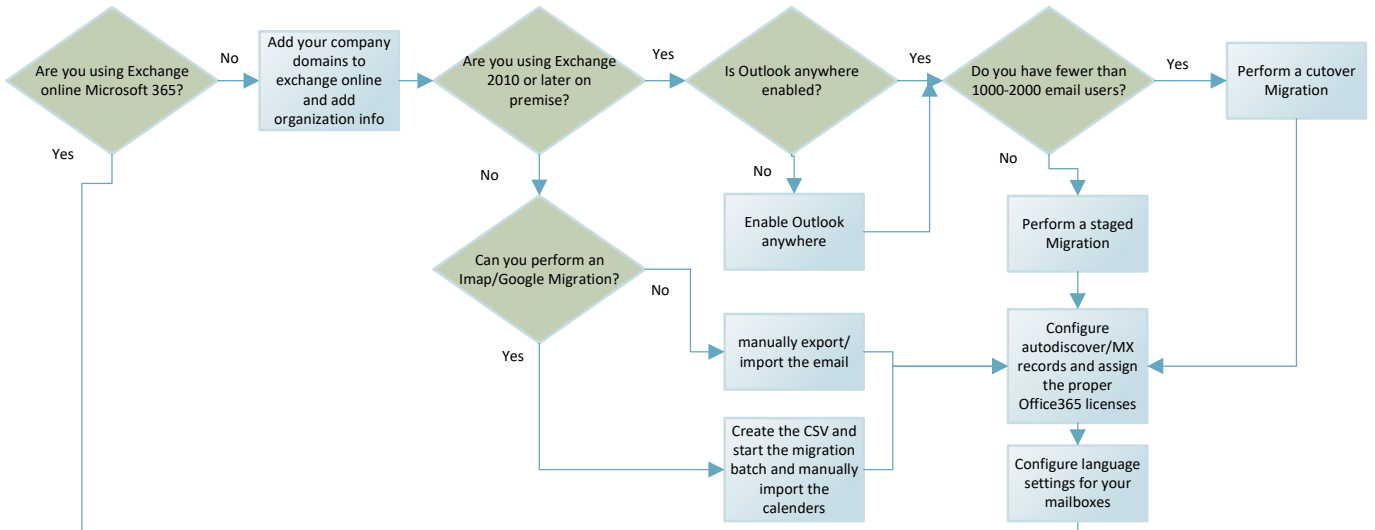
Transformation to a modern zero trust workplace V2.42

