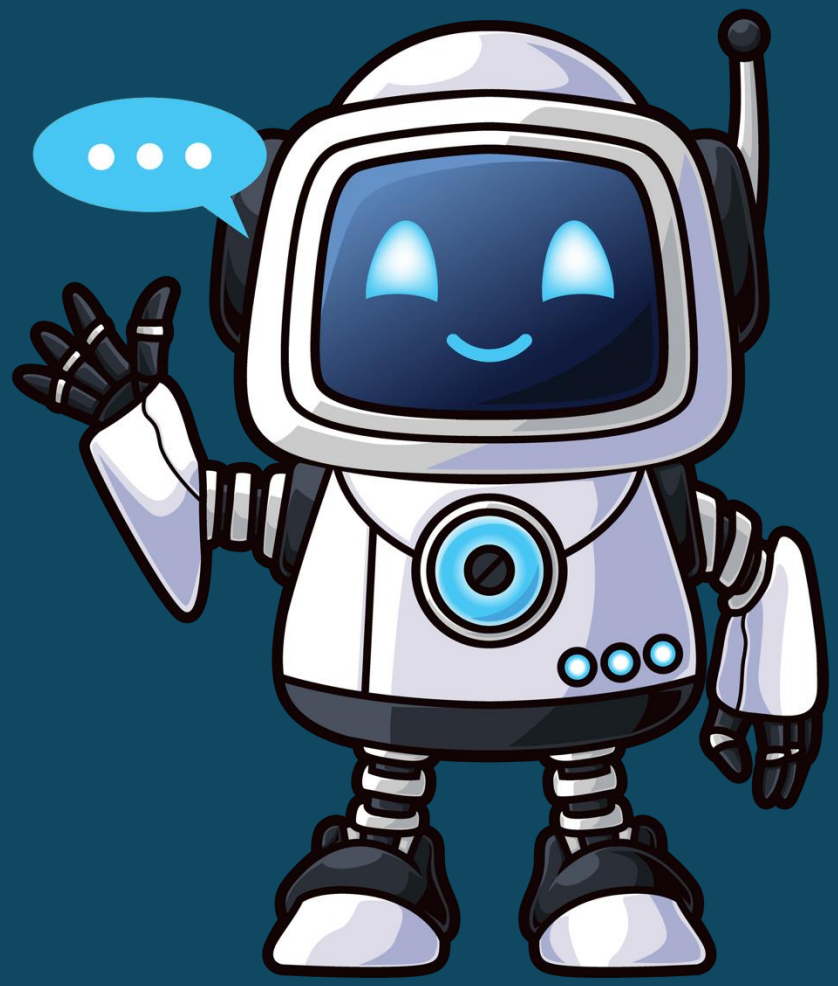
Fusion 360

AI-Enhanced Automation Engine

Automation Mapping Guide



vCIO TOOLBOX

January 26th, 2026

Fusion 360 | AI-Enhanced Automation Engine Mapping Guide

The Rules define what the rule that should be aligned to a template question to run the automation.

The Mapped Questions in the vCIOToolbox Templates represent the default questions that vCIOToolbox provided in your Global Templates at the time of subscription. If you made customizations to your templates this data will provide you the context behind each rule and mapped control so you can align appropriately in your custom templates.

Items outlined in **green** are new automations that do not tie to any existing template question/control. Users will need to create a new template question for each. These new automations focus on end-of-life data which is now generated in our Asset Management section via Asset Policies.

