AllowGoogleDrive : True AllowShareFile : True

		AllowEgnyte : True
Ensure users cant send emails to a channel email address	**NotExecuted**	**IMPACT:** Item does not meet all the requirements as per test. Teams channel email addresses are an optional feature that allows users to email the Teams channel directly. Channel email addresses are not under the tenants domain and organizations do not have control over the security settings for this email address. An attacker could email channels directly if they discover the channel email address. Users will not be able to email the channel directly. **ACTION:** To remediate using the UI: 1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com. 2. Click to expand Teams select Teams settings. 3. Under email integration set Users can send emails to a channel email address to Off. To remediate using PowerShell: 1. Connect to Teams PowerShell using Connect-MicrosoftTeams. 2. Run the following command to set the recommended state: Set-CsTeamsClientConfiguration -Identity Global -AllowEmailIntoChannel $false Test Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/step-by-step-guides/reducing-attack-surface-in-microsoft-teams?view=o365-worldwide#restricting-channel-email-messages-to-approved-domains:https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsclientconfiguration?view=skype-ps Default Value: On (True)
Ensure End-to-end encryption for Microsoft Teams is enabled	**High**	**IMPACT:** End-To-End encryption is not enabled for Teams Calling. In recent times, Microsoft Teams has emerged as the ultimate workspace for real-time collaboration and communication. Since most of the business communication is carried out by MS teams, security has become a concern. By default, Teams calls over VOIP are encrypted using Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP). However, these protocols allow admins to configure automatic recording and transcription of calls. **ACTION:** It is recommended to enable end-to-end calling encryption enabled for Teams calls. Test Reference: No Link Found Default Value: No Default Value Found
Ensure external domains are not allowed in Teams	**High**	**IMPACT:** External Domains are not allowed in Teams is not configured. The 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. Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft Teams External Domain Communication Policies are configured	**Medium**	**IMPACT:** Item does not meet all the requirements as per test. Microsoft Teams External Domain Communication Policies. **ACTION:** Review Microsoft Teams External Access Policies and validate that all results are expected, and no conflicting rules are in place. Test Reference: https //docs.microsoft.com/en-us/microsoftteams/communicate-with-users-from-other-organizations Default Value: No Default Value Found
Ensure Microsoft Teams Users Allowed to Invite Anonymous Users is disabled	**High**	**IMPACT:** Item does not meet all the requirements as per test. Microsoft Teams by default enables and allows anonymous users to join Teams meetings. This finding returns the users within the Tenant that have the ability to invite anonymous users into the Teams environment. Some organizations may wish to disable this functionality, or restrict certain users, members, or roles from allowing anonymous users to join meetings. Changing these settings may have unintended consequences. Speak with shareholders and understand what functionality may be affected before disabling this access. **ACTION:** This can be mitigated by navigating to the Teams admin center and turning off 'Anonymous users can join a meeting' under Meeting settings. This disables anonymous access globally. Alternatively, specific users and groups can be targeted by creating a new Meeting Policy and issuing the listed command in PowerShell. Test Reference: https //docs.microsoft.com/en-us/skypeforbusiness/set-up-policies-in-your-organization/block-point-to-point-file-transfers Default Value: No Default Value Found
Ensure Microsoft Teams Policies Allow Anonymous Members is disabled	**High**	**IMPACT:** Item does not meet all the requirements as per test. Microsoft Teams by default enables and allows authenticated users to invite anonymous users to join Teams meetings. Some organizations may wish to disable this functionality, or restrict certain users, members, or roles from allowing anonymous users to join meetings. Changing these settings may have unintended consequences. Speak with shareholders and understand what functionality may be affected before disabling this access. **ACTION:** This can be mitigated by navigating to the Teams admin center and turning off 'Anonymous users can join a meeting' under Meeting settings. This disables anonymous access globally. Alternatively, specific users and groups can be targeted by creating a new Meeting Policy and issuing the listed command in PowerShell.

		Test Reference: https //docs.microsoft.com/en-us/skypeforbusiness/set-up-policies-in-your-organization/block-point-to-point-file-transfers Default Value: No Default Value Found
Ensure Microsoft Teams Consumer Communication Policies are configured	**High**	**IMPACT:** Item does not meet all the requirements as per test. Microsoft Teams External Access Policies allow communication with Teams users not managed by an organization. **ACTION:** Review Microsoft Teams External Access Policies and validate that all results are expected, and no conflicting rules are in place. Test Reference: https //docs.microsoft.com/en-us/microsoftteams/communicate-with-users-from-other-organizations Default Value: No Default Value Found
Ensure Microsoft Teams External Access Policies are configured	**Low**	**IMPACT:** Item does not meet all the requirements as per test. Microsoft Teams External Access Policies. **ACTION:** Review Microsoft Teams External Access Policies and validate that all results are expected, and no conflicting rules are in place. Test Reference: https //docs.microsoft.com/en-us/microsoftteams/communicate-with-users-from-other-organizations Default Value: No Default Value Found
Ensure Microsoft Teams Users Allowed to Preview Links in Messages is disabled	**High**	**IMPACT:** Item does not meet all the requirements as per test. Microsoft Teams by default enables and allows users to preview links in messages. Some organizations may wish to disable this functionality. Changing these settings may have unintended consequences. Speak with stakeholders and understand what functionality may be affected before disabling this access. **ACTION:** This can be mitigated by navigating to the Teams admin center and turning off 'Allow URL Previews' under Messaging settings. This disables link previews globally. Alternatively, specific users and groups can be targeted by creating a new Messaging Policy and issuing the listed command in PowerShell. Test Reference: https //positive.security/blog/ms-teams-1-feature-4-vulns Default Value: No Default Value Found
Ensure Safe Links for Teams is Enabled	**High**	**IMPACT:** Item does not meet all the requirements as per test. Safe Links is a feature of O365 that enables real-time detection of malicious links in incoming Exchange emails and other Office 365 applications. The Safe Links feature can also be enabled for links shared via Microsoft Teams. However, this setting is disabled in the 365 instance. Enabling it can decrease the risk of phishing and other attacks that might utilize malicious links sent via Teams, although it is not a panacea for these attacks. **ACTION:** Perhaps the most convenient way to enable this feature is to use the Set-SafeLinksPolicy command in PowerShell as listed below. Note that some organizations may have chosen to disable Safe Links for Teams if it interferes with day-to-day operations, so key stakeholders should be surveyed before enabling Safe Links for Teams.

