

# MICROSOFT CLOUD ASSESSMENT

## Management Plan



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: HQ

Prepared by: Indusflow Systems

02/21/2025





Scan Date: 02/21/2025





# Management Plan







The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the Overall Risk Score but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

## High Risk













RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
90	<b>Unimplemented Microsoft Control: Disable JavaScript on Adobe DC</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.	HF	HF
90	<b>Unimplemented Microsoft Control: Disable 'Continue running background apps when Google Chrome is closed'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.	HF	HF
90	<b>Control sharing of documents to external domains by either blocking domains or only allowing sharing with specific named domains. Note - this control's mandatory compliance requirement is to set allow list domains.</b> To configure document sharing restrictions: Navigate to SharePoint admin center - <a href="https://admin.microsoft.com/sharepoint">https://admin.microsoft.com/sharepoint</a> . Expand Policies then click Sharing. Expand More external sharing settings and check Limit external sharing by domain. Select Add domains to add a list of approved domains. Click Save at the bottom of the page. To configure document sharing restrictions using PowerShell: Connect to SharePoint Online using Connect-SPOService. Run the following PowerShell command: Set-SPOTenant - SharingDomainRestrictionMode AllowList - SharingAllowedDomainList "domain1.com domain2.com"	HF	HF

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
90	<p><b>Unimplemented Microsoft Control: Fix Microsoft Defender for Endpoint sensor data collection</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Ensure multifactor authentication is enabled for all users in administrative roles</b></p> <p>Microsoft services provide step-by-step guidance to select and enable the right MFA method for your organization in the Microsoft 365 admin center. Go to the Microsoft 365 MFA (<a href="https://admin.microsoft.com/adminportal/home?Q=SecureScore#/featureexplorer/security/ConditionalAccess)wizard">https://admin.microsoft.com/adminportal/home?Q=SecureScore#/featureexplorer/security/ConditionalAccess)wizard</a>, If you would like to perform the implementation yourself, first check what Microsoft Entra ID license you have under "Prerequisites" in Microsoft Secure Score or see your license type under "Basic information" in the Microsoft Entra ID Overview (<a href="https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview">https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview</a>). If you've invested in Microsoft Entra ID Premium P1 or P2 licenses, you can create a Conditional Access policy from scratch or by using a template. Follow these steps to create a Conditional Access policy from scratch or by using a template (<a href="https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa">https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa</a>), If you would like to perform the implementation yourself and you're using Microsoft Entra ID Free, turn on security defaults. Note: Security defaults and Conditional Access can't be used side by side. Enable security defaults (<a href="https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults">https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults</a>), Keep track of your admin's progress of registering authentication methods by going to Microsoft Entra ID &gt; Security &gt; Authentication methods &gt; User registration details (requires Microsoft Entra ID Premium P1 or P2 licenses). Go to User registration details (<a href="https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/_/UserRegistrationDetails">https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/_/UserRegistrationDetails</a>)</p>		










RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
90	<p><b>Unimplemented Microsoft Control: Enable Conditional Access policies to block legacy authentication</b></p> <p>Microsoft services provide step-by-step guidance to select and enable the right method to block legacy authentication for your organization in the Microsoft 365 admin center (part of the MFA wizard). Go to the Microsoft 365 MFA wizard (<a href="https://admin.microsoft.com/adminportal/home?Q=SecureScore#/featureexplorer/security/ConditionalAccess">https://admin.microsoft.com/adminportal/home?Q=SecureScore#/featureexplorer/security/ConditionalAccess</a>), If you would like to perform the implementation yourself, first check what Microsoft Entra ID license you have under "Prerequisites" in Microsoft Secure Score or see your license type under "Basic information" in the Microsoft Entra ID Overview (<a href="https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview">https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview</a>). If you've invested in Microsoft Entra ID Premium P1 or P2 licenses, you can create a Conditional Access policy from scratch or by using a template. Follow these steps to create a Conditional Access policy from scratch or by using a template (<a href="https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-policy-block-legacy">https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-policy-block-legacy</a>), If you would like to perform the implementation yourself and you're using Microsoft Entra ID Free, turn on security defaults. Note: Security defaults and Conditional Access can't be used side by side. Enable security defaults (<a href="https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults">https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults</a>)</p>		
90	<p><b>Unimplemented Microsoft Control: Ensure multifactor authentication is enabled for all users</b></p> <p>Microsoft services provide step-by-step guidance to select and enable the right MFA method for your organization in the Microsoft 365 admin center. Go to the Microsoft 365 MFA wizard (<a href="https://admin.microsoft.com/adminportal/home?Q=SecureScore#/featureexplorer/security/ConditionalAccess">https://admin.microsoft.com/adminportal/home?Q=SecureScore#/featureexplorer/security/ConditionalAccess</a>), If you would like to perform the implementation yourself, first check what Microsoft Entra ID license you have under "Prerequisites" in Microsoft Secure Score or see your license type under "Basic information" in the Microsoft Entra ID Overview (<a href="https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview">https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview</a>). If</p>		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	<p>you've invested in Microsoft Entra ID Premium P1 or P2 licenses, you can create a Conditional Access policy from scratch or by using a template. Follow these steps to create a Conditional Access policy from scratch or by using a template  <a href="https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-policy-registration">https://docs.microsoft.com/azure/active-directory/conditional-access/howto-conditional-access-policy-registration</a>), If you would like to perform the implementation yourself and you're using Microsoft Entra ID Free, turn on security defaults. Note: Security defaults and Conditional Access can't be used side by side. Enable security defaults  <a href="https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults">https://docs.microsoft.com/azure/active-directory/fundamentals/concept-fundamentals-security-defaults</a>), Keep track of your user's progress of registering authentication methods by going to Microsoft Entra ID &gt; Security &gt; Authentication methods &gt; User registration details (requires Microsoft Entra ID Premium P1 or P2 licenses). Go to User registration details  <a href="https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/_/UserRegistrationDetails">https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/_/UserRegistrationDetails</a>),</p>		
90	<p><b>Unimplemented Microsoft Control: Deploy a log collector to discover shadow IT activity</b>            In the Defender for Cloud Apps portal, go to the Automatic log upload page. In the Data sources tab, select Add data source to create a data source for your appliance. In the Log collector tab, select Add log collector to add a new one. Follow the instructions provided to deploy Docker (<a href="https://docs.microsoft.com/cloud-app-security/discovery-docker">https://docs.microsoft.com/cloud-app-security/discovery-docker</a>) and the log collector container.</p>		
90	<p><b>Unimplemented Microsoft Control: Restrict anonymous users from joining meetings</b>            1. Log into Microsoft Teams admin center 2. In the left navigation, go to Meetings &gt; Meeting Settings 3. Under the Participants section, toggle "Anonymous users can join a meeting" to Off</p>		
90	<p><b>Unimplemented Microsoft Control: Enable Automatic Updates</b>            Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or</p>		











RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	exception options.		
90	<p><b>Unimplemented Microsoft Control: Enable 'Hide Option to Enable or Disable Updates'</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Turn on Microsoft Defender for Endpoint sensor</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Block Office applications from creating executable content</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Fix Microsoft Defender for Endpoint impaired communications</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Block Office applications from injecting code into other processes</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Turn on PUA protection in block mode</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or</p>		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	exception options.		
90	<p><b>Unimplemented Microsoft Control: Set controlled folder access to enabled or audit mode</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Turn on Microsoft Defender Credential Guard</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Disable 'Password Manager'</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Enable 'Block third party cookies'</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Enable 'Local Security Authority (LSA) protection'</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Block executable content from email client and webmail</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		











RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
90	<b>Unimplemented Microsoft Control: Block JavaScript or VBScript from launching downloaded executable content</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Block Win32 API calls from Office macros</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Enable 'Apply UAC restrictions to local accounts on network logons'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Disable merging of local Microsoft Defender Firewall connection rules with group policy firewall rules for the Public profile</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Set User Account Control (UAC) to automatically deny elevation requests</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Block executable files from running unless they meet a prevalence, age, or trusted list criterion</b> Within Microsoft 365 security, go to		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Use advanced protection against ransomware</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Block credential stealing from the Windows local security authority subsystem (lsass.exe)</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Block process creations originating from PSEXec and WMI commands</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Block untrusted and unsigned processes that run from USB</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Block Office communication application from creating child processes</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Block Adobe Reader from creating child</b>		













RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	<p><b>processes</b>            Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Block persistence through WMI event subscription</b>            Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Block abuse of exploited vulnerable signed drivers</b>            Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Disable 'Enumerate administrator accounts on elevation'</b>            Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Block execution of potentially obfuscated scripts</b>            Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Disable the built-in Administrator account</b>            Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Set 'Minimum password length' to '14 or more</b></p>		







RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	<b>characters'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Set 'Enforce password history' to '24 or more password(s)'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Set 'Minimum password age' to '1 or more day(s)'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Disable Microsoft Defender Firewall notifications when programs are blocked for Domain profile</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Disable Microsoft Defender Firewall notifications when programs are blocked for Private profile</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Disable Microsoft Defender Firewall notifications when programs are blocked for Public profile</b> Within Microsoft 365 security, go to Vulnerability management >		









RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Block all Office applications from creating child processes</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Disable SMBv1 client driver</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Enable 'Network Protection'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Disable 'Allow Basic authentication' for WinRM Client</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Publish M365 sensitivity label data classification policies</b> Open Microsoft Purview compliance portal, Under Solutions click Information protection, Ensure Labels exist, Click on Label policies tab, Ensure that a Label policy exists and is published accordingly, Make sure Labels are published on all of your licensed users and groups,		
90	<b>Unimplemented Microsoft Control: Ensure 'External sharing' of calendars is not</b>		











RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	<b>available</b> In the Microsoft 365 Exchange admin center ( <a href="https://admin.exchange.microsoft.com/">https://admin.exchange.microsoft.com/</a> ), go to Organization > Sharing. Under Individual Sharing, make sure all policies are unticked.		
90	<b>Unimplemented Microsoft Control: Limit external participants from having control in a Teams meeting</b> Log into Microsoft Teams admin center ( <a href="https://admin.teams.microsoft.com/">https://admin.teams.microsoft.com/</a> ), In the left navigation, go to Meetings > Meeting Policies, Under Manage Policies, select a group/direct policy, Under the Content Sharing section, toggle "Allow an external participant to give or request control" to Off, You'll need to change this setting for each group/direct policy,		
90	<b>Unimplemented Microsoft Control: Set 'Minimum PIN length for startup' to '6 or more characters'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Enable 'Require additional authentication at startup'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Disable 'Autoplay for non-volume devices'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Disable 'Autoplay' for all drives</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		







RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
90	<b>Unimplemented Microsoft Control: Set default behavior for 'AutoRun' to 'Enabled: Do not execute any autorun commands'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Set LAN Manager authentication level to 'Send NTLMv2 response only. Refuse LM &amp; NTLM'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Disable 'Allow Basic authentication' for WinRM Service</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Disable 'Installation and configuration of Network Bridge on your DNS domain network'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Disable Flash on Adobe Reader DC</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Disable JavaScript on Adobe Reader DC</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or		





RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	exception options.		
90	<p><b>Unimplemented Microsoft Control: Set IPv6 source routing to highest protection</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Disable IP source routing</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Disable Solicited Remote Assistance</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Disable Anonymous enumeration of shares</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Enable Microsoft Defender Antivirus email scanning</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Disable the local storage of passwords and credentials</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		





RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
90	<p><b>Unimplemented Microsoft Control: Enable 'Microsoft network client: Digitally sign communications (always)'</b></p> <p>Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
90	<p><b>Unimplemented Microsoft Control: Ensure that Auto-labeling data classification policies are set up and used</b></p> <p>Open Microsoft Purview compliance portal, Under Solutions, click Information protection, Click on Auto-Labeling tab, Ensure that an Auto-Labeling policy exists and is published accordingly, Make sure Auto-Labeling policies are published on all of your licensed users and group,</p>		
90	<p><b>Microsoft OneDrive allows users to sign in their cloud tenant account, and begin syncing select folders or the entire contents of OneDrive to a local computer. By default this includes any computer with OneDrive already installed, whether or not it is Azure Domain Joined or Active Directory Domain joined. 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 Microsoft Entra ID domains. If you have devices which are only Microsoft Entra ID joined, consider using a Conditional Access Policy instead.</b></p> <p>To block the sync client on unmanaged devices, use the Microsoft 365 Admin Center: Navigate to Microsoft 365 administration portal (<a href="https://admin.microsoft.com">https://admin.microsoft.com</a>), Click on All Admin Centers and then Show All, then SharePoint. Now click Settings followed by OneDrive - Sync, Check the Allow syncing only on computers joined to specific domains, Use the Get-ADDomain PowerShell command to obtain the GUID from each domain then add</p>		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	them to the box. Click Save		
90	<b>Determines whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication.</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Determines the amount of inactivity time (in seconds) of a logon session, beyond which the screen saver will run, locking the session. This security control is only applicable for machines with Windows 10, version 1709 or later.</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Unimplemented Microsoft Control: Enable 'Require domain users to elevate when setting a network's location'</b> Within Microsoft 365 security, go to Vulnerability management > Recommendations, read the relevant security recommendation and choose remediation or exception options.		
90	<b>Administrative accounts are special privileged accounts that could have varying levels of access to data, users, and settings. Regular user accounts should never be utilized for Administrative tasks and care should be taken, in the case of a hybrid environment, to keep Administrative accounts separated from on-prem accounts. Administrative accounts should not have applications assigned so that they have no access to potentially vulnerable services (EX. email, Teams, SharePoint, etc.) and only access to perform tasks as needed for Administrative purposes.</b> 1. Navigate to Microsoft 365 admin center 2. Click to expand Users select Active users. 3. Sort by the Licenses column. 4. For each user account in an administrative role verify the following: The account is Cloud only (not		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	synced) The account is assigned a license that is not associated with applications i.e. (Microsoft Entra ID P1, Microsoft Entra ID P2)		
90	<p><b>Unimplemented Microsoft Control: Ensure that no sender domains are allowed for anti-spam policies</b></p> <p>Remove all allowed domains and allowed senders from all your inbound anti-spam policies.</p>		
90	<p><b>Automatic email forwarding is enabled</b></p>		
90	<p><b>Unimplemented Microsoft Control: Block users who reached the message limit</b></p> <p>Ensure that all users have an assigned outbound anti-spam policy with the 'Over limit action' option set to recommended values (<a href="https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365?view=o365-worldwide#eop-outbound-spam-policy-settings">https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365?view=o365-worldwide#eop-outbound-spam-policy-settings</a>) which is "Restrict the user from sending mail", by either updating your existing policies or creating new ones.</p>		
90	<p><b>Unimplemented Microsoft Control: Start your Defender for Identity deployment, installing Sensors on Domain Controllers and other eligible servers.</b></p> <p>Go to the sensor page in Settings, you can view the already installed sensors in your environment and download the install package to deploy them on your remaining domain controllers. You will be scored as a percentage of your deployment progress.</p>		
90	<p><b>Unimplemented Microsoft Control: Ensure mailbox auditing for all users is Enabled</b></p> <p>To enable mailbox auditing for all users: Connect to Exchange Online using Connect-ExchangeOnline. Run the following PowerShell command: Set-OrganizationConfig -AuditDisabled \$false, For each unconfigured MailBox of type Resource Mailboxes, Public Folder Mailboxes or DiscoverySearch Mailbox run: Get-Mailbox -Filter "Name -eq 'MailBox name'"   Set-Mailbox -AuditEnabled \$true,</p>		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