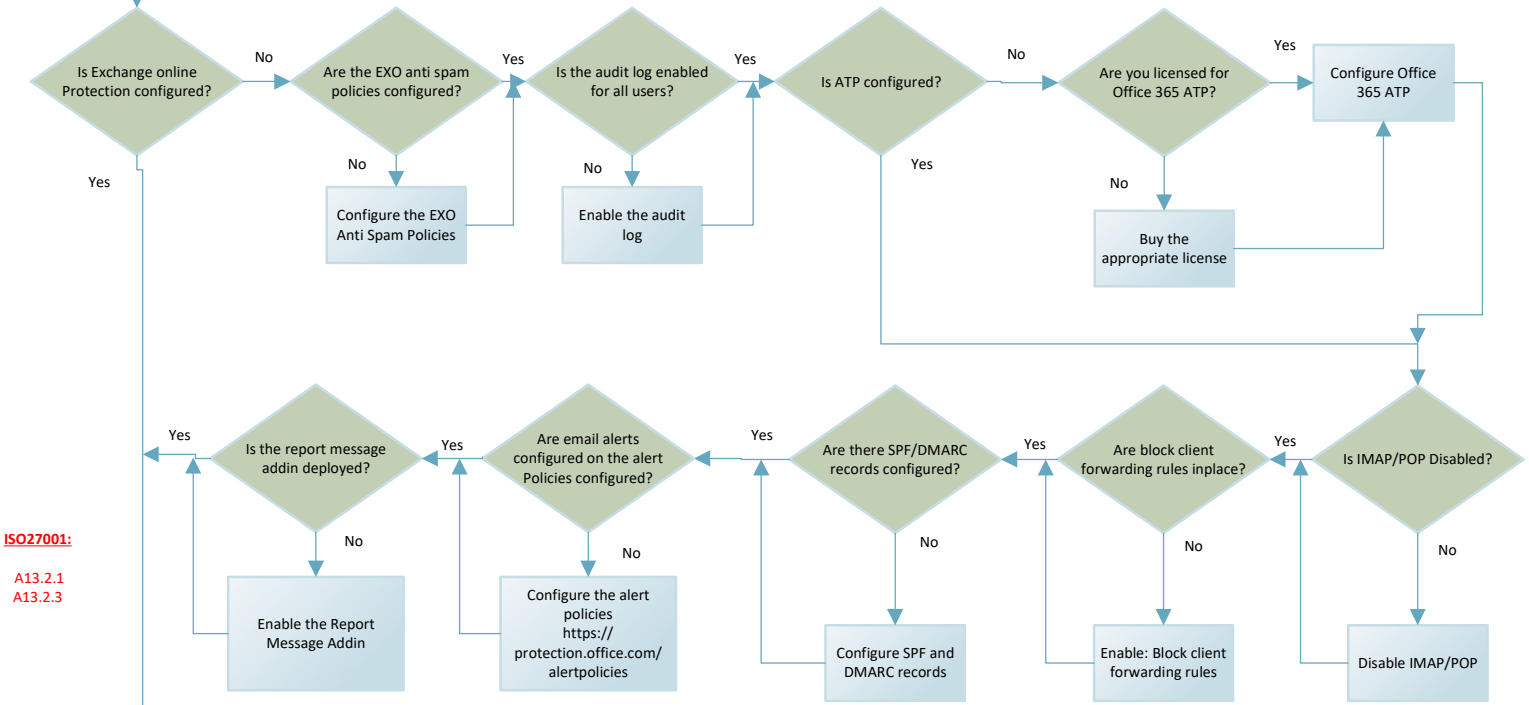
Exchange Migration Paths



Version 2.41

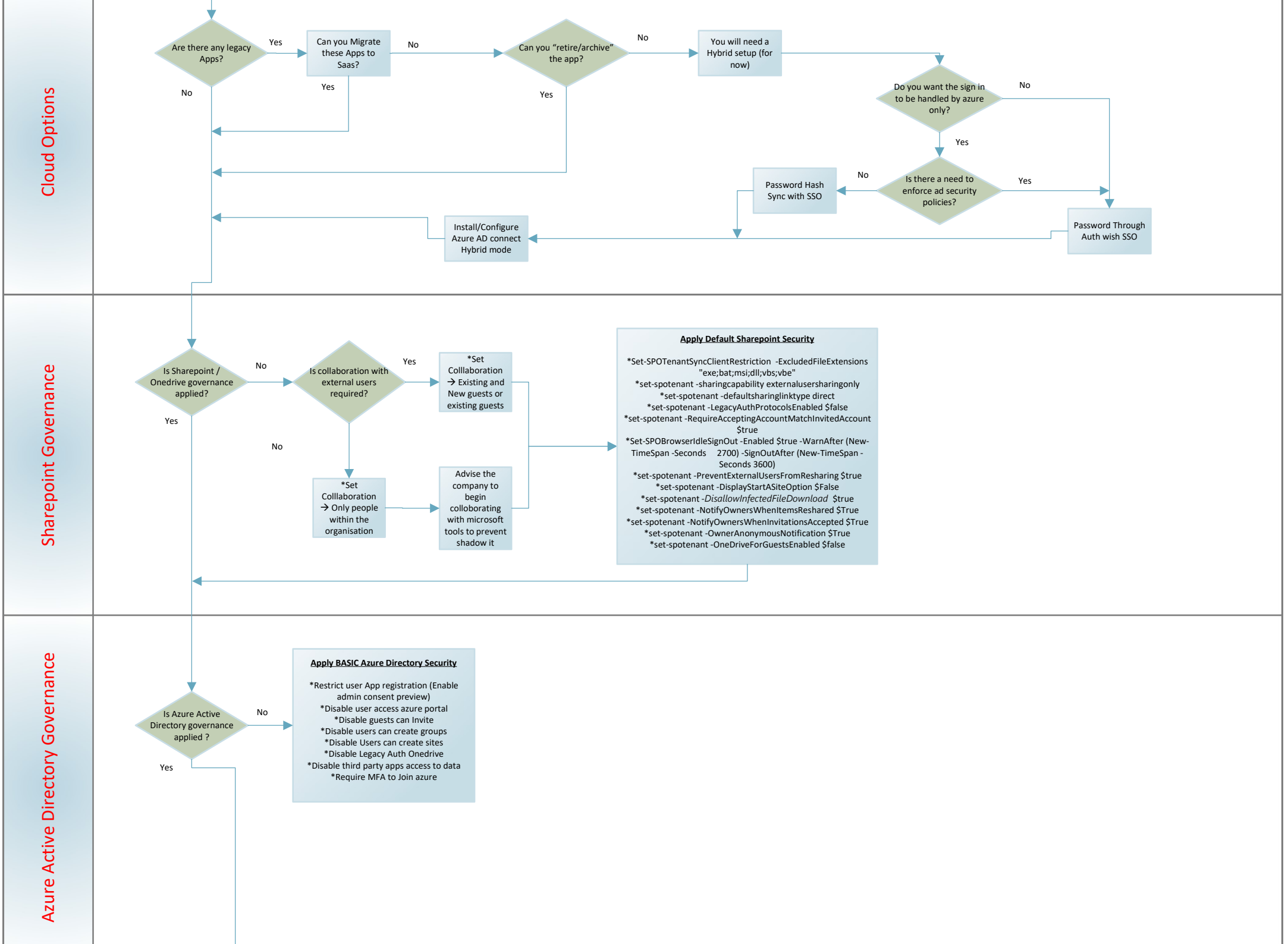
*2.0 Added: Applications
*2.1 Added Printing
*2.2 Added License groups
2.3 Added IOS Mac ATP
*2.4 Added White Glove TPM Attestion
*2.41 added Mp remediation
*2.42 Added report message addin

Exchange Online Security

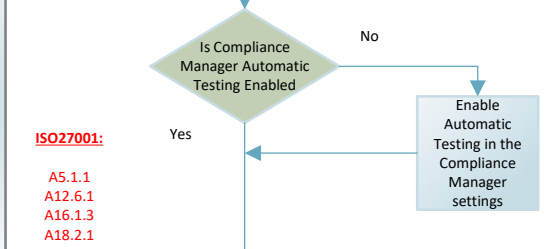


ISO27001:

A13.2.1
A13.2.3


Cloud Options
Are there any legacy Apps?
Yes
No
Can you Migrate these Apps to Saas?
Yes
No
Can you "retire/archive" the app?
Yes
No
You will need a Hybrid setup (for now)
Do you want the sign in to be handled by azure only?
Yes
No
Is there a need to enforce ad security policies?
Yes
No
Password Through Auth wish SSO
Password Hash Sync with SSO
Install/Configure Azure AD connect Hybrid mode
Sharepoint Governance
Is Sharepoint / Onedrive governance applied?
Yes
No
Is collaboration with external users required?
Yes
No
*Set Colllaboration → Existing and New guests or existing guests
*Set Colllaboration → Only people within the organisation
Advise the company to begin colloborating with microsoft tools to prevent shadow it
Apply Default Sharepoint Security
*Set-SPOTenantSyncClientRestriction -ExcludedFileExtensions "exe;bat;msi;dll;vbs;vbe"
*set-spotenant -sharingcapability externalusersharingonly
*set-spotenant -defaultsharinglinktype direct
*set-spotenant -LegacyAuthProtocolsEnabled $false
*set-spotenant -RequireAcceptingAccountMatchInvitedAccount $true
*Set-SPOBrowserIdleSignOut -Enabled $true -WarnAfter (New-TimeSpan -Seconds 2700) -SignOutAfter (New-TimeSpan -Seconds 3600)
*set-spotenant -PreventExternalUsersFromResharing $true
*set-spotenant -DisplayStartASiteOption $False
*set-spotenant -DisallowInfectedFileDownload $true
*set-spotenant -NotifyOwnersWhenItemsReshared $True
*set-spotenant -NotifyOwnersWhenInvitationsAccepted $True
*set-spotenant -OwnerAnonymousNotification $True
*set-spotenant -OneDriveForGuestsEnabled $false
Azure Active Directory Governance
Is Azure Active Directory governance applied ?
Yes
No
Apply BASIC Azure Directory Security
*Restrict user App registration (Enable admin consent preview)
*Disable user access azure portal
*Disable guests can Invite
*Disable users can create groups
*Disable Users can create sites
*Disable Legacy Auth Onedrive
*Disable third party apps access to data
*Require MFA to Join azure