Automation Mapping – Rule to Control

Rules		Mapped Questions in vCIOToolbox Templates			
Rule Name	Base Asset Type	Template	Topic	Question	Questions Text
SAT Program	None	Cybersecurity and Risk	Awareness and Training	Security Awareness Program	All users are informed and trained on how to identify information risk and bad actor tactics (i.e. phishing, smshing, social engineering tactics, etc.)
SAT Training	None	Cybersecurity and Risk	Awareness and Training	Awareness Training - Users	Are all users up to date on their training?
SAT Phishing	None	Cybersecurity and Risk	Awareness and Training	Phishing - Users	Are users clicking on phishing emails?
Microsoft:2/4 Global Admins Designated	None	Microsoft 365/Office 365	MS 365 Admin Center	Global Admins Designated	Ensure that between two and four global admins are designated
Microsoft:Password Expiration Policy	None	Microsoft 365/Office 365	MS 365 Admin Center	Password Expiration Policy	Ensure the `Password expiration policy` is set to `Set passwords to never expire (recommended)`
Microsoft:Idle Session Timeout	None	Microsoft 365/Office 365	MS 365 Admin Center	Idle Session Timeout	Ensure `Idle session timeout` is set to `3 hours (or less)` for unmanaged devices
Microsoft:Calendar Sharing - External	None	Microsoft 365/Office 365	MS 365 Admin Center	Calendar Sharing - External	Ensure `External sharing` of calendars is not available
Microsoft:Customer Lockbox Enabled	None	Microsoft 365/Office 365	MS 365 Admin Center	Customer Lockbox Enabled	Ensure the customer lockbox feature is enabled
Microsoft:3rd Party Storage Services Retricted	None	Microsoft 365/Office 365	MS 365 Admin Center	3rd Party Storage Services Retricted	Ensure `third-party storage services` are restricted in `Microsoft 365 on the web`
Microsoft:Safelinks for Email	None	Microsoft 365/Office 365	MS 365 Defender	Safelinks for Email	Ensure Safe Links for Office Applications is Enabled
Microsoft:Common Attachment Types	None	Microsoft 365/Office 365	MS 365 Defender	Common Attachment Types	Ensure the Common Attachment Types Filter is enabled
Microsoft:Safe Attachments Policy	None	Microsoft 365/Office 365	MS 365 Defender	Safe Attachments Policy	Ensure Safe Attachments policy is enabled
Microsoft:Safe Attachments for Apps	None	Microsoft 365/Office 365	MS 365 Defender	Safe Attachments for Apps	Ensure Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is Enabled
Microsoft:Spam - Notify Admins	None	Microsoft 365/Office 365	MS 365 Defender	Spam - Notify Admins	Ensure Exchange Online Spam Policies are set to notify administrators
Microsoft:Connection Filter - Allow List	None	Microsoft 365/Office 365	MS 365 Defender	Connection Filter - Allow List	Ensure the connection filter IP allow list is not used
Microsoft:Inbound Spam Policy - Allowed Domains	None	Microsoft 365/Office 365	MS 365 Defender	Inbound Spam Policy - Allowed Domains	Ensure inbound anti-spam policies do not contain allowed domains
Microsoft:Outbound Antispam Limits	None	Microsoft 365/Office 365	MS 365 Defender	Outbound Antispam Limits	Ensure outbound anti-spam message limits are in place
Microsoft:MS 365 Audit Log	None	Microsoft 365/Office 365	MS 365 Pureview	MS 365 Audit Log	Ensure Microsoft 365 audit log search is Enabled
Microsoft:DLP Policies - Enabled	None	Microsoft 365/Office 365	MS 365 Pureview	DLP Policies - Enabled	Ensure DLP policies are enabled
Microsoft:DLP Policies - Enabled for Teams	None	Microsoft 365/Office 365	MS 365 Pureview	DLP Policies - Enabled for Teams	Ensure DLP policies are enabled for Microsoft Teams
Microsoft:IP Label Policies	None	Microsoft 365/Office 365	MS 365 Pureview	IP Label Policies	Ensure Information Protection sensitivity label policies are published