90	<p><b>Unimplemented Microsoft Control: Ensure MailTips are enabled for end users</b></p> <p>To enable MailTips, use the Exchange Online PowerShell Module: Run Microsoft Exchange Online PowerShell Module, Connect using "Connect-ExchangeOnline", Run the following PowerShell command: Set-OrganizationConfig -MailTipsAllTipsEnabled \$true - MailTipsExternalRecipientsTipsEnabled \$true - MailTipsGroupMetricsEnabled \$true - MailTipsLargeAudienceThreshold '25'</p>		
90	<p><b>Unimplemented Microsoft Control: Ensure additional storage providers are restricted in Outlook on the web</b></p> <p>Restrict additional storage providers are restricted using PowerShell: Connect to Exchange Online using Connect-ExchangeOnline. Run the following PowerShell command: Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default - AdditionalStorageProvidersAvailable \$false, Run the following Powershell command to verify that the value is now False: Get-OwaMailboxPolicy   Format-Table Name, AdditionalStorageProvidersAvailable,</p>		
90	<p><b>Unimplemented Microsoft Control: Ensure all forms of mail forwarding are blocked and/or disabled</b></p> <p>NOTE: In this control, remediation is carried out in two stages - Step 1 is manual and will not be monitored automatically by secure score, whereas Step 2 is monitored automatically: STEP 1: Transport rules To alter the mail transport rules so they do not forward email to external domains, use the Microsoft 365 Admin Center: Select Exchange to open the Exchange admin center. Select Mail Flow then Rules. For each rule that redirects email to external domains, select the rule and click the 'Delete' icon. To perform remediation you may also use the Exchange Online PowerShell Module: Connect to Exchange Online user Connect-ExchangeOnline. Run the following PowerShell command: Remove-TransportRule {RuleName}, To verify this worked you may re-run the audit command as follows: Get-TransportRule   Where-Object {\$_.RedirectMessageTo -ne \$null}   ft Name,RedirectMessageTo, STEP 2: Anti-spam outbound policy Configure an anti-spam outbound policy: Navigate to Microsoft 365 Defender <a href="https://security.microsoft.com/">https://security.microsoft.com/</a>,</p>		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	Expand E-mail & collaboration then select Policies & rules. Select Threat policies > Anti-spam. Select Anti-spam outbound policy (default), Click Edit protection settings, Set Automatic forwarding rules dropdown to Off - Forwarding is disabled and click Save, Repeat steps 4-6 for any additional higher priority, custom policies.		
90	<b>Unimplemented Microsoft Control: Ensure modern authentication for SharePoint applications is required</b> In the Microsoft 365 Admin Center: 1. Go to SharePoint Admin Center. 2. Expand the Policies section then select Access control. 3. Select Apps that don't use modern authentication. 4. Select the radio button for Block access. 5. Click Save.		
90	<b>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 ID 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. Rationale: 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.</b> To enable Microsoft Azure Management restrictions: Navigate to the Microsoft Entra ID admin center <a href="https://entra.microsoft.com">https://entra.microsoft.com</a> . Click expand Protection > Conditional Access select		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	<p>Policies. Click New Policy and then name the policy. Select Users &gt; Include &gt; All Users, Select Users &gt; Exclude &gt; Directory roles and select only administrative roles (See below). Select Cloud apps or actions &gt; Select apps &gt; Select then click the box next to Microsoft Azure Management. Click Select. Select Grant &gt; Block access and click Select. Ensure Enable Policy is On then click Create. <b>WARNING:</b> 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. Below is an example list of Administrator roles that could be excluded: 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, Default Value: No - Non-administrators can access the Microsoft Entra ID administration portal.</p>		
<p><b>90</b></p>	<p><b>Unimplemented Microsoft Control: Prohibit use of Internet Connection Sharing on your DNS domain network</b>            Within Microsoft 365 security, go to Vulnerability management &gt; Recommendations, read the relevant security recommendation and choose remediation or exception options.</p>		
<p><b>90</b></p>	<p><b>Enable Microsoft Entra ID 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 impact unless working with on-premises Active Directory.</b>            To setup Microsoft Entra ID Password Protection, use the following steps: Download and install the Microsoft Entra ID Password Proxies and DC Agents from the following location:  <a href="https://www.microsoft.com/download/details.aspx?id=57071">https://www.microsoft.com/download/details.aspx?id=57071</a>, After the installation is complete, login to <a href="https://admin.microsoft.com">https://admin.microsoft.com</a> as a Global Administrator. Go to Admin centers and click on Microsoft Entra ID. Select Microsoft Entra ID then Security on the left side navigation</p>		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
------------	----------------	----------	-------------