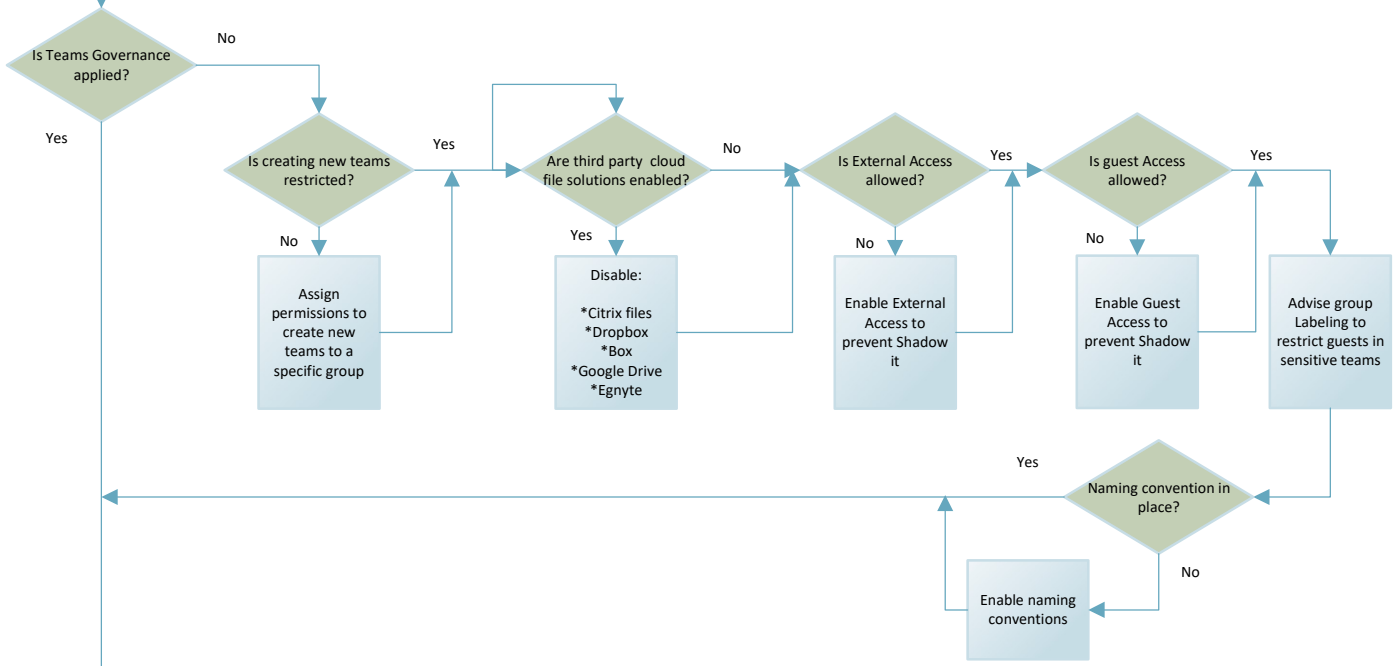
Compliance Score



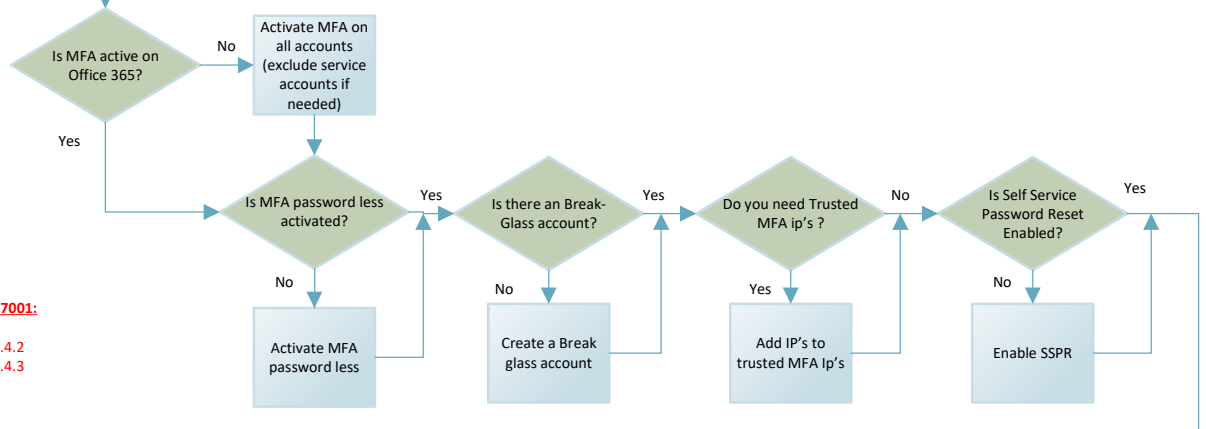
ISO27001:

A5.1.1
A12.6.1
A16.1.3
A18.2.1

Teams Governance



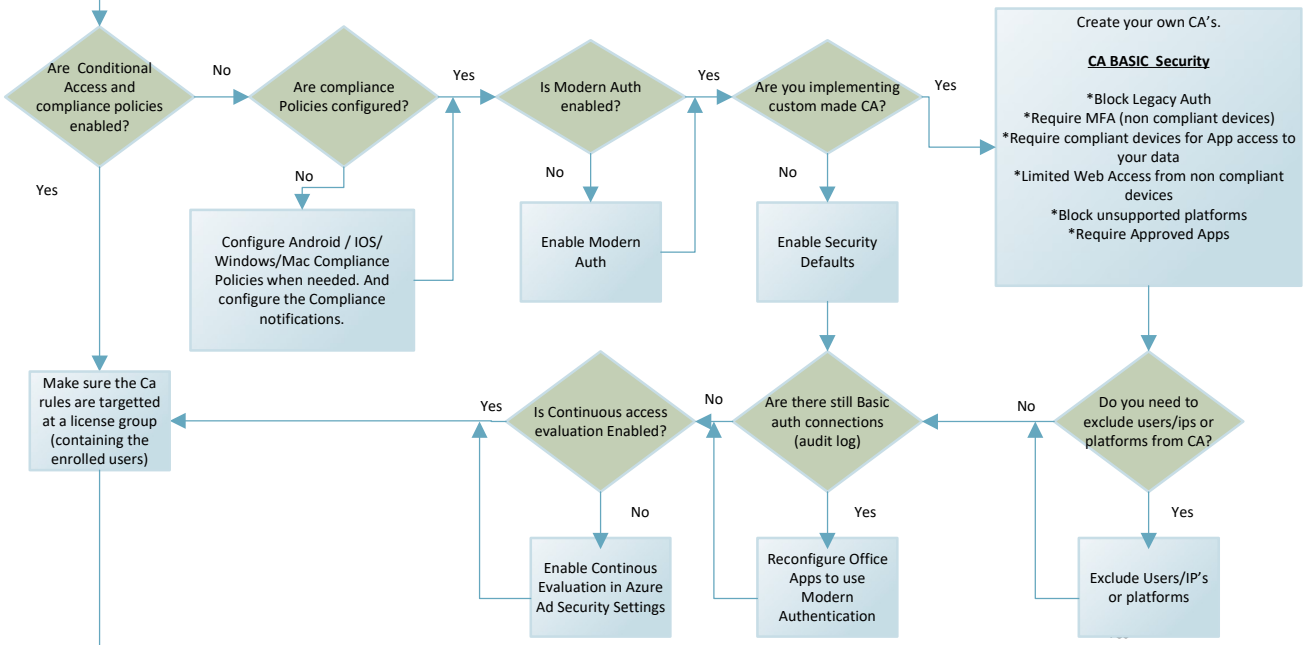
MFA Cloud Options



ISO27001:

