Omgevingsdienst
Veluwe

Bijlage 9: Assessment op CIS4.0 controls en andere criteria

deze bijlage bevat een Overview van alle controls waarop de Tenant is getoetst (pagina 2 t/m 7).
Daarna zijn, per onderwerp en per control, de assessmentresultaten weergegeven (Configured setting and remarks) en de daaropvolgende acties (Actions and Decisions)
De informatie in de kolom `status' wordt uigelegd in de legenda

App	Categorie	Test	Control
Overwiew pagina 1 van 6 Microsoft 365 Admin Center	Microsoft 365 Admin Center users	Ensure Administrative accounts are separate and cloud-only	*CIS v4.0*
		Ensure administrative accounts ause licenses with a reduced application footprint	
		Ensure two emergency access accounts have been defined	
		Ensure that between two and four global admins are designated	
		Ensure guest users are reviewed and disabled	*other*
	Microsoft 365 Admin Center Accounts and Authenticating	Ensure Microsoft 365 users roles have les than 10 admins	*other*
		Ensure Microsoft 365 user have strong password requirements configured	
		Ensure self-service password reset is enabled	
		Ensure that Microsoft 365 passwords are not set to expire	
		Ensure Microsoft 365 exchange inline modern authentication is used	
		Ensure Microsoft 365 exchange online Privileged Access Management is used	
	Microsoft 365 Admin Center Auditing	Ensure Enterprise Applications Role Assignements are reviewd weekly	*other*
	Microsoft 365 Admin Center Teams and Groups	Ensure that only organizationally managed-approved public groups exist	*CIS v4.0*
		Ensure sign-in to shared mailboxes is blocked	*CIS v4.0*
	Microsoft 365 Admin Center Settings	Ensure the password expiration policy is set to Set passwords to never expire	*CIS v4.0*
		Ensure idle session timeout is set to 3 hours or less for unmanaged devices	
		Ensure calendar details sharing with external users is disabled	
		Ensure user owned apps and services is restricted	
		Ensure internal phishing protection for forms is enabled	
		Ensure the customer lockbox feature is enabled	
		Ensure third-party storage services are restricted in Microsoft 365 on the web	
		Ensure that sways cannot be share with people outside of your organization	

App	Categorie	Test	Control
Overwiew pagina 2 van 6 Microsoft 365 Defender	Microsoft 365 Defender Email and Collaboration	Ensure Safe Links for Office Applications is enabled	CIS v4.0
		Ensure the Common Attachment Types	
		Ensure notifications for internal users sending malware is Enabled	
		Ensure Safe Attachments policy is enabled	
		Ensure Exchange Online Spam Policies are set correctly	
		Ensure that an anti-phising policy has been created	
		Ensure that SPF records are published for all Exchange Domains	
		Ensure No Domains with SPF soft fail are configured	other
		Ensure that DKIM is enabled for all Exhange Online Domains	CIS v4.0
		Ensure DMARC Records for all Exchange Online Domains are published	
		Ensure the spoofed domains are reviewed and actioned	other
		Ensure the restricted entities are reviewed and actioned	
		Ensure all security threats in the Threat protection status report are reviewed and actioned	
		Ensure comprehensive attachment filtering is applied	CIS v4.0
		Ensure the connection filter allow list is not used	
		Ensure the connection filter safe list is off	
		Ensure inbpound anti-spam policies do not contain allowed domains	
	Microsoft 365 Defender Audit	Ensure the Account Provisioning Activity report is reviewed and actioned	other
		Ensure non-global administrator role group assignments are reviewed and actioned	other
	Microsoft 365 Defender Settings	Ensure Priority account protection is enabled and configured	CIS v4.0
		Ensure Priority accounts have Strict protection presets applied	
		Ensure Microsoft Defender for Cloud Apps is enabled	
		Ensure Zero-hour auto purge for Microsoft Teams is on	
Purview	Microsoft 365 Purview Audit	Ensure Microsoft 365 audit log search is enabled	CIS v4.0
		Ensure role group changes are reviewed and actioned	other
	Microsoft 365 Purview - Data Loss Protection	Ensure DLP policies are enabled	CIS v4.0
		Ensure DLP policies are enabled for Microsoft Teams	
		Ensure DLP policy are enabled for Microsoft OneDrive	other
		Ensure DLP policy is configured for Microsoft SharePoint	
		Ensure Custom Anti-Malware policy is present	
		Ensure Custom Anti-Phishing policy is present	
		Ensure Custom DLP policy are present	
		Ensure Custom DLP sensitive information types are defined	
	Microsoft 365 Purview Information Protection	Ensure SharePoint Online Information Protection are set up and used	CIS v4.0

App	Categorie	Test	Control
Overwiew pagina 3 van 6 Microsoft 365 Entra ID	Microsoft 365 Entra ID admin center - Overview	Ensure Security Defaults is disabled on Azure Active Directory	*CIS v4.0*
	Microsoft 365 Entra ID admin center - Users	Ensure Per-user MFA is disabled Ensure third party integrated applications are not allowed Ensure Restrict non-admin users from creating tenants is set to Yes Ensure Restrict access to the Azure AD administration portal is set to Yes Ensure the option to remain signed in is hidden Ensure LinkedIn account connections is disabled Ensure access to the Entra admin center is restricted	*CIS v4.0*
	Microsoft 365 Entra ID admin center - Groups	Ensure a dynamic grop for guest users is created	*CIS v4.0*
	Microsoft 365 Entra ID admin center - Applications	Ensure the Application Usage report is reviewed and actioned	*other*
		Ensure user consent to apps accessing company data on their behalf is not allowed Ensure that guest user access is restricted Ensure guest user invitations are limited to the Guest Inviter role	*CIS v4.0*
	Microsoft 365 Entra ID admin center - External Identies	Ensure that collaboration invitations are sent to allowed domains only	*CIS v4.0*
	Microsoft 365 Entra ID admin center - Hybrid Management	Ensure that password hash sync is enabled for hybrid deployments	*CIS v4.0*
	Microsoft 365 Entra ID admin center - Conditional Access	Ensure MFA is enabled for all users in administrative roles Enusre MFA is enabled for all users Enable Conditional Access policies to block legacy authentication Ensure Sign-in frequency is enabled and browser sessions are not presistent for administrative users Ensure Phishing-resistant MFA strength is required for administrators Enable Azure AD Identity Protection user risk policies Enable Azure AD Identity Protection sign-in riks policies Ensure admin center access is limited to administrative roles Enusre sign-in risk is blocked for medium and high risk Ensure a managed device is required for authentication Ensure a managed device is required for MFA registration	*CIS v4.0*
	Microsoft 365 Entra ID admin center - Authentication Methods	Ensure Microsoft Authenticator is configured to protect agains MFA fatigue Ensure custom banned passwords lists are used Ensure that password protection is enabled for Active Directory	*CIS v4.0*
	Microsoft 365 Entra ID admin center - Password Reset	Ensure self-service password reset enabled is set to All	*CIS v4.0*
		Ensure the self-service password reset activity report is reviewed and actioned	*other*
	Microsoft 365 Entra ID admin center - Risk Activities	Ensure the Azure AD Risky sign-ins report is reviewed at least weekly	*CIS v4.0*
	Microsoft 365 Entra ID admin center - Governance	Use Just-in-Time privileged access to Microsoft 365 roles	*other*
		Ensure Privileged Identity Management is used to manage roles Ensure Access reviews for Guest Users are configured Ensure Access reviews for high privileged Azure AD roles are configured Ensure approval is required for Global Administrator role activation	*CIS v4.0*