		Test Reference: https //www.microsoft.com/en-us/microsoft-365/roadmap?rtc=2&filters=&searchterms=Safe%2CLinks%2CProtection%2Cfor%2CMicrosoft%2CTeams Default Value: No Default Value Found
Ensure external access is restricted in the Teams admin center	**NotExecuted**	**IMPACT:** Item does not meet all the requirements as per test. This policy setting controls chat with external unmanaged Skype and Teams users. Users in the organization will not be searchable by unmanaged Skype or Teams users and will have to initiate all communications with unmanaged users. Note: As of December 2021, the default for Teams external communication is set to People in my organization can communicate with Teams users whose accounts are not managed by an organization. Note #2: Skype for business is deprecated as of July 31, 2021, although these settings may still be valid for a period of time. See the link in the reference section for more information. Allowing users to communicate with Skype or Teams users outside of an organization presents a potential security threat as external users can interact with organization users over Skype for Business or Teams. While legitimate, productivity-improving scenarios exist, they are outweighed by the risk of data loss, phishing, and social engineering attacks against organization users via Teams. Therefore, it is recommended to restrict external communications in order to minimize the risk of security incidents. The impact of disabling external access to Teams and Skype for an organization is highly dependent on current usage practices. If users infrequently communicate with external parties using these channels, the impact is likely to be minimal. However, if users regularly use Teams and Skype for client communication, the impact could be significant. Therefore, before disabling external access, users should be notified, and alternate communication mechanisms should be identified to ensure continuity of communication. Note: Chat with external unmanaged Teams users is not available in GCC, GCC High, or DOD deployments, or in private cloud environments. **ACTION:** To remediate using the UI: 1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com/. 2. Click to expand Users select External access. 3. Under Teams and Skype for Business users in external organizations Select Block all external domains - NOTE: If the organizations policy allows selecting any allowed external domains. 4. Under Teams accounts not managed by an organization move the slider to Off. 5. Under Skype users move the slider is to Off. 6. Click Save. To remediate using PowerShell: - Connect to Teams PowerShell using Connect-MicrosoftTeams - Run the following command: Set-CsTenantFederationConfiguration -AllowTeamsConsumer False -AllowPublicUsers False -AllowFederatedUsers $false

		- To allow only specific external domains run these commands replacing the example domains with approved domains: Set-CsTenantFederationConfiguration -AllowTeamsConsumer $false -AllowPublicUsers $false -AllowFederatedUsers $true $list = New-Object Collections.Generic.List[String] $list.add() $list.add() Set-CsTenantFederationConfiguration -AllowedDomainsAsAList $list Test Reference: https://learn.microsoft.com/en-us/skypeforbusiness/set-up-skype-for-business-online/set-up-skype-for-business-online:https://learn.microsoft.com/en-US/microsoftteams/manage-external-access?WT.mc_id=TeamsAdminCenterCSH Default Value: - AllowTeamsConsumer : True - AllowPublicUsers : True - AllowFederatedUsers : True - AllowedDomains : AllowAllKnownDomains
Ensure app permission policies are configured	**High**	**IMPACT:** Item does not meet all the requirements as per test. This policy setting controls which class of apps are available for users to install. Allowing users to install third-party or unverified apps poses a potential risk of introducing malicious software to the environment. Users will only be able to install approved classes of apps. **ACTION:** To set app permission policies: 1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com. 2. Click to expand Teams apps select Permission policies. 3. Click Global (Org-wide default). 4. For Microsoft apps set app permission policies to Allow all apps. 5. For Third-party apps set app permission policies to Block all apps OR Allow specific apps and block all others. 6. For Custom apps set app permission policies to Block all apps OR Allow specific apps and block all others. Test Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/step-by-step-guides/reducing-attack-surface-in-microsoft-teams?view=o365-worldwide#disabling-third-party--custom-apps:https://learn.microsoft.com/en-us/microsoftteams/teams-app-permission-policies Default Value: Microsoft apps: Allow all apps Third-party apps: Allow all apps Custom apps: Allow all apps
Ensure anonymous users cant join a meeting	**NotExecuted**	**IMPACT:** Item does not meet all the requirements as per test. This policy setting can prevent anyone other than invited attendees (people directly invited by the organizer, or to whom an invitation was forwarded) from bypassing the lobby and entering the meeting. For more information on how to setup a sensitive meeting, please visit: [Configure Teams meetings with protection for sensitive data - Microsoft Teams | Microsoft

		Learn] (https://learn.microsoft.com/en-us/MicrosoftTeams/configure-meetings-sensitive-protection) For meetings that could contain sensitive information, it is best to allow the meeting organizer to vet anyone not directly sent an invite before admitting them to the meeting. This will also prevent the anonymous user from using the meeting link to have meetings at unscheduled times. Note: Those companies that don't normally operate at a Level 2 environment, but do deal with sensitive information, may want to consider this policy setting. Individuals who were not sent or forwarded a meeting invite will not be able to join the meeting automatically. **ACTION:** To remediate using the UI: 1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com. 2. Click to expand Meetings select Meeting policies. 3. Click Global (Org-wide default) 3. Under meeting join & lobby set Anonymous users can join a meeting to Off. To remediate using PowerShell: 1. Connect to Teams PowerShell using Connect-MicrosoftTeams 2. Run the following command to set the recommended state: Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToJoinMeeting $false Test Reference: https://learn.microsoft.com/en-us/MicrosoftTeams/configure-meetings-sensitive-protection Default Value: On (True)
Ensure anonymous users and dial-in callers cant start a meeting	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. This policy setting controls if an anonymous participant can start a Microsoft Teams meeting without someone in attendance. Anonymous users and dial-in callers must wait in the lobby until the meeting is started by someone in the organization or an external user from a trusted organization. Anonymous participants are classified as: - Participants who are not logged in to Teams with a work or school account. - Participants from non-trusted organizations (as configured in external access). - Participants from organizations where there is not mutual trust. Note: This setting only applies when Who can bypass the lobby is set to Everyone. If the anonymous users can join a meeting organization-level setting or meeting policy is Off, this setting only applies to dial-in callers. Not allowing anonymous participants to automatically join a meeting reduces the risk of meeting spamming. Anonymous participants will not be able to start a Microsoft Teams meeting. ACTION: To remediate using the UI: 1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com. 2. Click to expand Meetings select Meeting policies.