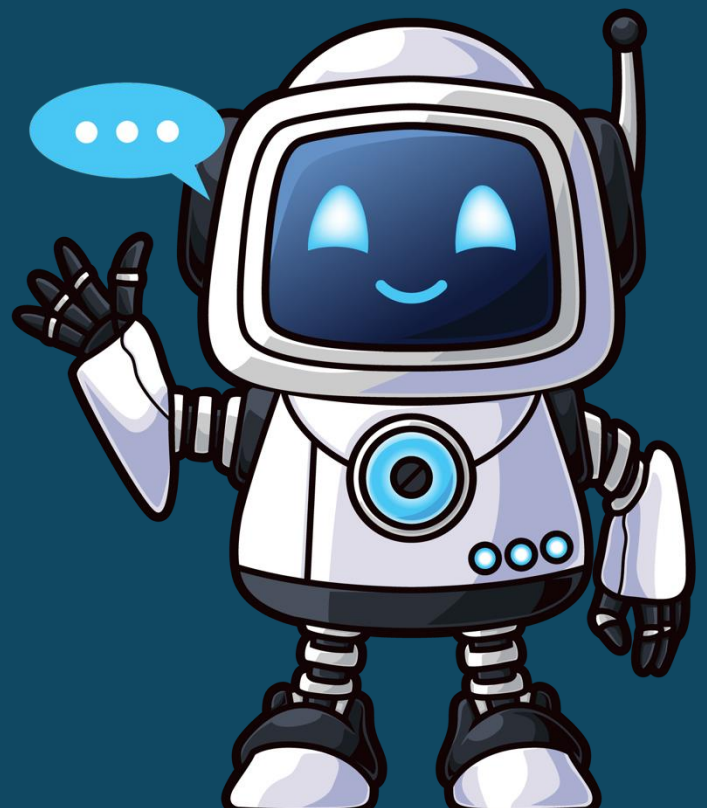
Automation Mapping – Rule to Control (Cont.)

Rules		Mapped Questions in vCIOToolbox Templates			
Rule Name	Base Asset Type	Template	Topic	Question	Questions Text
Microsoft:User Consent - Apps	None	Microsoft 365/Office 365	MS Entra Admin Center	User Consent - Apps	Ensure user consent to apps accessing company data on their behalf is not allowed
Microsoft:MFA - Admins	None	Microsoft 365/Office 365	MS Entra Admin Center	MFA - Admins	Ensure multifactor authentication is enabled for all users in administrative roles
Microsoft:MFA - Users	None	Microsoft 365/Office 365	MS Entra Admin Center	MFA - Users	Ensure multifactor authentication is enabled for all users
Microsoft:Block Legacy Authentication	None	Microsoft 365/Office 365	MS Entra Admin Center	Block Legacy Authentication	Enable Conditional Access policies to block legacy authentication
Microsoft:IP User Risk Policies	None	Microsoft 365/Office 365	MS Entra Admin Center	IP User Risk Policies	Enable Identity Protection user risk policies
Microsoft:IP- Sign-on Risk Policies	None	Microsoft 365/Office 365	MS Entra Admin Center	IP- Sign-on Risk Policies	Enable Identity Protection sign-in risk policies
Microsoft:Self-Service Password	None	Microsoft 365/Office 365	MS Entra Admin Center	Self-Service Password	Ensure `Self service password reset enabled` is set to `All`
Microsoft:Exchange - Audit Disabled	None	Microsoft 365/Office 365	Exchange Admin Center	Exchange - Audit Disabled	Ensure `AuditDisabled` organizationally is set to `False`
Microsoft:Block Mail Forwarding	None	Microsoft 365/Office 365	Exchange Admin Center	Block Mail Forwarding	Ensure all forms of mail forwarding are blocked and/or disabled
Microsoft:Outlook Add-ins	None	Microsoft 365/Office 365	Exchange Admin Center	Outlook Add-ins	Ensure users installing Outlook add-ins is not allowed
Microsoft:Exchange - Moderen Authentication	None	Microsoft 365/Office 365	Exchange Admin Center	Exchange - Moderen Authentication	Ensure modern authentication for Exchange Online is enabled
Microsoft:MailTips	None	Microsoft 365/Office 365	Exchange Admin Center	MailTips	Ensure MailTips are enabled for end users
Microsoft:OWA -Storage Providers Restricted	None	Microsoft 365/Office 365	Exchange Admin Center	OWA -Storage Providers Restricted	Ensure additional storage providers are restricted in Outlook on the web
Microsoft:Modern Authentication - SharePoint	None	Microsoft 365/Office 365	SharePoint Admin Center	Modern Authentication - SharePoint	Ensure modern authentication for SharePoint applications is required
Microsoft:Teams - Anonymous Users Join Meeting	None	Microsoft 365/Office 365	MS Teams Admin Center	ConnecTeams - Anonymous Users Join Meetingtion Filter - Safe List	Ensure anonymous users can`t join a meeting
Microsoft:Teams -Dial-in Callers Start Meeting	None	Microsoft 365/Office 365	MS Teams Admin Center	Teams -Dial-in Callers Start Meeting	Ensure anonymous users and dial-in callers can`t start a meeting
Microsoft:Teams -Dial-in Callers Lobby Bypass	None	Microsoft 365/Office 365	MS Teams Admin Center	Teams -Dial-in Callers Lobby Bypass	Ensure users dialing in can`t bypass the lobby
Microsoft:Teams -Presenters	None	Microsoft 365/Office 365	MS Teams Admin Center	Teams -Presenters	Ensure only organizers and co-organizers can present
Microsoft:Teams -External Participants Control	None	Microsoft 365/Office 365	MS Teams Admin Center	Teams -External Participants Control	Ensure external participants can`t give or request control
Microsoft:Safelinks for Apps	None	Microsoft 365/Office 365	MS 365 Defender	Connection Filter - Safe List	Ensure the connection filter safe list is off
Microsoft:Zero-hour Purge	None	Microsoft 365/Office 365	Connection Filter - Safe List	Zero-hour Purge	Ensure Zero-hour auto purge for Microsoft Teams is on
Microsoft:Anti-Phishing Policy	None	Microsoft 365/Office 365	MS 365 Defender	Anti-Phishing Policy	Ensure that an anti-phishing policy has been created