App	Categorie	Test	Control
Overwiew pagina 4 van 6 Microsoft 365 Exchange Online	Microsoft 365 Exchange Online admin center - Audit	Ensure AuditDisabled organizationally is set to False	CIS v4.0
		Ensure mailbox auditing for E3 users is Enabled	
		Ensure mailbox auditing for E5 users is Enabled	
		Ensure AuditBypassEnabled is not enabled on mailboxes	
		Ensure Admin Auditing is Enabled	other
		Ensure Unified Audititing is Enabled	
	Microsoft 365 Echange Online admin center - Mailflow	Ensure all forms of mail forwarding are blocked and-or disabled	CIS v4.0
		Ensure mail transport rules do not whitelist specific domains	
		Ensure Tagging is enabled for External Emails	
		Ensure Tagging does not allow specific domains	
		Ensure Transport Rules to Block Exchange Auto-Forwarding is configured	other
		Ensure Do Not Bypass the Safe Attachments Filter is not configured	
		Ensure Do Not Bypass the Safe Links Feature is not configured	
		Ensure Exchange Online Legacy Authentication is Enabled	
		Ensure Transport Rules to Block Executable Attachments are configured	
		Ensure Malware Filter Policies Alert for Internal Users Sending Malware is configured	
		Ensure Safe Attachments is Enabled	
		Ensure Safe Links is Enabled	
		Ensure Safe Links Click-Through is Not Allowed	
		Ensure Safe Links Flags Links in Real Time	
		Ensure SMTP Authentication is disabled for all users	
		Ensure mail transport rules do not forward email to external domains	
		Ensure automatic forwarding options are disabled	
		Ensure the Client Rules Forwarding Block is enabled	
		Ensure the Advanced Threat Protection Safe Links policy is enabled	
		Ensure the Advanced Threat Protection Safe Attachments policy is enabled	
		Enesure that an anti-phising policy is configured	
		Ensure all member users are MFA capable	CIS v4.0
		Ensure weak authentication methods are disabled	
		Ensure email from external senders is identified	
	Microsoft 365 Exchange Online admin center - Roles	Ensure users installing Outlook add-ins is not allowed	CIS v4.0
	Microsoft 365 Exchange Onling admin center - Reports	Ensure mail forwarding rules are reviewed and actioned	other
		Ensure the Malware Detections report is reviewed at least weekly	
		Ensure Microsoft 365 Deleted Mailboxes are identified and reviewed	
		Ensure Microsoft 365 Hidden Mailboxes are identified	
		Ensure Exchange Mailboxes with Full Access Delegates are reported and reviewed	
		Ensure Echange Mailboxes with Send As Delegates are reported and reviewed	
		Ensure Exchange Mailboxes with Send On Behalf Of Delegates are reported and reviewed	
		Ensure Microsoft 365 Exchange Online Admin access attempts are reported and reviewed	
	Microsoft 365 Excange Online admin center - Settings	Ensure modern authentication for Exchange Online is enabled	CIS v4.0
		Ensure MailTips are enabled for end users	
		Ensure external storage providers available in Outlook on the Web are restricted	
		Ensure Always Deliver Messages From These Senders for specific IP and Domain are not configured	other

App	Categorie	Test	Control
Overwiew pagina 5 van 6 Microsoft 365 SharePoint Online	Microsoft 365 SharePoint Online admin center - Settings	Ensure modern authentication for SharePoint Online applications is required Ensure Sharepoint Online and OneDrive intergration with Entra ID B2B is enabled Ensure SharePoint Online external content sharing is restricted Ensure OneDrive content sharing is restricted Ensure that SharePoint Online guest users cannot share item they don't own Ensure link sharing is restricted in SharePoint Online and OneDrive Ensure external sharing is restricted by security group Ensure reathentication with verification code is restricted Ensure guest access to a site or OneDrive will expire automatically Ensure the SharePoint default sharing link permission is set	*CIS v4.0*
		Ensure sharing is being white- or blacklisted on domain basis	*other*
		Ensure Microsoft 365 SharePoint Online infected files are disallowed for download Block OneDrive for Business sync from unmanaged devices Ensure custom script extension is restricted on personal sites Ensure custom script extension is restricted on site collections	*CIS v4.0*
		Ensure Legacy Authentication is disabled for all users Ensure External Sharing is not set to Anyone at Global level Ensure SharePoint Online sign-out inactive users is configured	*other*
Microsoft 365 Teams	Microsoft 365 Teams admin center - Teams	Ensure external file sharing in Teams is enabled for only approved cloud storage services Ensure users cant send emails to a channel email address Ensure End-To-End encryption is enabled for Teams	*CIS v4.0*
		Ensure a Custom Teams Policy is assigned to an group Ensure specific users can create Teams Team from a template	*other*
	Microsoft 365 Teams admin center - Policies	Ensure External Domain Communication Policies are configured Ensure Users Allowed to Invite Anonymous Users is disabled Ensure Policies Allow Anonymous Members is disabled Ensure Consumer Communication Policies are configured Ensure External Access Policies are configured Ensure Users Allowed to Invite Anonymous Users is disabled Ensure Safe Links for Teams is Enabled	*other*
	Microsoft 365 Teams admin center - Users	Ensure extrernal access is restricted in the Teams admin center	*CIS v4.0*
	Microsoft 365 Teams admin center - Teams Apps	Ensure app permission policies are configured Ensure communication with unmanaged Teams users is disabled Ensure external Teams users cannot initiate conversations Ensure communication with Skyper users is disabled	*CIS v4.0*
	Microsoft 365 Teams admin center - Meetings	Ensure anonymous users can't join a meeting Ensure anonymous users and dial-in callers can't start a meeting Ensure only people in my organization can bypass the lobby Ensure users dialing in can't bypass the lobby Ensure meeting chat does not allow anonmymous users Ensure only organizers and co-organizers can present Ensure external participants can't give or request control Ensure external meeting chat is off Ensure meeting recording is off by default	*CIS v4.0*
	Microsoft 365 Teams admin center - Messaging	Ensure users can report security concerns in Teams	*CIS v4.0*