		3. Click Global (Org-wide default). 3. Under meeting join & lobby set Anonymous users and dial-in callers can start a meeting to Off. To remediate using PowerShell: 1. Connect to Teams PowerShell using Connect-MicrosoftTeams. 2. Run the following command to set the recommended state: Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToStartMeeting $false Test Reference: https://learn.microsoft.com/en-us/microsoftteams/anonymous-users-in-meetings:https://learn.microsoft.com/en-US/microsoftteams/who-can-bypass-meeting-lobby?WT.mc_id=TeamsAdminCenterCSH#overview-of-lobby-settings-and-policies Default Value: Off (False)
Ensure only people in my org can bypass the lobby	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. This policy setting controls who can join a meeting directly and who must wait in the lobby until they are admitted by an organizer, co-organizer, or presenter of the meeting. For meetings that could contain sensitive information, it is best to allow the meeting organizer to vet anyone not directly sent an invite before admitting them to the meeting. This will also prevent the anonymous user from using the meeting link to have meetings at unscheduled times. Individuals who were not part of the organization will have to wait in the lobby until they are admitted by an organizer, co-organizer, or presenter of the meeting. ACTION: To remediate using the UI: 1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com. 2. Click to expand Meetings select Meeting policies. 3. Click Global (Org-wide default). 3. Under meeting join & lobby set Who can bypass the lobby to People in my org. To remediate using PowerShell: 1. Connect to Teams PowerShell using Connect-MicrosoftTeams. 2. Run the following command to set the recommended state: Set-CsTeamsMeetingPolicy -Identity Global -AutoAdmittedUsers Test Reference: https://learn.microsoft.com/en-US/microsoftteams/who-can-bypass-meeting-lobby?WT.mc_id=TeamsAdminCenterCSH:https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps Default Value: People in my org and guests (EveryoneInCompany)
Ensure users dialing in cant bypass the lobby	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. This policy setting controls if users who dial in by phone can join the meeting directly or must wait in the lobby. Admittance to the meeting from the lobby is authorized by the meeting organizer, co-organizer, or presenter of the meeting.

		For meetings that could contain sensitive information, it is best to allow the meeting organizer to vet anyone not directly from the organization. Individuals who are dialing in to the meeting must wait in the lobby until a meeting organizer, co-organizer, or presenter admits them. ACTION: To remediate using the UI: 1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com. 2. Click to expand Meetings select Meeting policies. 3. Click Global (Org-wide default). 3. Under meeting join & lobby set People dialing in can not bypass the lobby to Off. To remediate using PowerShell: 1. Connect to Teams PowerShell using Connect-MicrosoftTeams. 2. Run the following command to set the recommended state: Set-CsTeamsMeetingPolicy -Identity Global -AllowPSTNUsersToBypassLobby $false Test Reference: https://learn.microsoft.com/en-US/microsoftteams/who-can-bypass-meeting-lobby?WT.mc_id=TeamsAdminCenterCSH#choose-who-can-bypass-the-lobby-in-meetings-hosted-by-your-organization:https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps Default Value: Off (False)
Ensure meeting chat does not allow anonymous users	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. This policy setting controls who has access to read and write chat messages during a meeting. Ensuring that only authorized individuals can read and write chat messages during a meeting reduces the risk that a malicious user can inadvertently show content that is not appropriate or view sensitive information. Only authorized individuals will be able to read and write chat messages during a meeting. ACTION: To remediate using the UI: 1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com. 2. Click to expand Meetings select Meeting policies. 3. Click Global (Org-wide default). 3. Under meeting engagement set Meeting chat to On for everyone but anonymous users. To remediate using PowerShell: 1. Connect to Teams PowerShell using Connect-MicrosoftTeams. 2. Run the following command to set the recommended state: Set-CsTeamsMeetingPolicy -Identity Global -MeetingChatEnabledType Test Reference: https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps#-meetingchatenabledtype

		Default Value: On for everyone (Enabled)
Ensure only organizers and co-organizers can present	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. This policy setting controls who can present in a Teams meeting. Note: Organizers and co-organizers can change this setting when the meeting is set up. Ensuring that only authorized individuals are able to present reduces the risk that a malicious user can inadvertently show content that is not appropriate. Only organizers and co-organizers will be able to present without being granted permission. ACTION: To remediate using the UI: 1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com. 2. Click to expand Meetings select Meeting policies. 3. Click Global (Org-wide default). 3. Under content sharing set Who can present to Only organizers and co-organizers. To remediate using PowerShell: 1. Connect to Teams PowerShell using Connect-MicrosoftTeams. 2. Run the following command to set the recommended state: Set-CsTeamsMeetingPolicy -Identity Global -DesignatedPresenterRoleMode Test Reference: https://learn.microsoft.com/en-US/microsoftteams/meeting-who-present-request-control:https://learn.microsoft.com/en-us/microsoftteams/meeting-who-present-request-control#manage-who-can-present:https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/step-by-step-guides/reducing-attack-surface-in-microsoft-teams?view=o365-worldwide#configure-meeting-settings-restrict-presenters:https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps Default Value: Everyone (EveryoneUserOverride)
Ensure external participants cant give or request control	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. This policy setting allows control of who can present in meetings and who can request control of the presentation while a meeting is underway. Ensuring that only authorized individuals and not external participants are able to present and request control reduces the risk that a malicious user can inadvertently show content that is not appropriate. External participants are categorized as follows: external users, guests, and anonymous users. External participants will not be able to present or request control during the meeting. Warning: This setting also affects webinars. Note: At this time, to give and take control of shared content during a meeting, both parties must be using the Teams desktop client. Control is not supported when either party is running Teams in a browser.

		ACTION: To remediate using the UI: 1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com. 2. Click to expand Meetings select Meeting policies. 3. Click Global (Org-wide default). 3. Under content sharing set External participants can give or request control to Off. To remediate using PowerShell: 1. Connect to Teams PowerShell using Connect-MicrosoftTeams. 2. Run the following command to set the recommended state: Set-CsTeamsMeetingPolicy -Identity Global -AllowExternalParticipantGiveRequestControl $false Test Reference: https://learn.microsoft.com/en-us/microsoftteams/meeting-who-present-request-control:https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps Default Value: Off (False)
Ensure users can report security concerns in Teams	**NotExecuted**	IMPACT: Item does not meet all the requirements as per test. User reporting settings allow a user to report a message as malicious for further analysis. This recommendation is composed of 3 different settings and all be configured to pass: **- In the Teams admin c**enter: On by default and controls whether users are able to report messages from Teams. When this setting is turned off, users can not report messages within Teams, so the corresponding setting in the Microsoft 365 Defender portal is irrelevant. **- In the Microsoft 365 Defender portal: On by default for new tenants. Existing tenants need to enable it. If user reporting of messages is turned on in the Teams admin center, it also needs to be turned on the Defender portal for user reported messages to show u**p correctly on the User reported tab on the Submissions page. **- Defender - Report message destinations: This applies to more than just Microsoft Teams and allows for an organization to keep their reports contained. Due to how the parameters are configure**d on the backend it is included in this assessment as a requirement. **Users will be able to more quickly and systematically alert administrators of suspicious malicious messages within Teams. The content of these messages may be sensitive in nature and the**refore should be kept within the organization and not shared with Microsoft without first consulting company policy. Note: - The reported message remains visible to the user in the Teams client. - Users can report the same message multiple times. **- The** message sender is not notified that messages were reported. **Enabling message reporting has an impact beyond just addressing security concerns. When users of the platform report a message, the content could include messages that are threatening or harassin**g in nature, possibly stemming from colleagues.