followed by Authentication methods. Select Password protection and toggle Enable password protection on Windows Server Active Directory to Yes and Mode to Enforced, Click Save at the top of the right pane.

90

**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, Passwordless 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 must 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. Rationale: 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. References: FIDO2 security keys (<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless#fido2-security-keys>), Enable passwordless security key sign-in**



RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
------------	----------------	----------	-------------

(<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key>), Conditional Access authentication strength (<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths>), How To: Configure the Microsoft Entra ID multifactor authentication registration policy (<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy>),

To create a phishing-resistant MFA CA policy for users in administrative roles: Navigate to the Microsoft Entra ID admin center <https://entra.microsoft.com>. Click to expand Microsoft Entra ID > Applications select Enterprise Applications. Under Security, select Conditional Access. Click New policy. Go to Users > Users and groups > Include > Select users and groups > Directory roles, Add at least the Directory roles listed after these steps. Select Cloud apps or actions > All cloud apps (and don't exclude any apps). Grant > Grant Access with Require authentication strength (Preview): Phishing-resistant MFA, Click 'Select', 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".

90

**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**



RISK SCORE RECOMMENDATION SEVERITY PROBABILITY

**from your tenancy without having to maintain the breached account**

In the Microsoft 365 Admin Center Select Admin Centers and Microsoft Entra ID. Select Users from the Azure navigation pane, Select Users settings. Set App registrations is set to No. Click Save.

90

**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. Rationale: 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 Word, Excel, or PowerPoint helps reduce your threat-surface and mitigate this risk. Impact: 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.**





To prohibit users installing Office Store add-ins and starting 365 trials: Navigate to Microsoft 365 admin center <https://admin.microsoft.com>. 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. Note - Due to temporary limitations, only "Let users access the Office Store" will be taken into account in scoring this control. It is suggested to uncheck both settings for the sake of better posture.



90

**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. 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**



RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
	<p><b>exploits, leading to potential breaches of accounts and data. Note: To comply, only mobile devices must be configured (Windows or MacOS is not required). User impact: The impact associated with this change is dependent upon the settings specified in the mobile device configuration profile.</b></p> <p>To set mobile device management profiles, use the Microsoft Intune admin center (<a href="https://intune.microsoft.com/#home">https://intune.microsoft.com/#home</a>): Select Devices and then under Policy select Configuration profiles, Select Create profile to create a new profile. Select the appropriate Platform (iOS or Android). Choose, based on your organization's needs, the desired settings from the configuration screens. Note that the condition to comply is the mere existence of such profile, the specific settings should be decided according to your organization's needs. To comply, there should be at least one configuration policy for mobile devices. It is suggested to create two policies for both iOS and Android.</p>		
90	<p><b>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. Note: To comply, there should be at least one device configuration for Android with device password encryption. User impact: This setting should have no user impact, provided the device supports the feature.</b></p> <p>To set mobile device management profiles, use the Microsoft Intune admin center (<a href="https://intune.microsoft.com/#home">https://intune.microsoft.com/#home</a>): Select Devices, then under Policy select Configuration profiles, If there are no policies, select Create Policy. Set a Name for the policy, choose the appropriate Platform and select Device restrictions. In the Password section, ensure that Encryption is set to Require. If there are existing policies, per each policy - Select the policy by clicking on it. Select Edit next to Configuration settings. In the Password section, ensure that Encryption is set to Require. Note: To comply, there should be at least one device configuration for Android with device password encryption.</p>		
90	<p><b>Sway is a new app from Microsoft Office that allows users to create and share</b></p>		

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
------------	----------------	----------	-------------

**interactive reports, personal stories, presentations, and more. This setting controls user Sway sharing capability, both within and outside of the organization. By default, Sway is enabled for everyone in the organization. Rationale: Disable external sharing of Sway documents that can contain sensitive information to prevent accidental or arbitrary data leak.**

To ensure Sways cannot be viewed outside of your organization: Navigate to Microsoft 365 admin center <https://admin.microsoft.com>. Click to expand Settings then select Org settings. Under Services select Sway and block Let people in your organization share their sways with people outside your organization. Click Save.

 **Low Risk**

RISK SCORE	RECOMMENDATION	SEVERITY	PROBABILITY
------------	----------------	----------	-------------

**25**

**Team settings allows guests to create and remove channels. This could cause loss of data as guests add and remove channels.**

Verify if guest creation and removal of channels is desired on the specified Teams. When not necessary, disable the ability of Team guests to create and remove channels to avoid potential data loss and channel proliferation.



- Coordinator of Volunteers Interest Group (CVIG)
- Design Build Interest Group (DBIG)
- PACE Team