App	Categorie	Test	Control
Overwiew pagina 6 van 6 Microsoft 365 Fabric	Microsoft 365 Fabric - Tenant Settings	Ensure guest user access is restricted Ensure external user invitations are restricted Ensure guest access to content is restricted Ensure Publish to web is restricted Ensure Interact with and share R and Python visuals disabled Ensure Allow users to apply sensitivity labels for content is enabled Ensure shareable links are restricted Ensure enabling of external data sharing is restricted Ensure Block ResourceKey Authentication is enabled Ensure access to APIs by Service Principals is restricted Ensure Service Principals cannot create and user profiles	*CIS v4.0*
Microsoft 365 Operational Excellence	Microsoft 365 Operational Excellence - Users and Groups	Ensure all Microsoft 365 user are licensed Ensure deleted Microsoft 365 users are identified Ensure disabled Microsoft 365 users are identified Ensure no Provisioning errors for Microsoft 365 users in hybric environments Ensure blocked Microsoft 365 users are identified Ensure deleted and licensed Microsoft 365 are identified Ensure Microsoft 365 groups without members are identified	*other*
	Microsoft 365 Operational Excellence -Dangerous Defaults	Ensure users can read all attributes in Entra ID is disabled Ensure users can create security groups is disabled Ensure users are allowed to create and register applications is disabled Ensure users with a verified mail domain can join the tenant is disabled Ensure that guests cannot invite guests Ensure users are allowed to create new Azure Active Directory Tenants is disabled Ensure policy exists to restrict non-administrator access to Entra ID	*other*
	Microsoft 365 Operation Excellence - Configuration	Ensure all Microsoft 365 domains have been verified Ensure Microsoft 365 license are assigned to groups Ensure Microsoft 365 domain services have services assigned Ensure Microsoft 365 notification email is configured	*other*

Legenda

Status	Desription
✗	Not implemented
!	Partially implemented
✓	Completely implemented
na	Not applicable
go-live	Implementation after go-live with new service partner

App	Categorie	Test	Control	Status	*Configured setting and remarks*	*Actions and Decisions*
Microsoft 365 Admin Center	Microsoft 365 Admin Center users	Ensure administrative accounts are separate and cloud-only	CIS v4.0		*A limited amount of users in the portal*	*Implementatie na go-live met nieuwe service partner*
		Ensure administrative accounts use licenses with a reduced application footprint			*A limited amount of users in the portal*	*Implementatie na go-live met nieuwe service partner*
		Ensure two emergency access accounts have been defined		✓	2 Brake glass account but one temporary?	1 extra bg accountant aangemaakt.
		Ensure that between two and four global admins are designated		✓	*4 Global admin accounts*	
		Ensure guest users are reviewed and disabled	other		No dynamic group to collect all guest accounts	Aangemaakt maar moet nog verder gefinetuned worden cq procedureel worden ingeregeld (new service parter) D.m.v. Access Review regel gerealiseerd.
	Microsoft 365 Admin Center Accounts and Authenticating	Ensure Microsoft 365 users roles have less than 10 permanent admins	other	✓	*8 admin roles configured*	
		Ensure Microsoft 365 user have strong password requirements configured			*Lockout time is limited, no custom banned password list and not enforced*	*"odveluwe, apeldoorn, harderwijk, marktplein, oosteinde" toegevoegd aan lijst; andere woorden kunnen worden aangeleverd; wie 'beheert' de lijst (bijv. na verhuizing naar nieuwe locatie)?*
		Ensure self-service password reset is enabled		✓	*Self-service password reset enabled*	*SSPR is aangezet op basis van een groep waarin alle gebruikers vallen behalve de break glass accounts*
		Ensure that Microsoft 365 passwords are not set to expire		✓	*Password expiration is disabled*	
	Microsoft 365 Admin Center Auditing	Ensure Enterprise Applications Role Assignements are reviewd weekly	other		*No reviewers added to review the Enterprise Applications Role Assignment*	*Implementatie na go-live met nieuwe service partner*
	Microsoft 365 Admin Center Teams and Groups	Ensure sign-in to shared mailboxes is blocked	CIS v4.0		*No shared mailboxes configured. Revisit this setting later*	*Implementatie na go-live met nieuwe service partner*
		Ensure that only organizationally managed-approved public groups exist			*3 public sites. 2 are default created sites and 1 test site. Be aware that when created throught admin center site is default public otherwise private*	*Implementatie na go-live met nieuwe service partner*
	Microsoft 365 Admin Center Settings	Ensure the password expiration policy is set to Set passwords to never expire	CIS v4.0	✓	*Password expiration is disabled*	
		Ensure idle session timeout is set to 3 hours or less for unmanaged devices		✓	*Configuration is not set*	*unmanaged devices hebben geen toegang hierdoor gemitigeerd*
		Ensure calendar details sharing with external users is disabled		✗	*Check box is checked*	*moet nu nog gedeeld worden met externen ivm het ontvlechtingsproject -> later opnieuw bekijken*
		Ensure user owned apps and services is restricted		✓	*Both 'Let users acces the office store' and 'Let users start trials on behalf of your organization' are unchecked*	
		Ensure internal phishing protection for forms is enabled		✓	*Check box 'Add internal phising protection' is checked*	
		Ensure the customer lockbox feature is enabled		✓	*Check box 'Require approval for all data access requests' is unchecked*	
		Ensure third-party storage services are restricted in Microsoft 365 on the web		✓	*Check box 'Let users open files stored in thrid-party storage services in Microsoft 365 on the web' is checked*	
		Ensure that sways cannot be share with people outside of your organization		✓	*Cannot login to M365 admin center to check*	