Due to this the security staff responsible for reviewing and acting on these reports should be equipped with the skills to discern and appropriately direct such messages to the relevant departments, such as Human Resources (HR).

ACTION: To remediate using the UI:

1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com.
2. Click to expand Messaging select Messaging policies.
3. Click Global (Org-wide default).
4. Set Report a security concern to On.
5. Next, navigate to Microsoft 365 Defender https://security.microsoft.com/
6. Click on Settings > Email & collaboration > User reported settings.
7. Scroll to Microsoft Teams.
8. Check Monitor reported messages in Microsoft Teams and Save.
9. Set Send reported messages to: to My reporting mailbox only with reports configured to be sent to authorized staff.

To remediate using PowerShell:

1. Connect to Teams PowerShell using Connect-MicrosoftTeams.
2. Connect to Exchange Online PowerShell using Connect-ExchangeOnline.
3. Run the following cmdlet:

```
Set-CsTeamsMessagingPolicy -Identity Global -AllowSecurityEndUserReporting $true
```

4. To configure the Defender reporting policies, edit and run this script:

```
$usersub =  # Change this.

$params = @{
 Identity =
 EnableReportToMicrosoft = $false
 ReportChatMessageEnabled = $false
 ReportChatMessageToCustomizedAddressEnabled = $true
 ReportJunkToCustomizedAddress = $true
 ReportNotJunkToCustomizedAddress = $true
 ReportPhishToCustomizedAddress = $true
 ReportJunkAddresses = $usersub
 ReportNotJunkAddresses = $usersub
 ReportPhishAddresses = $usersub
}

Set-ReportSubmissionPolicy @params

New-ReportSubmissionRule -Name DefaultReportSubmissionRule -
ReportSubmissionPolicy DefaultReportSubmissionPolicy -SentTo $usersub
```

Test Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/submissions-teams?view=o365-worldwide
Default Value: On (True)

Report message destination: Microsoft Only

8.8 Microsoft Fabric-Tenant Settings

Test	Status	Remark

8.9 Microsoft M365 Users

Test	Status	Remark
Ensure All Microsoft 365 Users are licensed	Medium	**IMPACT:** Some Microsoft 365 Users are not licensed. Unlicensed users will not be able to use Microsoft 365 Services. **ACTION:** It is recommended to assign Licenses to users. Test Reference: No Link Found Default Value: No Default Value Found
Ensure Deleted Microsoft 365 Users are Identified	Passed	**IMPACT:** No users were found in Microsoft 365 Recycle Bin. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Disabled Microsoft 365 Users are Identified	Passed	**IMPACT:** No users are disabled. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Users have no Reconciliation Errors	Passed	**IMPACT:** No users require License Reconciliation **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Users Password Expires	Passed	**IMPACT:** No users passwords are set to NOT expire. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Users are Syncing and No Sync Errors	Passed	**IMPACT:** All Microsoft 365 Users have been syncing.asdasd **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found

Ensure no Provisioning Errors for Microsoft 365 Users	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Blocked Users are Identified	**Passed**	**IMPACT:** No Blocked Users were found in Microsoft 365. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Users Have Changed Passwords	**High**	**IMPACT:** Some Microsoft 365 users have not changed their passwords within 90 days. It is a security risk. Every user in Microsoft 365 Users must change their passwords within 90 days. **ACTION:** Please identify these users and make sure they change their passwords. Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Company Administrators have less than 5 Admins	**Passed**	**IMPACT:** There are lesser than five company administrators in Microsoft 365. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Deleted and Licensed Users are Identified	**Passed**	**IMPACT:** Item has met all the requirements as per test. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Groups Without Members are Identified	**Low**	**IMPACT:** Some Microsoft 365 Groups do not contain user members. **If these Groups were created for some reason, then they should have members in it.** **ACTION:** Please review the list of Groups provided by the test and add users or remove these groups. Test Reference: No Link Found **Default Value: No Default Value Found**

8.10Microsoft Mobile Device Management

Test	Status	Remark
Ensure mobile device management policies are set to require advanced security configurations for Android Devices	High	**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. Test Reference: No Link Found Default Value: No Default Value Found
Ensure mobile device management policies are set to require advanced security configurations for iOS Devices	High	**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. Test Reference: No Link Found Default Value: No Default Value Found
Ensure that mobile device password reuse is prohibited for Android Devices	High	**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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure that mobile device password reuse is prohibited for iOS Devices	High	**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.

		Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure that mobile devices are set to never expire passwords for Android Devices	**High**	**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 strong password: long, complex and without any pragmatic words present, it should remain just as strong is 60 days as it is today. It is Microsoft's official security position to not expire passwords periodically without a specific reason. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure that mobile devices are set to never expire passwords for iOS Devices	**High**	**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 strong password: long, complex and without any pragmatic words present, it should remain just as strong is 60 days as it is today. It is Microsoft's official security position to not expire passwords periodically without a specific reason. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure that users cannot connect from devices that are jail broken or rooted	**High**	**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 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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise for Android Devices	**High**	**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.

		Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise for iOS Devices	**High**	**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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure that mobile devices require a minimum password length to prevent brute force attacks for Android Devices	**High**	**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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure that mobile devices require a minimum password length to prevent brute force attacks for iOS Devices	**High**	**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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure devices lock after a period of inactivity to prevent unauthorized access for Android Devices	**High**	**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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found

Ensure devices lock after a period of inactivity to prevent unauthorized access for iOS Devices	**High**	**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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data for Android Devices	**High**	**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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data for iOS Devices	**High**	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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure that mobile devices require complex passwords (Type = Alphanumeric) for Android Devices	**High**	IMPACT: Ensure that mobile devices require complex passwords (Type = Alphanumeric) is not configured. This setting will have a moderate user impact. ACTION: You should require your users to use a complex password with at least two-character sets (letters and numbers, for example) to unlock their mobile devices. 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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure that mobile devices require complex passwords (Type = Alphanumeric) for iOS Devices	**High**	IMPACT: Ensure that mobile devices require complex passwords (Type = Alphanumeric) is not configured. This setting will have a moderate user impact. ACTION: You should require your users to use a complex password with at least two-character sets (letters and numbers, for example) to unlock their mobile devices. 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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure that mobile devices require complex passwords (Simple Passwords = Blocked) for iOS Devices	**High**	IMPACT: Ensure that mobile devices require complex passwords (Simple Passwords = Blocked) is not configured. This has a moderate impact on users. ACTION: You should require your users to use a complex password to unlock their mobile devices. 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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure that devices connecting have AV and a local firewall enabled	**High**	IMPACT: Ensure that devices connecting have AV and a local firewall enabled is not configured. Impact should be minimal however, in the event that a device is not running appropriate protection it will be blocked from connecting. ACTION: You should configure your mobile device management policies to require the PC to have anti-virus and have a firewall enabled. If you do not require this, users will be able to connect from devices that are vulnerable. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure mobile device management policies are required for email profiles	**High**	IMPACT: Ensure mobile device management policies are required for email profiles is not configured. This setting will have a moderate impact on users. ACTION: You should configure your mobile device management policies to require the policy to manage the email profile of the user. If you do not require this, users will be able to set up and configure email accounts. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies Default Value: No Default Value Found
Ensure mobile devices require the use of a password for Android Devices	**High**	IMPACT: Ensure mobile devices require the use of a password is not configured. This change will require users to provide a password to unlock their mobile device after the timeout period expires. ACTION: You should require your users to use a password to unlock their mobile devices. 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. Test Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies

		Default Value: No Default Value Found
Ensure mobile devices require the use of a password for iOS Devices	High	**IMPACT:** Ensure mobile devices require the use of a password is not configured. **This change will require users to provide a password to unlock their mobile device after the timeout period expires.** **ACTION:** You should require your users to use a password to unlock their mobile devices. 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. **Test** Reference: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/exchange-activesync/mobile-device-mailbox-policies **Default Value: No Default Value Found**

8.11 Microsoft M365 Dangerous Defaults

Test	Status	Remark
Ensure Users can read all attributes in Azure AD is disabled	Medium	**IMPACT:** Item does not meet all the requirements as per test. Dangerous default configuration settings were found in the Tenant. By default, Azure tenants allow all users to access the Azure Active Directory blade, to read all other users' accounts, create groups, and invite guests. These default settings extend to guest accounts as well, allowing guests to perform these same actions. Other default configurations allow for Self-Service creation of accounts from accepted mail domains. **ACTION:** The excessive user permissions can be mitigated by running the listed PowerShell commands as a Global Admin. User access to the Azure AD blade can be restricted by navigating to the Azure Active Directory blade; User Settings and toggling the 'Restrict access to Azure AD administration portal' to Yes. Guest invites may be restricted by navigating to the Azure Active Directory blade; External Identities; External Collaboration Settings, or by going to the Azure Active Directory blade; User Settings; Manage external collaboration settings and toggling 'Members can invite' and 'Guests can invite' to No. Test Reference: https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions Default Value: No Default Value Found
Ensure Users can create security groups is disabled	High	**IMPACT:** Item does not meet all the requirements as per test. Dangerous default configuration settings were found in the Tenant. By default, Azure tenants allow all users to access the Azure Active Directory blade, to read all other users' accounts, create groups, and invite guests. These default settings extend to guest accounts as well, allowing guests to perform these same actions. Other default configurations allow for Self-Service creation of accounts from accepted mail domains. **ACTION:** The excessive user permissions can be mitigated by running the listed PowerShell commands as a Global Admin. User access to the Azure AD blade can be restricted by navigating to the Azure Active Directory blade; User Settings and toggling the 'Restrict access to Azure AD administration portal' to Yes. Guest invites may be restricted by navigating to the Azure Active Directory blade; External Identities; External Collaboration Settings, or by going to the Azure Active Directory blade; User Settings; Manage external collaboration settings and toggling 'Members can invite' and 'Guests can invite' to No. Test Reference: https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions

		Default Value: No Default Value Found
Ensure Users are allowed to create and register applications is disabled	**High**	**IMPACT:** Item does not meet all the requirements as per test. Dangerous default configuration settings were found in the Tenant. By default, Azure tenants allow all users to access the Azure Active Directory blade, to read all other users' accounts, create groups, and invite guests. These default settings extend to guest accounts as well, allowing guests to perform these same actions. Other default configurations allow for Self-Service creation of accounts from accepted mail domains. **ACTION:** The excessive user permissions can be mitigated by running the listed PowerShell commands as a Global Admin. User access to the Azure AD blade can be restricted by navigating to the Azure Active Directory blade; User Settings and toggling the 'Restrict access to Azure AD administration portal' to Yes. Guest invites may be restricted by navigating to the Azure Active Directory blade; External Identities; External Collaboration Settings, or by going to the Azure Active Directory blade; User Settings; Manage external collaboration settings and toggling 'Members can invite' and 'Guests can invite' to No. Test Reference: https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions Default Value: No Default Value Found
Ensure Users with a verified mail domain can join the tenant is disabled	**High**	**IMPACT:** Item does not meet all the requirements as per test. Dangerous default configuration settings were found in the Tenant. By default, Azure tenants allow all users to access the Azure Active Directory blade, to read all other users' accounts, create groups, and invite guests. These default settings extend to guest accounts as well, allowing guests to perform these same actions. Other default configurations allow for Self-Service creation of accounts from accepted mail domains. **ACTION:** The excessive user permissions can be mitigated by running the listed PowerShell commands as a Global Admin. User access to the Azure AD blade can be restricted by navigating to the Azure Active Directory blade; User Settings and toggling the 'Restrict access to Azure AD administration portal' to Yes. Guest invites may be restricted by navigating to the Azure Active Directory blade; External Identities; External Collaboration Settings, or by going to the Azure Active Directory blade; User Settings; Manage external collaboration settings and toggling 'Members can invite' and 'Guests can invite' to No. Test Reference: https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions Default Value: No Default Value Found
Ensure Guests can invite other guests into the tenant is disabled	**High**	**IMPACT:** Item does not meet all the requirements as per test. Dangerous default configuration settings were found in the Tenant. By default, Azure tenants allow all users to access the Azure Active Directory blade, to read all other users' accounts, create groups, and invite guests. These default settings extend to guest accounts as well, allowing guests to perform these same actions. Other default configurations allow for Self-Service creation of accounts from accepted mail domains. **ACTION:** The excessive user permissions can be mitigated by running the listed PowerShell commands as a Global Admin. User access to the Azure AD blade can be restricted by navigating to the Azure Active Directory blade; User Settings and toggling the 'Restrict access to Azure AD administration portal' to Yes. Guest invites may be restricted by navigating to the Azure Active Directory blade; External Identities; External Collaboration Settings, or by going to the Azure Active Directory blade; User Settings; Manage external collaboration settings and toggling 'Members can invite' and 'Guests can invite' to No.