A9.4.2
A9.4.3

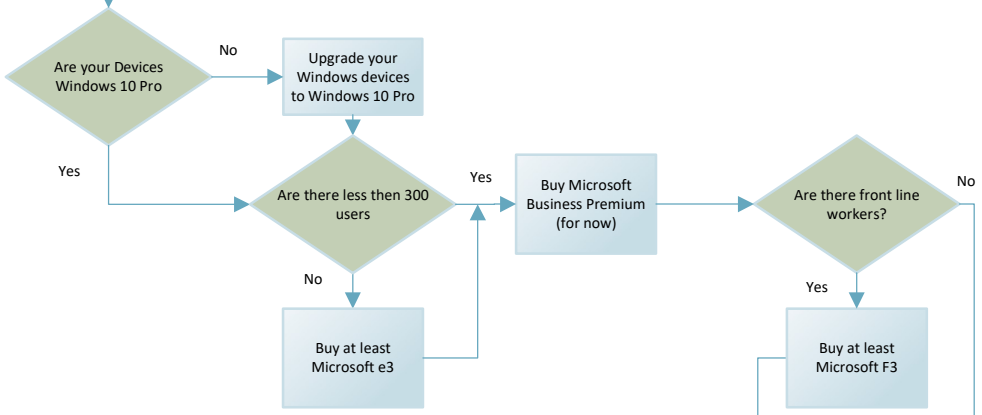
Conditional Access



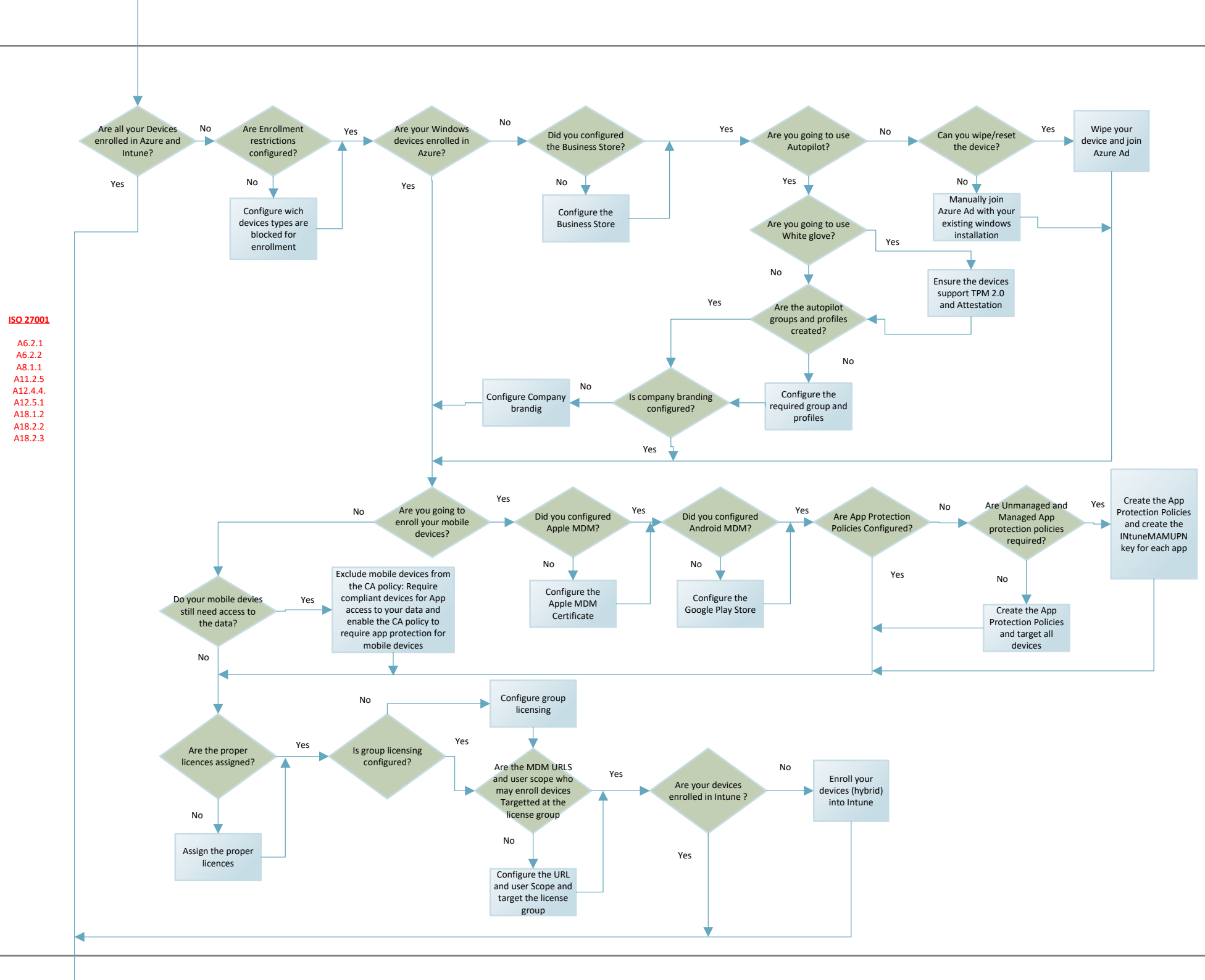
ISO27001:

A5.1.1
A6.2.2
A9.1.1
A9.1.2

Azure Ad Windows and License Requirements



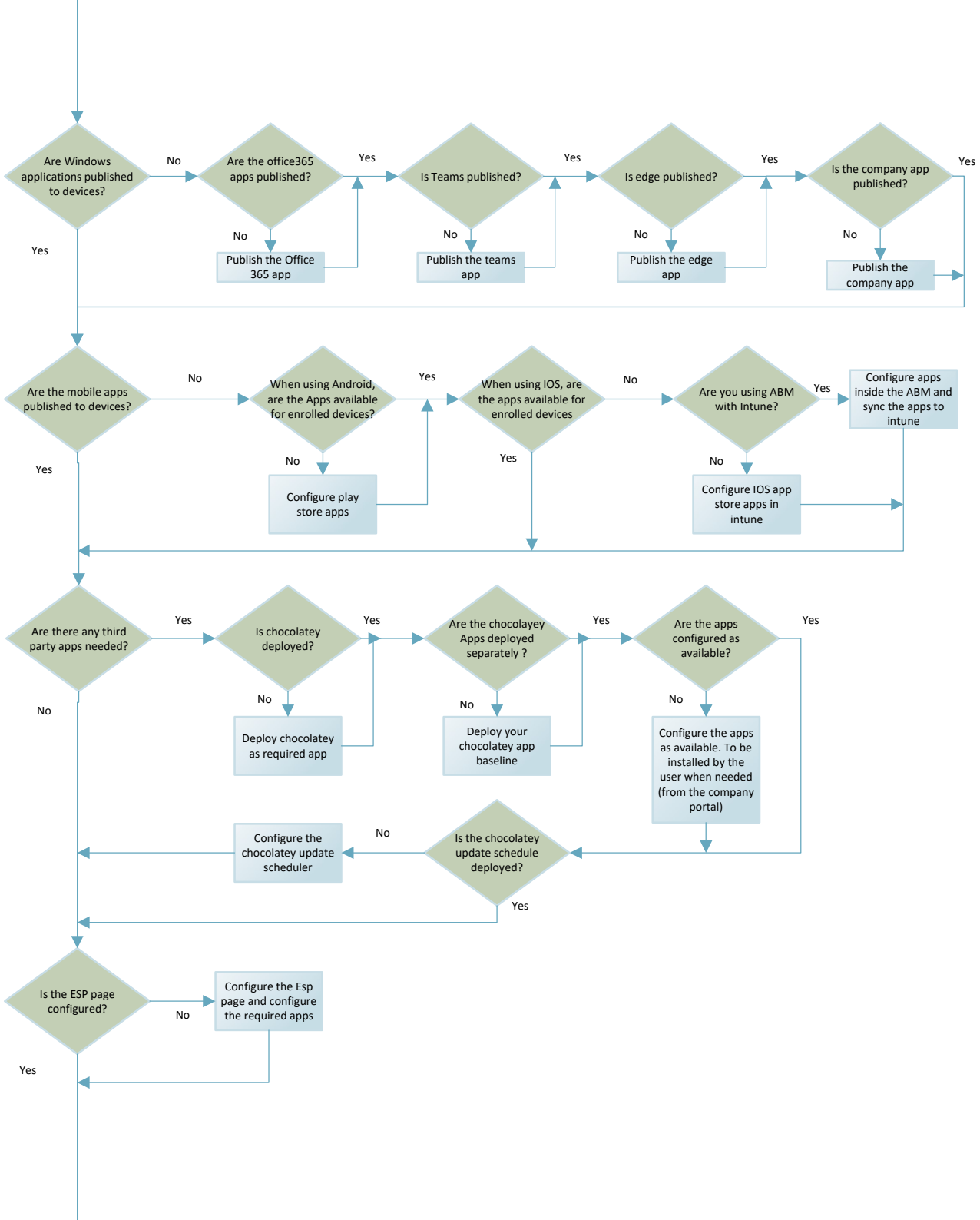
Device Enrollment



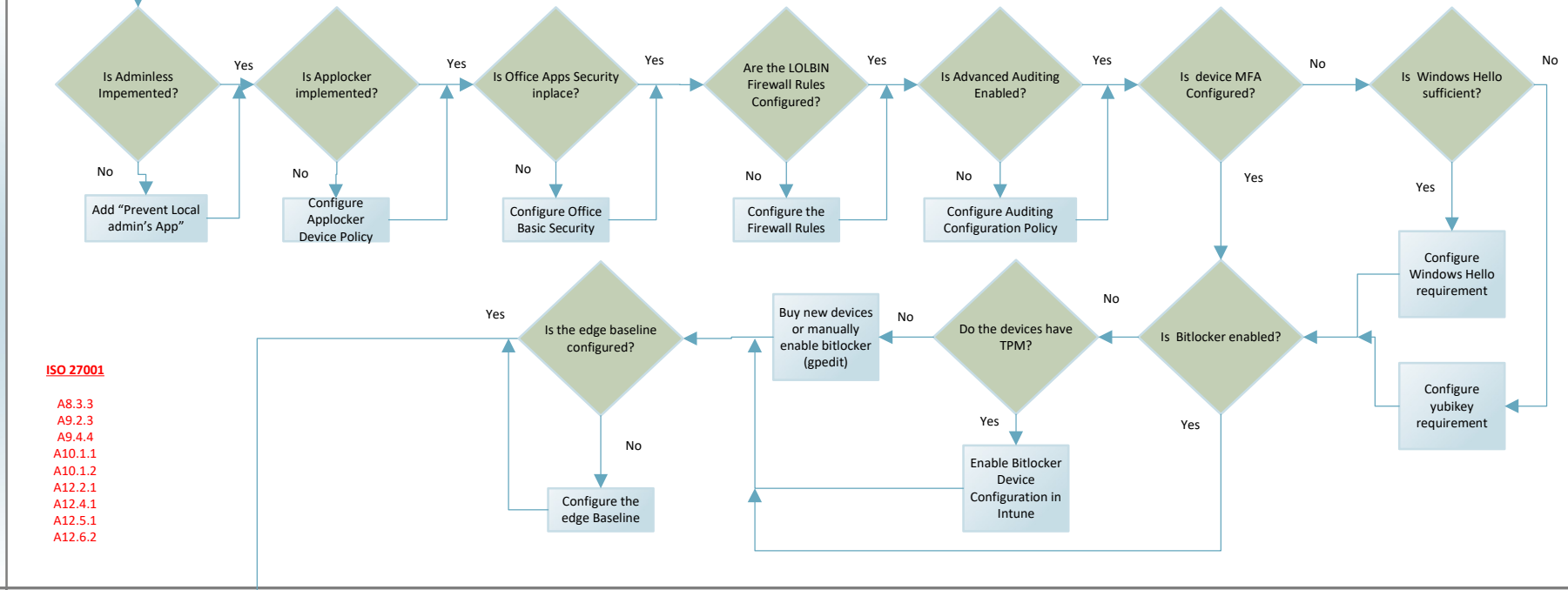
ISO 27001

A6.2.1
A6.2.2
A8.1.1
A11.2.5
A12.4.4.
A12.5.1
A18.1.2
A18.2.2
A18.2.3

Applications



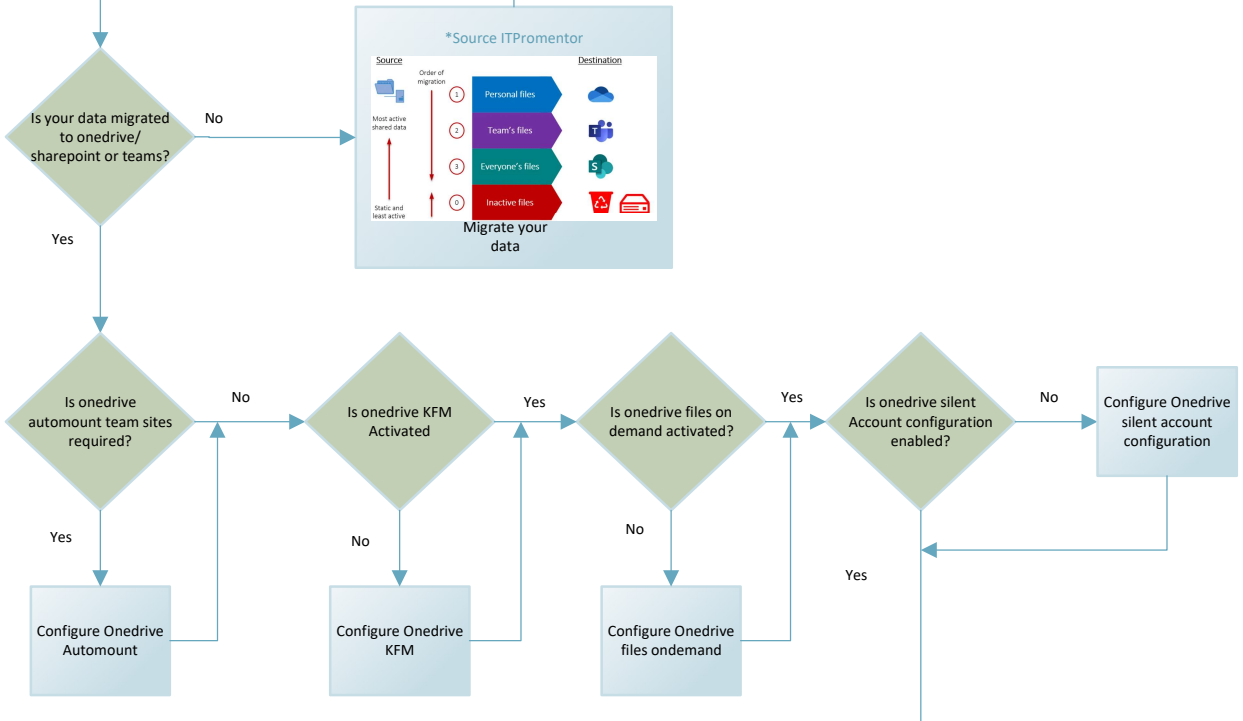
Intune Device Security Configuration



ISO 27001

A8.3.3
A9.2.3
A9.4.4
A10.1.1
A10.1.2
A12.2.1
A12.4.1
A12.5.1
A12.6.2

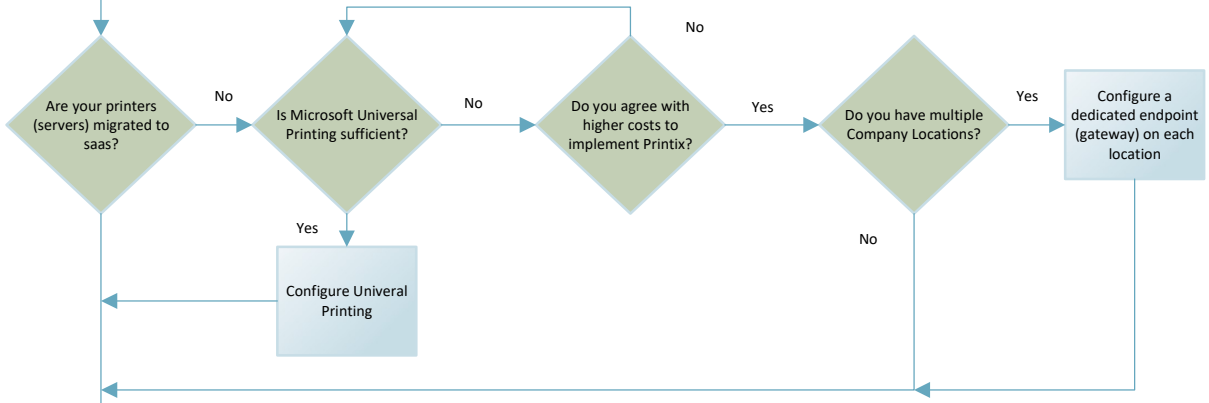
Data Migration



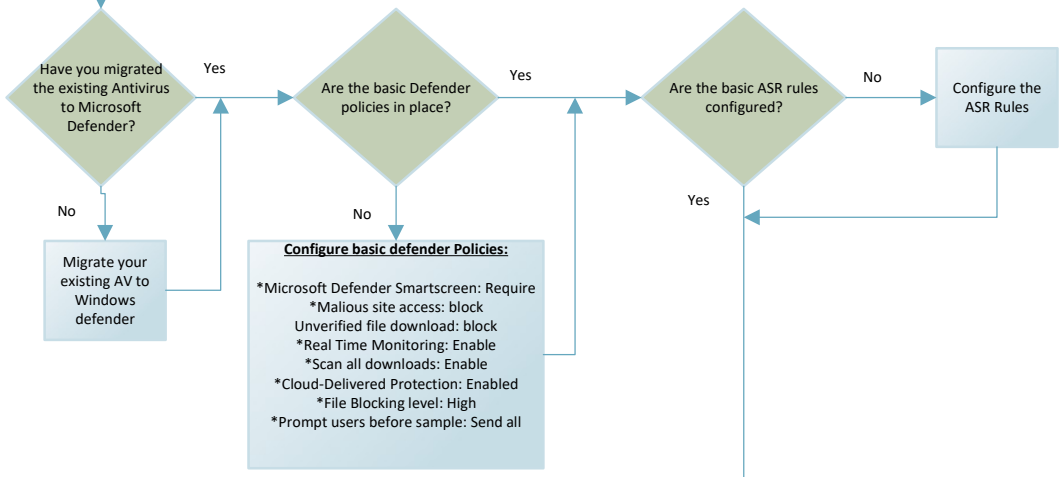
ISO 27001

A12.3.1
A13.2.2

Printer Migration

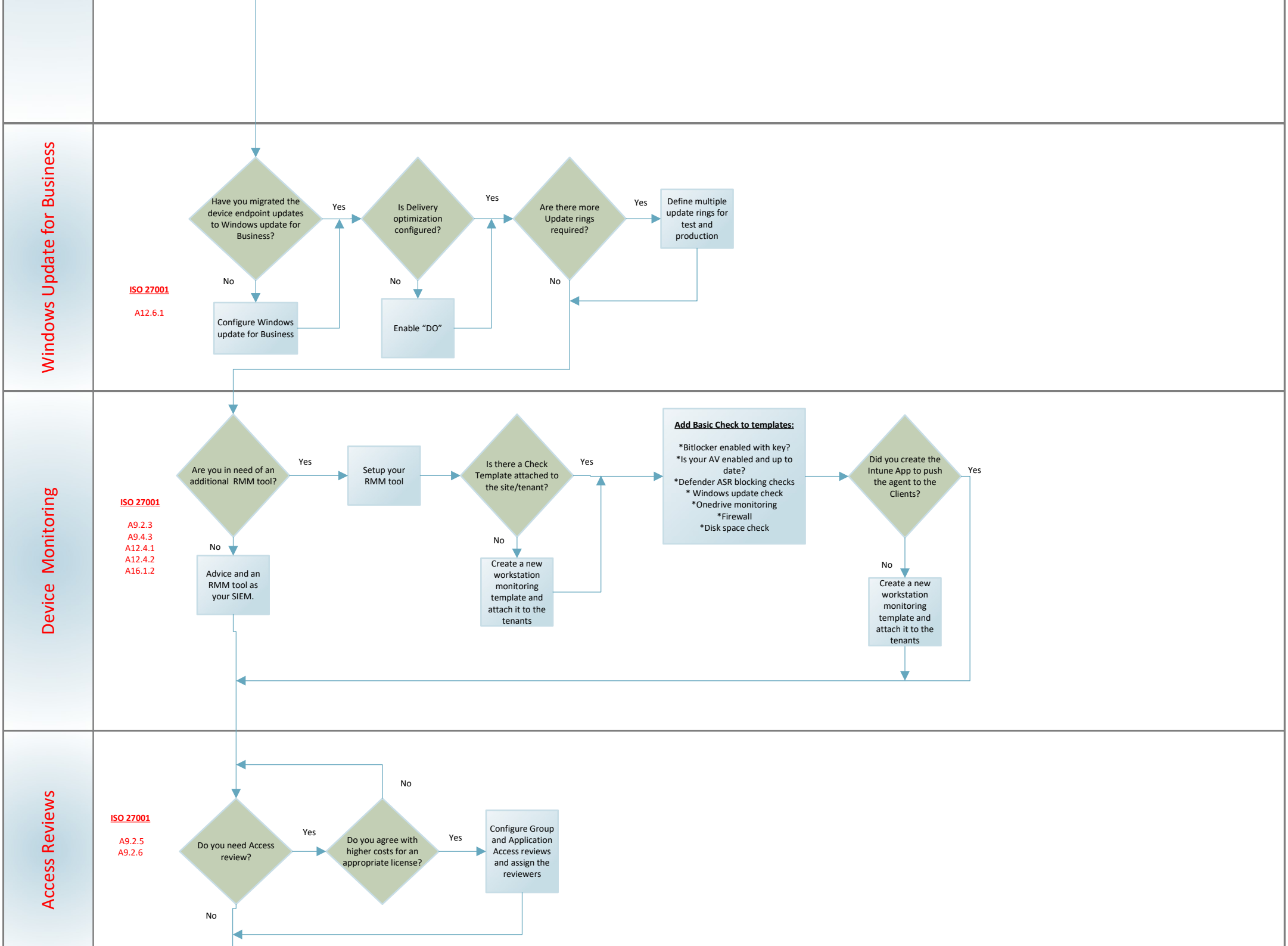


Antivirus Migration

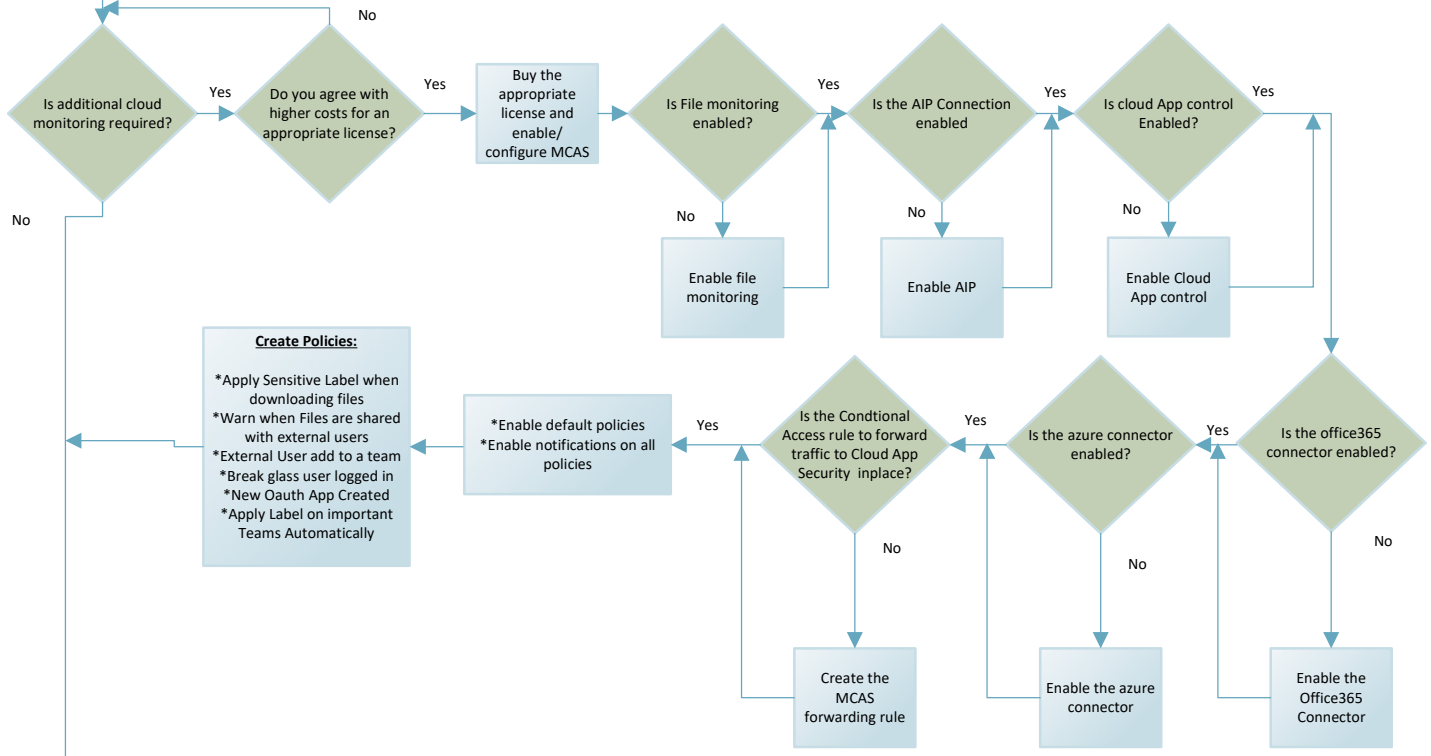


ISO 27001