App	Categorie	Control	Control	Status	*Configured setting and remarks*	*Actions and Decisions*
Microsoft 365 Defender (1 van 2)	Microsoft 365 Defender Email and Collaboration	Ensure Safe Links for Office Applications is enabled	CIS v4.0	✔	*Built-in protection (Microsoft) is enabled*	
		Ensure the Common Attachment Types Filter is enabled		✔	*Default*	
		Ensure notifications for internal users sending malware is Enabled		✔	Off	Moet aangezet worden -> Actie in het project
		Ensure Safe Attachments policy is enabled		✔	*Built-in protection (Microsoft) is enabled*	
		Ensure Exchange Online Spam Policies are set correctly		✔	Notify these users and groups if a sender is blocked due to sending outbound spam' is not configured	Moet aangezet worden -> Actie in het project
		Ensure that an anti-phising policy has been created		✔	3 of 4 settings are correctly configured. 'Enable Intelligence for impersonation protection (Recommended)' is unchecked	Aangepast
		Ensure that SPF records are published for all Exchange Domains		!	*SPF record is created but not yet configured for Microsoft 365. Revisit this seting later. v=spf1 mx include:spf_servers.yard.nl include:spf_cluster.yard.nl -all*	*Kan pas aangepast worden bij de go-live ivm domein omzetting*
		Ensure No Domains with SPF soft fail are configured	other	✔	*No soft tail configured*	
		Ensure that DKIM is enabled for all Exhange Online Domains	CIS v4.0	✘	*No DKIM DNS record configured and not configured in Microsoft Defender*	*Kan pas aangepast worden bij de go-live ivm domein omzetting*
		Ensure DMARC Records for all Exchange Online Domains are published		✔	*DMARC DNS record is published. v=DMARC1; p=reject; rua=mailto:ciwuelq3@ag.eu.dmarcadvisor.com; ruf=mailto:ciwuelq3@fr.eu.dmarcadvisor.com; fo=1*	
		Ensure the spoofed domains are reviewed and actioned	other	Go live	*Needs to be addressed within a ITSM or planning tool to check periodically. This can also be automated via a script or other tool*	*Implementatie na go-live met nieuwe service partner*
		Ensure the restricted entities are reviewed and actioned		Go live	*Needs to be addressed within a ITSM or planning tool to check periodically. This can also be automated via a script or other tool*	*Implementatie na go-live met nieuwe service partner*
		Ensure all security threats in the Threat protection status report are reviewed and actioned		Go live	*Needs to be addressed within a ITSM or planning tool to check periodically. This can also be automated via a script or other tool*	*Implementatie na go-live met nieuwe service partner*
		Ensure comprehensive attachment filtering is applied	CIS v4.0	✔	43 file types are blocked but should be 187 according to the CIS benchmark	Via intune wordt attack surface reduction gemitigeerd. extra extensies toegevoegd
		Ensure the connection filter allow list is not used		✔	*No Ips are listed in the default Connection Filter policy*	
		Ensure the connection filter safe list is off		✔	*Safe list is of in the default Connection Filter policy*	
		Ensure inbound anti-spam policies do not contain allowed domains		✔	*Default inbound spam filter policy is used that contains no domains in the allowed list*	

App	Categorie	Control	Control	Status	*Configured setting and remarks*	*Actions and Decisions*
Microsoft 365 Defender (2 van 2)	Microsoft 365 Defender Audit	Ensure the Account Provisioning Activity report is reviewed and actioned	*other*	go live	*Needs to be addressed within a ITSM or planning tool to check periodically. This can also be automated via a script or other tool*	*Implementatie na go-live met nieuwe service partner*
		Ensure non-global administrator role group assignments are reviewed and actioned	*other*	go live	*Needs to be addressed within a ITSM or planning tool to check periodically. This can also be automated via a script or other tool*	*Implementatie na go-live met nieuwe service partner*
	Microsoft 365 Defender Settings	Ensure Priority account protection is enabled and configured	*CIS v4.0*	go live	*Priority Account protection is enabled but no tags are configured and assigned to priority accounts*	*Implementatie na go-live met nieuwe service partner*
		Ensure Priority accounts have Strict protection presets applied		✔	*Strict protection is not enabled*	*Er is voor gekozen omdeze instelling op de default Microsoft waarden te laten om een zo'n soepel mogelijke migratie*
		Ensure Microsoft Defender for Cloud Apps is enabled and configured		✔	File monitoring is not enabled, MDE app enforcement is not enabled and no notification is configured. App connectors is enabled and configured	Wordt later in het project geconfigureerd
		Ensure Zero-hour auto purge for Microsoft Teams is on		✔	*Zero hour auto purge is enabled and no exclusions are configured*	

App	Categorie	Control	Control	Status	*Configured setting and remarks*	*Actions and Decisions*
Microsoft 365 Purview	Microsoft 365 Purview Audit	Ensure Microsoft 365 audit log search is enabled	*CIS v4.0*	✔	No user and admin recording is configured	stond al aan
		Ensure role group changes are reviewed and actioned	*other*		*Needs to be addressed within a ITSM or planning tool to check periodically. This can also be automated via a script or other tool*	*Implementatie na go-live met nieuwe service partner*
	Microsoft 365 Purview - Data Loss Protection	Ensure DLP policies are enabled	*CIS v4.0*	!	Some policies are defined	DLP wordt niet aangezet dit wordt eerst via Information Protection ingeregeld
		Ensure DLP policies are enabled for Microsoft Teams		✔	*Microsoft Teams policy is created and configured*	
		Ensure DLP policy are enabled for Microsoft OneDrive	*other*	✘	Microsoft OneDrive policy is not created and configured	DLP wordt niet aangezet dit wordt eerst via Information Protection ingeregeld
		Ensure DLP policy is configured for Microsoft SharePoint		✘	Microsoft SharePoint policy is not created and configured	DLP wordt niet aangezet dit wordt eerst via Information Protection ingeregeld
		Ensure Custom Anti-Malware policy is present		✔	No custom anti-malware policy is present	Is geïmplementeerd
		Ensure Custom Anti-Phishing policy is present		✔	No custom anti-phising policy is present	Is geïmplementeerd
		Ensure Custom DLP policy are present		✘	No custom DLP are present	Geen DLP!
		Ensure Custom DLP sensitive information types are defined		✘	No custom DLP sensitive information types are defined	Geen DLP!
	Microsoft 365 Purview Information Protection	Ensure SharePoint Online Information Protection are set up and used	*CIS v4.0*	✔	Only published to Exchange email and no other app	N.v.t.