		Test Reference: https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions Default Value: No Default Value Found
Ensure Users are allowed to create new Azure Active Directory Tenants is disabled	**High**	**IMPACT:** Item does not meet all the requirements as per test. Dangerous default configuration settings were found in the Tenant. By default, Azure tenants allow all users to access the Azure Active Directory blade, to read all other users' accounts, create groups, and invite guests. These default settings extend to guest accounts as well, allowing guests to perform these same actions. Other default configurations allow for Self-Service creation of accounts from accepted mail domains. **ACTION:** The excessive user permissions can be mitigated by running the listed PowerShell commands as a Global Admin. User access to the Azure AD blade can be restricted by navigating to the Azure Active Directory blade; User Settings and toggling the 'Restrict access to Azure AD administration portal' to Yes. Guest invites may be restricted by navigating to the Azure Active Directory blade; External Identities; External Collaboration Settings, or by going to the Azure Active Directory blade; User Settings; Manage external collaboration settings and toggling 'Members can invite' and 'Guests can invite' to No. Test Reference: https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions Default Value: No Default Value Found
Ensure Policy exists to restrict non-administrator access to Azure Active Directory or Entra	**High**	**IMPACT:** Item does not meet all the requirements as per test. Restrict non-privileged users from signing into the Azure Active Directory portal. **Note: This recommendation only affects access to the Azure AD web portal. It does not prevent privileged users from us**ing other methods such as Rest API or PowerShell to obtain information. Those channels are addressed elsewhere in this document. **The Azure AD administrative (AAD) portal contains sensitive data and permission settings, which are still enforced based on the users role. However, an end user may inadvertently change properties or account settings that could result in increased administrative overhead. Additionally, a compromised end user account could be used by a malicious attacker as a means to gather addi**tional information and escalate an attack. **Note: Users will still be able to sign into Azure Active directory admin center but will be unable to see directory information.** **ACTION:** Ensure access to the Azure AD portal is restricted: 1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/ 2. Click to expand Identity> Users > User settings. **3. Set Restrict access to Microsoft Entra ID administration portal to Yes the**n Save. Test Reference: https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions **Default Value: No Default Value Found**

8.12Microsoft M365 Configuration

Test	Status	Remark

Ensure Microsoft 365 Licenses are consumed in SKUs	**High**	**IMPACT:** Some SKUs are not being used in Microsoft 365. Microsoft 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. Test Reference: No Link Found Default Value: No Default Value Found
Ensure All Microsoft 365 Domains Have been verified	**Passed**	**IMPACT:** All Microsoft 365 domains have been verified. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Domain Services Have Services Assigned	**Passed**	**IMPACT:** Microsoft 365 Domains have Services assigned. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Notification Email is configured	**Passed**	**IMPACT:** Technical Notification Emails are configured. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Organization Level Mailbox Auditing is configured	**Passed**	**IMPACT:** Auditing is enabled for Organization. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Dir Sync Feature is Configured	**Medium**	**IMPACT:** Microsoft 365 Dir Sync is not enabled. If you have Federated Identity configured, then Synchronization must be enabled. **ACTION:** Please review Dir Sync configuration. Test Reference: No Link Found Default Value: No Default Value Found
Ensure Microsoft 365 Dir Sync Features Are Used	**Low**	**IMPACT:** Some Dir Sync features are not enabled. Some Dir Sync Features are required to meet the compliance. **ACTION:** Please review the features list and make sure to enable the required features.

	[redacted]	Test Reference: No Link Found Default Value: No Default Value Found
Ensure No Microsoft 365 Dir Sync Property Conflicts	**Passed**	**IMPACT:** There are no property conflict objects. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure No Microsoft 365 Dir Sync Property Conflict with User Principal Name	**Passed**	**IMPACT:** There are no property conflict objects for User Principal Names. **ACTION:** Test Reference: No Link Found Default Value: No Default Value Found
Ensure No Microsoft 365 Dir Sync Property Conflict with ProxyAddress	**Passed**	**IMPACT: There are no property conflict objects for User Principal Names.** **ACTION:** Test Reference: No Link Found **Default Value: No Default Value Found**

APPENDIX-1: Passed/Completed

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

Category	Test	Status	Finding
M365 Admin Center-Users	Ensure Administrative accounts are separate and cloud-only	**Passed**	Sync-In Admins: 0
M365 Admin Center-Users	Ensure that between two and four global admins are designated	**Passed**	Total Global Admins: 4
M365 Admin Center-Accounts and Authentication	Ensure Microsoft 365 User Roles have less than 10 Admins	**Passed**	More than 10 Admins: 0
M365 Admin Center-Accounts and Authentication	Ensure Microsoft 365 Users Have Strong Password Requirements Configured	**Passed**	Users With Weak Password Requirements: 0
M365 Admin Center-Accounts and Authentication	Ensure self-service password reset is enabled	**Passed**	Status: Enabled

M365 Admin Center-Accounts and Authentication	Ensure that Microsoft 365 Passwords Are Not Set to Expire	**Passed**	Missing Password Policies Domains: 0
M365 Admin Center-Accounts and Authentication	Ensure Microsoft 365 Exchange Online Modern Authentication is Used	**Passed**	Status: Enabled
M365 Admin Center-Settings	Ensure the Password expiration policy is set to Set passwords to never expire (recommended)	**Passed**	Missing Password Policies Domains: 0
Microsoft 365 Defender-Email and Collaboration	Ensure Safe Attachments policy is enabled	**Passed**	Status: Not Enabled-Not Implemented
Microsoft 365 Defender-Email and Collaboration	Ensure that an anti-phishing policy has been created	**Passed**	Status: Created
Microsoft 365 Defender-Email and Collaboration	Ensure No Domains with SPF Soft Fail are Configured	**Passed**	Status: Not Configured
Microsoft 365 Defender-Email and Collaboration	Ensure the Restricted entities report is reviewed weekly	**Passed**	Status: There are no Restricted users at present
Microsoft 365 Defender-Audit	Ensure the Account Provisioning Activity report is reviewed at least weekly	**Passed**	Account Provisioning Items: 0
Microsoft 365 Defender-Audit	Ensure non-global administrator role group assignments are reviewed at least weekly	**Passed**	Status: There are no non-admin Global Role assignments found in past 7 days
Microsoft 365 Defender-Settings	Ensure Microsoft Defender for Cloud Apps is Enabled	**Passed**	Status: Enabled
Microsoft Purview-Audit	Ensure Microsoft 365 audit log search is Enabled	**Passed**	Status: Enabled
Microsoft Purview-Audit	Ensure user role group changes are reviewed at least weekly	**Passed**	Status: There are no user role group changes found in past 7 days
Microsoft Entra admin center-Identity-Overview	Ensure Security Defaults is disabled on Azure Active Directory	**Passed**	Status: Security Defaults are disabled.
Microsoft Entra admin center-Identity-Users	Ensure Per-user MFA is disabled	**Passed**	Total Per-User MFA Enabled: 0