A12.2.1
A13.1.1
A13.1.2


Windows Update for Business
Have you migrated the device endpoint updates to Windows update for Business?
Yes
Is Delivery optimization configured?
Yes
Are there more Update rings required?
Yes
Define multiple update rings for test and production
No
Configure Windows update for Business
No
Enable "DO"
No
ISO 27001
A12.6.1
Device Monitoring
Are you in need of an additional RMM tool?
Yes
Setup your RMM tool
Is there a Check Template attached to the site/tenant?
Yes
Add Basic Check to templates:
*Bitlocker enabled with key?
*Is your AV enabled and up to date?
*Defender ASR blocking checks
* Windows update check
*Onedrive monitoring
*Firewall
*Disk space check
Did you create the Intune App to push the agent to the Clients?
Yes
No
Advice and an RMM tool as your SIEM.
No
Create a new workstation monitoring template and attach it to the tenants
No
Create a new workstation monitoring template and attach it to the tenants
ISO 27001
A9.2.3
A9.4.3
A12.4.1
A12.4.2
A16.1.2
Access Reviews
No
Do you need Access review?
Yes
Do you agree with higher costs for an appropriate license?
Yes
Configure Group and Application Access reviews and assign the reviewers
No
ISO 27001
A9.2.5
A9.2.6

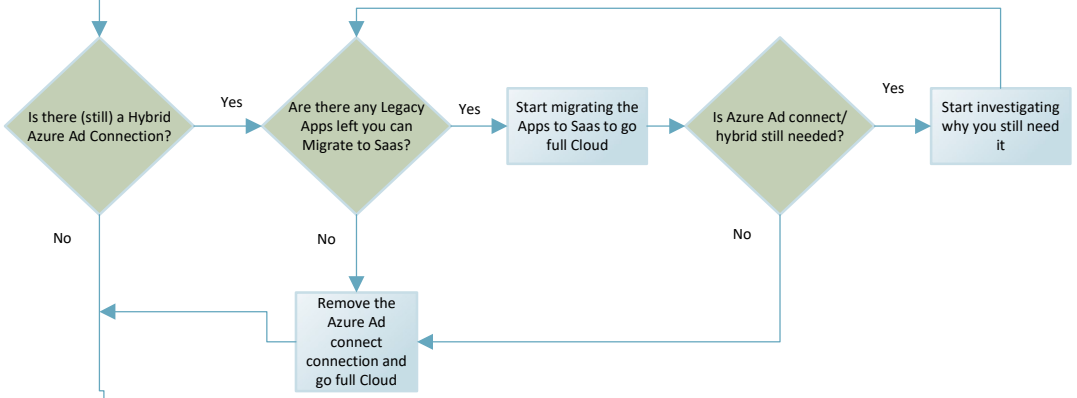
Microsoft Cloud App Security



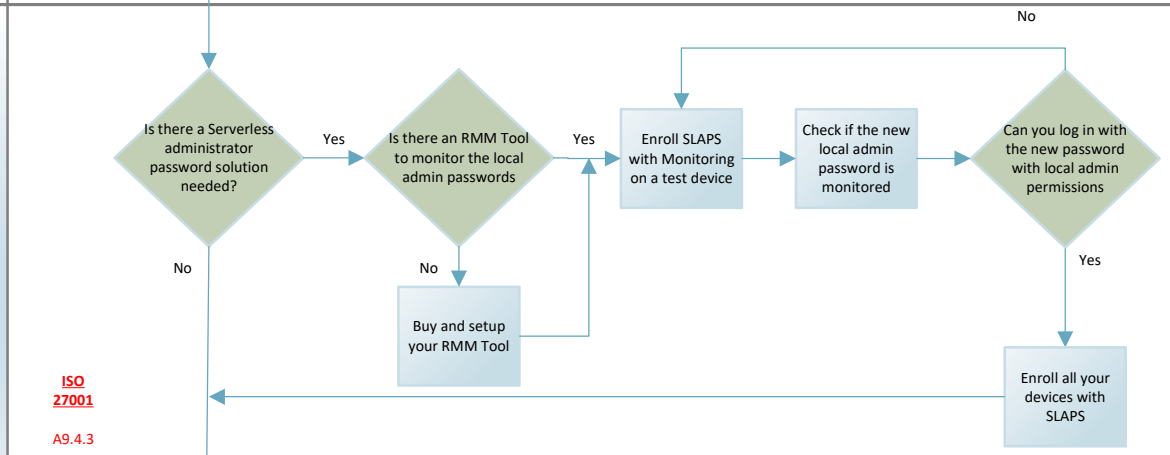
ISO 27001

A12.4.1
A12.4.2
A12.4.3
A.16.1.2
A.16.1.3
A16.1.5

Go Full Cloud?