App	Categorie	Control	Control	Status	*Configured setting and remarks*	*Actions and Decisions*
Microsoft 365 Entra ID (1 van 2)	Microsoft 365 Entra ID admin center - Overview	Ensure Security Defaults is disabled on Azure Active Directory	*CIS v4.0*	✔	Conditional Access policies are used with the correct license. Which in turn reasures that security defaults are disabled	
	Microsoft 365 Entra ID admin center - Users	Ensure Per-user MFA is disabled	*CIS v4.0*	✔	Per user MFA is disabled. Revisit setting regular to adhere this compliancy setting	
		Ensure third party integrated applications are not allowed		✔	Users cannot integrate third party applications	
		Ensure Restrict non-admin users from creating tenants is set to Yes		✔	Non-admin users cannot create new tenants	
		Ensure Restrict access to the Azure AD administration portal is set to Yes		✔	Restrict access to Mircrosoft Entra admin center is set to Yes	
		Ensure the option to remain signed in is hidden		✔	Show keep users signed in set to No	
		Ensure LinkedIn account connections is disabled		✔	LinkedIn account connection is set to disabled	
	Microsoft 365 Entra ID admin center - Groups	Ensure a dynamic group for guest users is created	*CIS v4.0*	✔	No group created for catching all guest users	
	Microsoft 365 Entra ID admin center - Applications	Ensure the Application Usage report is reviewed and actioned	*other*	go live	Needs to be addressed within a ITSM or planning tool to check periodically. This can also be automated via a script or other tool	*Implementatie na go-live met nieuwe service partner*
		Ensure user consent to apps accessing company data on their behalf is not allowed	*CIS v4.0*	✔	User consent is not allowed setting is configured	
		Ensure that guest user access is restricted		✔	Guest user access is set to their own directory objects	
		Ensure guest user invitations are limited to the Guest Inviter role		✔	Only users assigned to specific admin roles can invite guest users is set	
	Microsoft 365 Entra ID admin center - External Identies	Ensure that collaboration invitations are sent to allowed domains only	*CIS v4.0*	✔	Allow invitations to be sent to any domain is configured	is aangezet
	Microsoft 365 Entra ID admin center - Hybrid Management	Ensure that password hash sync is enabled for hybrid deployments	*CIS v4.0*	na	No hybrid environment. Only cloud	
	Microsoft 365 Entra ID admin center - Conditional Access	Ensure MFA is enabled for all users in administrative roles	*CIS v4.0*	✔	Default setting and is not configurable	
		Enusre MFA is enabled for all users		✔	Default setting and is not configurable	
		Enable Conditional Access policies to block legacy authentication		✔	Conditional Access policy to block legacy authentication is configured and enabled	
		Ensure Sign-in frequency is enabled and browser sessions are not presistent for administrative users		!	Sign-in frequency is configured for every time. Persistent browser session is not configured. Not all directory roles are selected	Wordt geconfigureerd binnen het project
		Ensure Phishing-resistant MFA strength is required for administrators		go live	Only require multifactor authentication is configured	Nakijken/onderzoeken wat dit precies inhoud/requirement nieuwe leverancier. We zetten eerst passwordless authenticatie voor admins aan en dit wordt eventueel aangepast als de nieuwe service partner dit wenst. Service partner kan aanmelden met unmanaged device

App	Categorie	Control	Control	Status	*Configured setting and remarks*	*Actions and Decisions*
Microsoft 365 Entra ID (2 van 2)		Enable Azure AD Identity Protection user risk policies		✔	User risk policy is configured and enabled	
		Enable Azure AD Identity Protection sign-in riks policies		✔	Sign-in risk policy is configured and enabled	
		Ensure admin center access is limited to administrative roles		✔	No conditional access policy created to block users from accessing Microsoft admin portals	Is geconfigureerd
		Enusre sign-in risk is blocked for medium and high risk		✔	Sign-in risk is configured at low and above. So more restrictive	
		Ensure a managed device is required for authentication		✔	Conditional access policy is configured but on report-only	is ingeregeld
		Ensure a managed device is required for MFA registration		✔	Conditional access policy is configured and enabled	
	Microsoft 365 Entra ID admin center - Authentication Methods	Ensure Microsoft Authenticator is configured to protect agains MFA fatigue	*CIS v4.0*	✔	Authentication methos settings configured correctly	
		Ensure custom banned passwords lists are used		Go-live	No custom banned passwords list uploaded	*Implementatie na go-live met nieuwe service partner*
		Ensure that password protection is enabled for Active Directory		na	Cloud only customer	
	Microsoft 365 Entra ID admin center - Password Reset	Ensure self-service password reset enabled is set to All	*CIS v4.0*	✔	Password reset is configured for all users	
		Ensure the self-service password reset activity report is reviewed and actioned	*other*	Go-live	Needs to be addressed within a ITSM or planning tool to check periodically. This can also be automated via a script or other tool	*Implementatie na go-live met nieuwe service partner*
	Microsoft 365 Entra ID admin center - Risk Activities	Ensure the Azure AD Risky sign-ins report is reviewed at least weekly	*CIS v4.0*	Go-live	Needs to be addressed within a ITSM or planning tool to check periodically. This can also be automated via a script or other tool	*Implementatie na go-live met nieuwe service partner*
	Microsoft 365 Entra ID admin center - Privileged Identity	Ensure Privileged Identity Management is used to manage roles	*CIS v4.0*	✘	No Privileged Idenity Management eligble assignments are configured. Only direct assignments configured	Voor nu wordt alleen Global admin ingericht op PIM. Aza zal dit inrichten
		Ensure Access reviews for Guest Users are configured		Go-live	No access reviews configured	*Implementatie na go-live met nieuwe service partner*
		Ensure Access reviews for high privileged Azure AD roles are configured		Go-live	No access reviews configured	*Implementatie na go-live met nieuwe service partner*
		Ensure approval is required for Global Administrator role activation		Go-live	No PIM used so no control over the Global Administrator role	Aantallen admins is nu te klein om dit in te richten. Moet wel met de nieuwe service partner