Microsoft Entra admin center-Protection-Password Reset	Ensure Self service password reset enabled is set to All	**Passed**	Self-Service Password Status: You have 0 of 0 users who don't have self-service password reset enabled.
Microsoft Entra admin center-Protection-Password Reset	Ensure the self-service password reset activity report is reviewed at least weekly	**Passed**	Status: Changed Password Found via SSPR
Microsoft Entra admin center-Protection-Risk Activities	Ensure the Azure AD Risky sign-ins report is reviewed at least weekly	**Passed**	Status: No Risky user found
Microsoft Entra admin center-Identity Governance	Ensure Privileged Identity Management is used to manage roles	**Passed**	Status: No permanent active role assignments found.
Microsoft Exchange admin center-Audit	Ensure AuditDisabled organizationally is set to False	**Passed**	Status: Enabled
Microsoft Exchange admin center-Audit	Ensure mailbox auditing for E3 users is Enabled	**Passed**	Missing Mailbox Auditing: 0
Microsoft Exchange admin center-Audit	Ensure mailbox auditing for E5 users is Enabled	**Passed**	Missing Mailbox Auditing: 0
Microsoft Exchange admin center-Audit	Ensure Microsoft 365 Exchange Online Admin Auditing Is Enabled	**Passed**	Status: Enabled
Microsoft Exchange admin center-Audit	Ensure Microsoft 365 Exchange Online Unified Auditing Is Enabled	**Passed**	Status: Enabled
Microsoft Exchange admin center-Mailflow	Ensure all forms of mail forwarding are blocked and-or disabled	**Passed**	Mails Forwarding Rules Enabled: 0
Microsoft Exchange admin center-Mailflow	Ensure mail transport rules do not whitelist specific domains	**Passed**	Whitelist Domains: 0
Microsoft Exchange admin center-Mailflow	Ensure Tagging does not allow specific domains	**Passed**	Tagging Allowed Domains: 0
Microsoft Exchange admin center-Mailflow	Ensure Do Not Bypass the Safe Attachments Filter is not configured	**Passed**	Status: Not Configured

Microsoft Exchange admin center-Mailflow	Ensure Do Not Bypass the Safe Links Feature is not configured	**Passed**	Status: Not Configured
Microsoft Exchange admin center-Mailflow	Ensure Exchange Modern Authentication is Enabled	**Passed**	Status: Enabled
Microsoft Exchange admin center-Mailflow	Ensure Transport Rules to Block Executable Attachments are configured	**Passed**	Status: Configured
Microsoft Exchange admin center-Mailflow	Ensure Malware Filter Policies Alert for Internal Users Sending Malware is configured	**Passed**	Status: Configured
Microsoft Exchange admin center-Mailflow	Ensure Transport Rules to Block Large Attachments are configured	**Passed**	Status: Configured
Microsoft Exchange admin center-Mailflow	Ensure Mailbox Auditing is Enabled at Tenant Level	**Passed**	Status: Enabled
Microsoft Exchange admin center-Mailflow	Ensure Mailboxes without Mailbox Auditing are not present	**Passed**	Mailboxes Without Auditing: 0
Microsoft Exchange admin center-Mailflow	Ensure Exchange Mailboxes with IMAP is not Enabled	**Passed**	Status: No Mailboxes with IMAP
Microsoft Exchange admin center-Mailflow	Ensure mail transport rules do not forward email to external domains	**Passed**	Mails Forwarding Rules Enabled: 0
Microsoft Exchange admin center-Mailflow	Ensure the Advanced Threat Protection Safe Links policy is enabled	**Passed**	Status: Not Enabled-Not Implemented
Microsoft Exchange admin center-Mailflow	Ensure the Advanced Threat Protection SafeAttachments policy is enabled	**Passed**	Status: Not Enabled-Not Implemented
Microsoft Exchange admin center-Mailflow	Ensure that an anti-phishing policy has been created	**Passed**	Status: Created
Microsoft Exchange admin center-Mailflow	Ensure mailbox auditing for all users is Enabled	**Passed**	Missing Mailbox Auditing: 0

Microsoft Exchange admin center-Reports	Ensure mail forwarding rules are reviewed at least weekly	**Passed**	Forwarding Rules To External Domains: 0
Microsoft Exchange admin center-Reports	Ensure the Malware Detections report is reviewed at least weekly	**Passed**	Malware Report Items: 0
Microsoft Exchange admin center-Reports	Ensure Microsoft 365 Deleted Mailboxes are identified and Verified	**Passed**	Deleted Mailboxes: 0
Microsoft Exchange admin center-Reports	Ensure Microsoft 365 Hidden Mailboxes are Identified	**Passed**	Hidden Mailboxes: 0
Microsoft Exchange admin center-Reports	Ensure Mailboxes External Address Forwarding is not configured	**Passed**	Mailboxes Forwarding To External Domains: 0
Microsoft Exchange admin center-Reports	Ensure Exchange Online Mailboxes on Litigation Hold	**Passed**	Mailboxes On Litigation Hold: 0
Microsoft Exchange admin center-Reports	Ensure Exchange Online Mailbox Auditing is enabled	**Passed**	Mailboxes Without Auditing: 0
Microsoft Exchange admin center-Reports	Microsoft 365 Exchange Online Admin Success and Failure Attempts	**Passed**	Failures for Online Admins: 0
Microsoft Exchange admin center-Reports	Microsoft 365 Exchange Online External Access Admin Success and Failure Attempts	**Passed**	Failures for External Admins: 0
Microsoft Exchange admin center-Settings	Ensure modern authentication for Exchange Online is enabled	**Passed**	Status: Enabled
Microsoft SharePoint Admin Center-Policies	Ensure document sharing is being controlled by domains with whitelist or blacklist	**Passed**	Status: Controlled
Microsoft SharePoint Admin Center-Policies	Ensure expiration time for external sharing links is set	**Passed**	Status: Expiration Time for Links Is Set to
Microsoft SharePoint Admin Center-Settings	External user sharing-share by email-and guest link sharing are both disabled	**Passed**	Status: Disabled