Automation Mapping – Rule to Control (Cont.)

RulesCybersecurity a		Mapped Questions in vCIOToolbox Templates			
Rule Name	Base Asset Type	Template	Topic	Question	Questions Text
Warranty:Network and Infrastructure	Firewall	Network and Infrastructure	Firewalls	Firewall Warranty	Is the Firewall Device currently Under Warranty? (If NO document end date in comments)
Warranty:Network and Infrastructure	Wireless	Network and Infrastructure	Wireless Access	Under Warranty	Is the Wireless Access Point/Console currently Under Warranty? (If NO document end date in notes)
Warranty:Network and Infrastructure	Switch	Network and Infrastructure	Network Switches	Under Warranty	Is the Network Switch(es) currently under warranty?
End-of-Life:Network and Infrastructure	Firewall	Network and Instrarsturcture	Firewalls	End of Support	Is the Network Appliance (Firewall/Router End of Support?
End-of-Life:Network and Infrastructure	Wireless	Network and Instrarsturcture	Wireless Access	End of Support	Is the Wireless Access Point/Console End of Support?
End-of-Life:Servers	Server/Managed Server	Servers			
Operating System:Servers	Server/Managed Server	Servers	Operating Systems	Windows Operating Systems	Are all servers running currently supported versions of their respective Vendor Operating System?
Warranty:Servers	Server/Managed Server	Servers			
End-of-Life:Workstations	Workstation,Desktop,Laptop	Workstation			
Operating System:Workstations	Workstation,Desktop,Laptop	Workstation	Operating Systems	Windows Professional	Are all Windows Desktop Operating systems installed 11 Professional?
Warranty:Workstations	Workstation,Desktop,Laptop	Workstation	Physical Harware	Workstations - Warranty	Are all workstations and laptops operating under current warranties?
Vulnerability Scans	None	Cybersecurity and Risk	Vulnerability	Vulnerability Monitoring	The network is monitored to detect potential cybersecurity vulnerabilities and threats

vCIO TOOLBOX



Need Support?

Email the support desk:

support@vciotoolbox.com

or

Contract your Partner Success Manager to schedule an Automation conference call