App	Categorie	Control	Control	Status	*Configured setting and remarks*	*Actions and Decisions*
Microsoft 365 Exchange Online (1 van 2)	Microsoft 365 Exchange Online admin center - Audit	Ensure Audit Disabled organizationally is set to False	*CIS v4.0*	✔	*Setting is set to false*	
		Ensure mailbox auditing for E3 users is Enabled			*Need to be set for specific mailboxes on mailbox level. This is een reoccuring task that can be resolved via a automation script or tool*	*Implementatie na go-live met nieuwe service partner*
		Ensure mailbox auditing for E5 users is Enabled			*Need to be set for specific mailboxes on mailbox level. This is een reoccuring task that can be resolved via an automation script or tool*	*Implementatie na go-live met nieuwe service partner*
		Ensure AuditBypassEnabled is not enabled on mailboxes			*Default value is is not enabled but this configuration should be checked regularly via an automation script or tool*	*Implementatie na go-live met nieuwe service partner*
		Ensure Admin Auditing is Enabled	*other*	✔	Is set to true	
		Ensure Unified Audititing is Enabled		✔	Needs to be set to true	Aangezet
	Microsoft 365 Echange Online admin center - Mailflow	Ensure all forms of mail forwarding are blocked and-or disabled	*CIS v4.0*	✔	*No rules exist. Revisit on regular basis to ensure compliancy*	
		Ensure mail transport rules do not whitelist specific domains		✔	*No rules exist. Revisit on regular basis to ensure compliancy*	
		Ensure Tagging is enabled for External Emails		✔	Settings is not enabled	Wordt binnen het project aangezet
		Ensure Tagging does not allow specific domains		✔	*No domains configured in the allow list*	
		Ensure Transport Rules to Block Exchange Auto-Forwarding is configured	*other*	✔	*Auto-forwarding is blocked by anti-spam policy*	
		Ensure Do Not Bypass the Safe Attachments Filter is not configured		✔	Builtin protection is enabled but advisable to at least enable standard protection	Is geïmplementeerd
		Ensure Do Not Bypass the Safe Links Feature is not configured		✔	Builtin protection is enabled but advisable to at least enable standard protection	Is geïmplementeerd
		Ensure Transport Rules to Block Executable Attachments are configured		✔	No rules exist to block unwanted attachment of specific file extensions	Is geïmplementeerd (outbound malware policy)
		Ensure Malware Filter Policies Alert for Internal Users Sending Malware is configured		✔	*Notifications are configured*	
		Ensure Safe Attachments is Enabled		✔	*Sate attachments policy is enabled*	
		Ensure Safe Links is Enabled		✔	*Safe links policy is enabled*	
		Ensure Safe Links Click-Through is Not Allowed		✔	*Setting is configured via Safe link policy*	
		Ensure Safe Links Flags Links in Real Time		✔	*Setting is configured via Safe link policy*	
		Ensure SMTP Authentication is disabled for all users		✔	*SMTP authentication is disabled globally*	
		Ensure automatic forwarding options are disabled		✔	Automatic forwarding is enabled	Is geïmplementeerd
		Ensure all member users are MFA capable	*CIS v4.0*	✔	*Conditional Access policy configured and enabled for all users and excluding no one*	
		Ensure weak authentication methods are disabled		✔	*Conditional Access policy configured and enabled for strong authentication methods*	
		Ensure email from external senders is identified		✔	Tagging for external senders should be enabled	Is geïmplementeerd
	Microsoft 365 Exchange Online admin center - Roles	Ensure users installing Outlook add-ins is not allowed	*CIS v4.0*	✔	*My Custom Apps, My Marketplace Apps and My ReadWriteMailboxApps are configured and should be disabled*	*Staat inmiddels uit*

Microsoft 365 Exchange Online (2 van 2)	Microsoft 365 Exchange Onling admin center - Reports	Ensure mail forwarding rules are reviewed and actioned	other		This is een reoccuring task that can be resolved via an automation script or tool	Implementatie na go-live met nieuwe service partner
		Ensure the Malware Detections report is reviewed at least weekly			This is een reoccuring task that can be resolved via an automation script or tool	Implementatie na go-live met nieuwe service partner
		Ensure Microsoft 365 Deleted Mailboxes are identified and reviewed			This is een reoccuring task that can be resolved via an automation script or tool	Implementatie na go-live met nieuwe service partner
		Ensure Microsoft 365 Hidden Mailboxes are identified			This is een reoccuring task that can be resolved via an automation script or tool	Implementatie na go-live met nieuwe service partner
		Ensure Exchange Mailboxes with Full Access Delegates are reported and reviewed			This is een reoccuring task that can be resolved via an automation script or tool	Implementatie na go-live met nieuwe service partner
		Ensure Echange Mailboxes with Send As Delegates are reported and reviewed			This is een reoccuring task that can be resolved via an automation script or tool	Implementatie na go-live met nieuwe service partner
		Ensure Exchange Mailboxes with Send On Behalf Of Delegates are reported and reviewed			This is een reoccuring task that can be resolved via an automation script or tool	Implementatie na go-live met nieuwe service partner
		Ensure Microsoft 365 Exchange Online Admin access attempts are reported and reviewed			This is een reoccuring task that can be resolved via an automation script or tool	Implementatie na go-live met nieuwe service partner
	Microsoft 365 Excange Online admin center - Settings	Ensure modern authentication for Exchange Online is enabled	CIS v4.0	✔	Legacy authentication is disabled via Conditional Access policy	
		Ensure MailTips are enabled for end users		✔	All MailTips are enabled	
		Ensure external storage providers available in Outlook on the Web are restricted		✔	No external storage providers are available	
		Ensure Always Deliver Messages From These Senders for specific IP and Domain are not configured	other	✔	No Rules configured	