Microsoft Fabric-Tenant Settings	Ensure Allow users to apply sensitivity labels for content is Enabled	**Passed**	Status: Allow users to apply sensitivity labels for content is enabled
Microsoft M365 Users-Users	Ensure Deleted Microsoft 365 Users are Identified	**Passed**	Deleted Users: 0
Microsoft M365 Users-Users	Ensure Disabled Microsoft 365 Users are Identified	**Passed**	Disabled Users: 4
Microsoft M365 Users-Users	Ensure Microsoft 365 Users have no Reconciliation Errors	**Passed**	Users Reconciliation Errors: 0
Microsoft M365 Users-Users	Ensure Microsoft 365 Users Password Expires	**Passed**	Password Never Expires Set: 0
Microsoft M365 Users-Users	Ensure Microsoft 365 Users are Syncing and No Sync Errors	**Passed**	Users in Sync Errors: 0
Microsoft M365 Users-Users	Ensure no Provisioning Errors for Microsoft 365 Users	**Passed**	Users Not Provisioned: 0
Microsoft M365 Users-Users	Ensure Microsoft 365 Blocked Users are Identified	**Passed**	Microsoft 365 Users Blocked: 0
Microsoft M365 Users-Users	Ensure Microsoft 365 Company Administrators have less than 5 Admins	**Passed**	More Than 10 Company Administrators Status: 4
Microsoft M365 Users-Users	Ensure Microsoft 365 Deleted and Licensed Users are Identified	**Passed**	Deleted Users Licensed: 0
Microsoft M365 Configuration	Ensure All Microsoft 365 Domains Have been verified	**Passed**	Domains Verification Pending: 0
Microsoft M365 Configuration	Ensure Microsoft 365 Domain Services Have Services Assigned	**Passed**	Domains Without Services: 0
Microsoft M365 Configuration	Ensure Microsoft 365 Notification Email is configured	**Passed**	Notifications Email: Nirmal@DynamicPacks.net
Microsoft M365 Configuration	Ensure Microsoft 365 Organization Level Mailbox Auditing is configured	**Passed**	Status: Enabled
Microsoft M365 Configuration	Ensure No Microsoft 365 Dir Sync Property Conflicts	**Passed**	Total Objects In Property Conflict: 0
Microsoft M365 Configuration	Ensure No Microsoft 365 Dir Sync Property Conflict with User Principal Name	**Passed**	Objects In UPN Conflicts: 0
Microsoft M365 Configuration	**Ensure No Microsoft 365 Dir Sync Property Conflict with ProxyAddress**	**Passed**	**Objects in ProxyAddress Conflicts: 0**

APPENDIX-2: Skipped Tests

The following table lists the Tests that were skipped. Some tests in the Auditing Category have been skipped because these tests need to be executed by an Microsoft 365 Engineer every week and execution of some tests were skipped as they require the creation of an Azure AD Application for Microsoft 365 Assessment.

Test	CATEGORY
Ensure two emergency access accounts have been defined	M365 Admin Center-Users
Ensure Idle session timeout is set to 3 hours (or less) for unmanaged devices	M365 Admin Center-Settings
Ensure User owned apps and services is restricted	M365 Admin Center-Settings
Ensure internal phishing protection for Forms is enabled	M365 Admin Center-Settings
Ensure that Sways cannot be shared with people outside of your organization	M365 Admin Center-Settings
Ensure that password protection is enabled for Active Directory	Microsoft Entra admin center-Protection-Authentication Methods
Ensure Access reviews for Guest Users are configured	Microsoft Entra admin center-Identity Governance
Ensure Access reviews for high privileged Azure AD roles are configured	Microsoft Entra admin center-Identity Governance
Ensure Dangerous Attachment Extensions are Filtered is configured	Microsoft Exchange admin center-Mailflow
Ensure Exchange Mailboxes with POP is not Enabled	Microsoft Exchange admin center-Mailflow
Ensure Common Malicious Attachment Extensions are Filtered	Microsoft Exchange admin center-Mailflow
Ensure the Mailbox Access by Non-Owners Report is reviewed at least biweekly	Microsoft Exchange admin center-Reports
Ensure the report of users who have had their email privileges restricted due to spamming is reviewed	Microsoft Exchange admin center-Reports
Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled	Microsoft SharePoint Admin Center-Policies
Ensure OneDrive content sharing is restricted	Microsoft SharePoint Admin Center-Policies
Ensure link sharing is restricted in SharePoint and OneDrive	Microsoft SharePoint Admin Center-Policies
Ensure external sharing is restricted by security group	Microsoft SharePoint Admin Center-Policies
Ensure reauthentication with verification code is restricted	Microsoft SharePoint Admin Center-Policies

Ensure custom script execution is restricted on site collections	Microsoft SharePoint Admin Center-Settings
Ensure users cant send emails to a channel email address	Microsoft Teams Admin Center-Teams
Ensure external access is restricted in the Teams admin center	Microsoft Teams Admin Center-Users
Ensure anonymous users cant join a meeting	Microsoft Teams Admin Center-Meetings
Ensure anonymous users and dial-in callers cant start a meeting	Microsoft Teams Admin Center-Meetings
Ensure only people in my org can bypass the lobby	Microsoft Teams Admin Center-Meetings
Ensure users dialing in cant bypass the lobby	Microsoft Teams Admin Center-Meetings
Ensure meeting chat does not allow anonymous users	Microsoft Teams Admin Center-Meetings
Ensure only organizers and co-organizers can present	Microsoft Teams Admin Center-Meetings
Ensure external participants cant give or request control	Microsoft Teams Admin Center-Meetings
Ensure users can report security concerns in Teams	Microsoft Teams Admin Center-Messaging
Ensure guest access to content is restricted	Microsoft Fabric-Tenant Settings
Ensure Publish to web is restricted	Microsoft Fabric-Tenant Settings
Ensure Interact with and share R and Python visuals is Disabled	Microsoft Fabric-Tenant Settings
Ensure shareable links are restricted	Microsoft Fabric-Tenant Settings
Ensure enabling of external data sharing is restricted	Microsoft Fabric-Tenant Settings
Ensure Block ResourceKey Authentication is Enabled	**Microsoft Fabric-Tenant Settings**