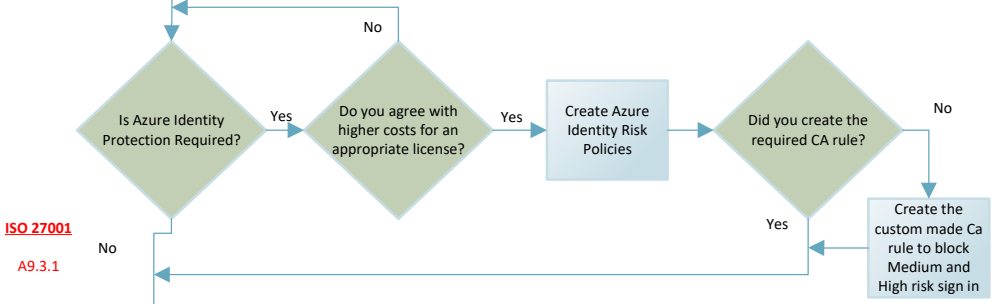
Slaps



ISO 27001

A9.4.3

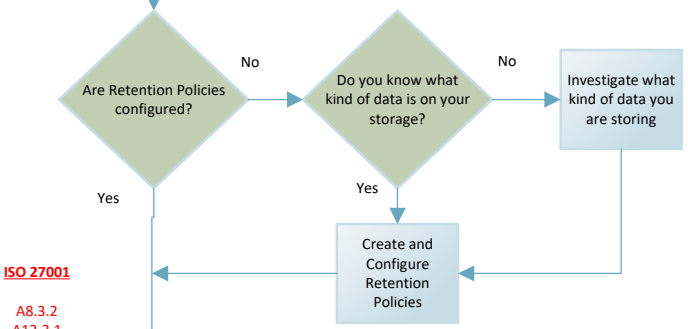
Azure Identity Protection



ISO 27001

A9.3.1

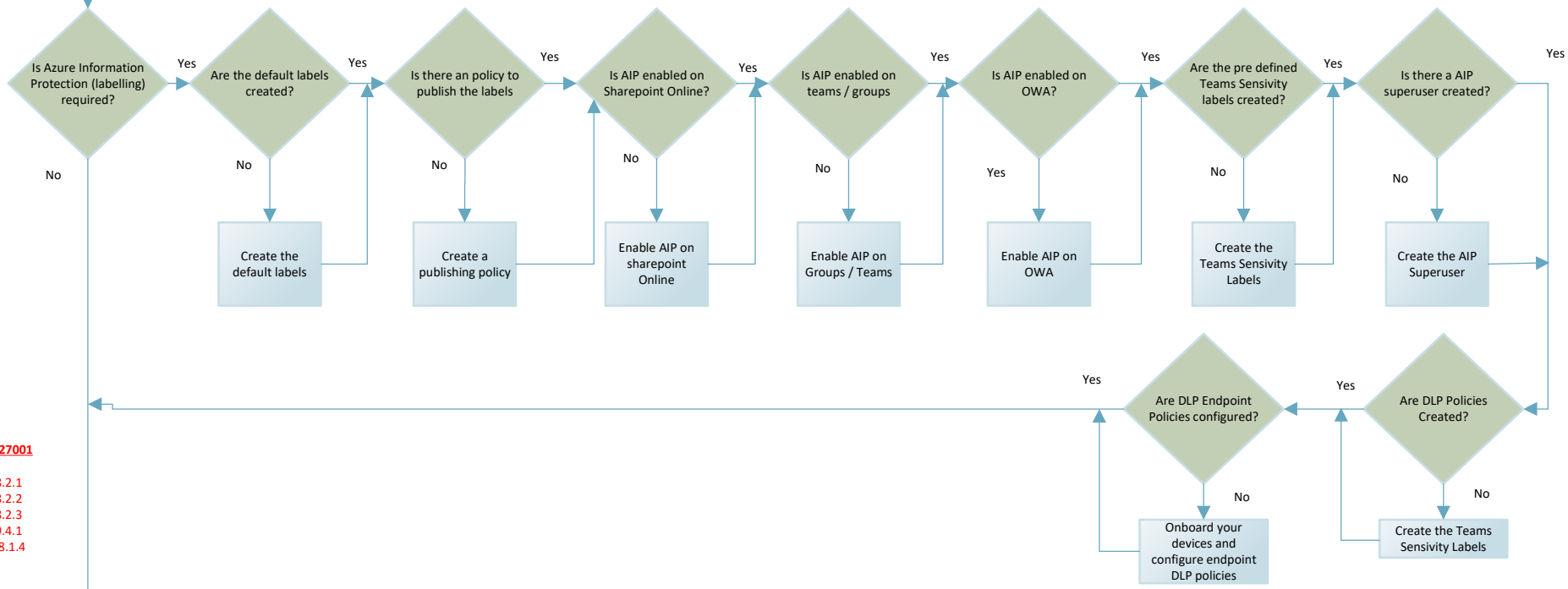
Retention Policies



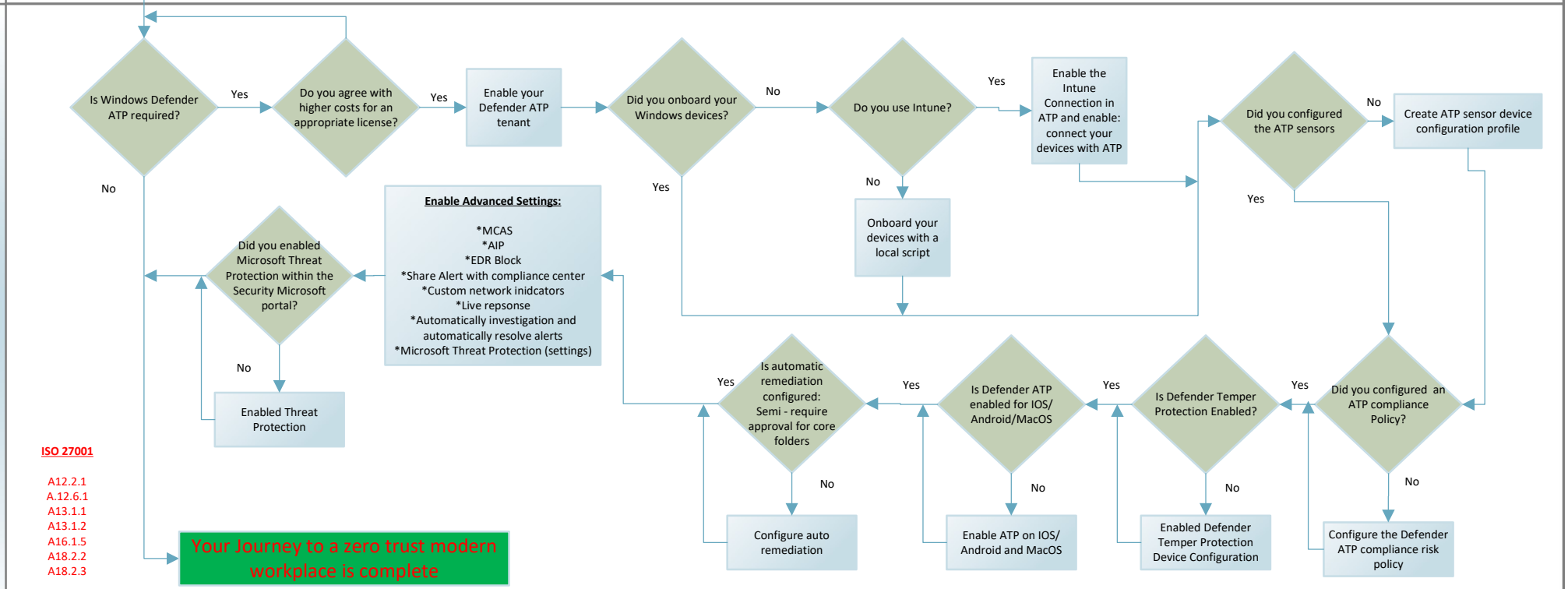
ISO 27001

A8.3.2
A12.3.1

Azure Information Protection



ISO 27001

A8.2.1
A8.2.2
A8.2.3
A9.4.1
A18.1.4

Windows Defender ATP