App	Categorie	Control	Control	Status	*Configured setting and remarks*	*Actions and Decisions*
Microsoft 365 SharePoint Online (1 van 2)	Microsoft 365 SharePoint Online admin center - Settings	Ensure modern authentication for SharePoint Online applications is required	CIS v4.0	✔	*Legacy authentication is disabled by Conditional Access policy*	
		Ensure Sharepoint Online and OneDrive intergration with Entra ID B2B is enabled		✔	*B2B Entra ID integration for Sharepoint and OneDrive is enabled*	
		Ensure SharePoint Online external content sharing is restricted		✔	*External sharing is set on disabled*	
		Ensure OneDrive content sharing is restricted		✔	*External sharing is set on disabled*	
		Ensure that SharePoint Online guest users cannot share item they don't own		gouwe	*External users can reshare*	*Sharing staat voor de gehele organistatie uit. Er kan dus niets gedeeld worden. Hier moet naar gekeken worden met de nieuwe service partner*
		Ensure link sharing is restricted in SharePoint Online and OneDrive		gouwe	*Link sharing is set to internal*	*Sharing staat voor de gehele organistatie uit. Er kan dus niets gedeeld worden. Hier moet naar gekeken worden met de nieuwe service partner*
		Ensure external sharing is restricted by security group		gouwe	*External sharing is disabled*	*Sharing staat voor de gehele organistatie uit. Er kan dus niets gedeeld worden. Hier moet naar gekeken worden met de nieuwe service partner*
		Ensure reauthentication with verification code is restricted		gouwe	*Reauthentication is disabled and authentication days is set to 30 (default)*	*Sharing staat voor de gehele organistatie uit. Er kan dus niets gedeeld worden. Hier moet naar gekeken worden met de nieuwe service partner*
		Ensure guest access to a site or OneDrive will expire automatically		gouwe	*Guest access expiration is not enabled and set to its default of 60 days*	*Sharing staat voor de gehele organistatie uit. Er kan dus niets gedeeld worden. Hier moet naar gekeken worden met de nieuwe service partner*
		Ensure the SharePoint default sharing link permission is set		✔	It's set to edit	Is op 'View' gezet.
		Ensure sharing is being white- or blacklisted on domain basis	other	gouwe	*No white- or blacklist on domain basis exists*	*Sharing staat voor de gehele organistatie uit. Er kan dus niets gedeeld worden. Hier moet naar gekeken worden met de nieuwe service partner. Voorkeur heeft een allowed list*
		Ensure Microsoft 365 SharePoint Online infected files are disallowed for download		✔	*Infected files are available for download*	*Is inmiddels ingeschakeld*

Microsoft 365 SharePoint Online (2 van 2)		**Ensure OneDrive sync is restricted for unmanaged devices**	*CIS v4.0*	na	TenantRestrictionEnabled is false so sync from unmanaged devices is available	N.v.t.; alleen voor AD domeinen (https://learn.microsoft.com/en-us/sharepoint/allow-syncing-only-on-specific-domains?WT.mc_id=365AdminCSH_spo)
		Ensure custom script extension is restricted on personal sites		✔	*Prevent users from running custom script on personal sites is set (default)*	
		Ensure custom script extension is restricted on site collections		✔	*DenyAddAndCustomizePages is enabled for every site*	
		Ensure that SharePoint user sessions are terminated upon user logoff and when the idle time limit is exceeded		✔	Can not check	Advies is dit niet in te regelen. Het is op dit moment niet van toepassing. Alle instellingen mbt. levensduur van sessies worden d.m.v. conditional access policies geregeld.

App	Categorie	Control	Control	Status	Configured setting and remarks	Actions and Decisions
Microsoft 365 Teams	Microsoft 365 Teams admin center - Teams	Ensure external file sharing in Teams is enabled for only approved cloud storage services	CIS v4.0	✓	All third party storage providers are enabled	Wordt binnen het project geconfigureerd
		Ensure users cant send emails to a channel email address			Users can send emails to a channel email address is enabled	Wordt voor nu uit gezet. Er wordt met de nieuwe service partner gekeken of dit aan of uit moet
		Ensure End-To-End encryption is enabled for Teams			Not enabled	Laten we uit staan. Er wordt met de nieuwe service partner gekeken of dit aan of uit moet
		Ensure a Custom Teams Policy is assigned to an group	other		Part of Teams premium	Er wordt met de nieuwe service partner gekeken of dit aan of uit moet
		Ensure specific users can create Teams Team from a template			Part of Teams premium	Er wordt met de nieuwe service partner gekeken of dit aan of uit moet
	Microsoft 365 Teams admin center - Users	Ensure extrernal access is restricted in the Teams admin center	CIS v4.0	✓	Allow all external domains is set	Geïmplementeerd conform Apeldoorn. Teams meetings zijn mogelijk, maar bestanden kunnen niet worden gedeeld
	Microsoft 365 Teams admin center - Teams Apps	Ensure app permission policies are configured	CIS v4.0	✓	Users are allowed to install custom apps	Is geïmplementeerd
		Ensure communication with unmanaged Teams users is disabled		✓	People in the organization can communicate with unmanaged Teams accounts is enabled	Policy Apeldoorn is gevolgd; Uitgaande communicatie met unmanaged Teams users is wel mogelijk; inkomend niet.
		Ensure external Teams users cannot initiate conversations		✓	Guest can start conversations	Is ingeregeld. Policy Apeldoorn is leidend
		Ensure communication with Skyper users is disabled		✓		Niet meer van toepassing (volledig beheerd door MS, geen aanpassingen mogelijk)
	Microsoft 365 Teams admin center - Meetings	Ensure anonymous users can't join a meeting	CIS v4.0	✓	Anonymous users can join a meeting is set to On	Is geïmplementeerd
		Ensure anonymous users and dial-in callers can't start a meeting		✓	Anonymous users and dial-in callers can start a meeting is Off	
		Ensure only people in my organization can bypass the lobby		✓	Who can bypass the lobby is set to People in my org	
		Ensure users dialing in can't bypass the lobby		✓	People dialing in can bypass the lobby is set to Off	
		Ensure meeting chat does not allow anonmymous users		✓	Anonymous users can join a meeting is set to On	Is geïmplementeerd
		Ensure only organizers and co-organizers can present		✓	Who can present is set to Everyone	Iedereen moet kunnen presenteren. Dit laten we dus op de setting 'EveryOne'
		Ensure external participants can't give or request control		✓	External participants can give or request control is set to Off	
		Ensure external meeting chat is off		✓	External meeting chat is set to On	Chat met externen is mogelijk; delen van bestanden niet
	Microsoft 365 Teams admin center - Messaging	Ensure users can report security concerns in Teams	CIS v4.0	✓	Report a security concern is set to On	

App	Categorie	Control	Control	Status	*Configured setting and remarks*	*Actions and Decisions*
Microsoft 365 Fabric	Microsoft 365 Fabric - Tenant Settings	Ensure guest user access is restricted	*CIS v4.0*	No Status	Can not check test	Wordt geen gebruik van gemaakt. Let op! Mocht dit in de toekomst wel gebeuren dan zullen deze controls weer gereviewed moeten worden
		Ensure external user invitations are restricted		No Status	Can not check test	Wordt geen gebruik van gemaakt. Let op! Mocht dit in de toekomst wel gebeuren dan zullen deze controls weer gereviewed moeten worden
		Ensure guest access to content is restricted		No Status	Can not check test	Wordt geen gebruik van gemaakt. Let op! Mocht dit in de toekomst wel gebeuren dan zullen deze controls weer gereviewed moeten worden
		Ensure Publish to web is restricted		No Status	Can not check test	Wordt geen gebruik van gemaakt. Let op! Mocht dit in de toekomst wel gebeuren dan zullen deze controls weer gereviewed moeten worden
		Ensure Interact with and share R and Python visuals disabled		No Status	Can not check test	Wordt geen gebruik van gemaakt. Let op! Mocht dit in de toekomst wel gebeuren dan zullen deze controls weer gereviewed moeten worden
		Ensure Allow users to apply sensitivity labels for content is enabled		No Status	Can not check test	Wordt geen gebruik van gemaakt. Let op! Mocht dit in de toekomst wel gebeuren dan zullen deze controls weer gereviewed moeten worden
		Ensure shareable links are restricted		No Status	Can not check test	Wordt geen gebruik van gemaakt. Let op! Mocht dit in de toekomst wel gebeuren dan zullen deze controls weer gereviewed moeten worden
		Ensure enabling of external data sharing is restricted		No Status	Can not check test	Wordt geen gebruik van gemaakt. Let op! Mocht dit in de toekomst wel gebeuren dan zullen deze controls weer gereviewed moeten worden
		Ensure Block ResourceKey Authentication is enabled		No Status	Can not check test	Wordt geen gebruik van gemaakt. Let op! Mocht dit in de toekomst wel gebeuren dan zullen deze controls weer gereviewed moeten worden
		Ensure access to APIs by Service Principals is restricted		No Status	Can not check test	Wordt geen gebruik van gemaakt. Let op! Mocht dit in de toekomst wel gebeuren dan zullen deze controls weer gereviewed moeten worden
		Ensure Service Principals cannot create and user profiles		No Status	Can not check test	Wordt geen gebruik van gemaakt. Let op! Mocht dit in de toekomst wel gebeuren dan zullen deze controls weer gereviewed moeten worden

App	Categorie	Control	Control	Status	Configured setting and remarks	Actions and Decisions
Microsoft 365 Operational Excellence	Microsoft 365 Operational Excellence - Users and Groups	Ensure all Microsoft 365 users are licensed	other	✓	Create a dynamic group to identify unlicensed users and review at least monthly	Group is aangemaakt
		Ensure deleted Microsoft 365 users are identified		✓	Create a dynamic group to identify deleted users and review at least monthly	Onduidelijk welk nut dit heeft In Entra ID kan in één oogopslag worden bekeken of er (soft-)deleted user accounts zijn
		Ensure disabled Microsoft 365 users are identified		✓	Create a dynamic group to identify disabled users and review at least monthly	Group is aangemaakt
		Ensure no Provisioning errors for Microsoft 365 users in hybric environments		na	No onprem AD	
		Ensure blocked Microsoft 365 users are identified		✓	Create a dynamic group to identify blocked users and review at least monthly	Onduidelijk welk nut dit heeft In de Defender portal kan in één oogopslag worden bekeken of er restricted entities zijn; Overigens zou monitoring hierop gedaan moeten worden door een monitoring-tool.
		Ensure Microsoft 365 groups without members are identified		✓	Create a dynamic group to identify empty groups and review at least monthly	Advies: inregelen frequente check op opruimen groepen, teams, users, mailboxen, applicaties enz. die niet meer nodig zijn c.q. niet meer gebruikt worden. Implementatie na go-live met nieuwe service partner
	Microsoft 365 Operational Excellence -Dangerous Defaults	Ensure users can create security groups is disabled	other	✓	Users can create security groups is set to off	
		Ensure users are allowed to create and register applications is disabled		✓	Users can register applications is set to No	
		Ensure that guests cannot invite guests		✓	Only users assigned to specific admin roles can invite guest users is set	
		Ensure users are allowed to create new Azure Active Directory Tenants is disabled		✓	Restrict non-admin users from creating tenants is set to Yes	
		Ensure policy exists to restrict non-administrator access to Entra ID		✓	Restrict access to Microsoft Entra admin center is set to Yes	
	Microsoft 365 Operation Excellence - Configuration	Ensure all Microsoft 365 domains have been verified	other	✓	Just one domain present. No custom domain configured	Dit is een vereiste en niet te missen actie tijdens de migratie (het odveluwe.nl zal dan worden toegevoegd aan de tenant.
		Ensure Microsoft 365 license are assigned to groups		✓	No groups configured to assign licenses	Is reeds geregeld/geïmplementeerd
		Ensure Microsoft 365 notification email is configured		✓	Technical contact is present	
3rd Party Tool voor Intune	3rd Party tool voor betere beheer van software-deploymen	RoboPack is ingezet om efficienter en beter software en updates van applicaties te kunnen distribueren naar de laptop				