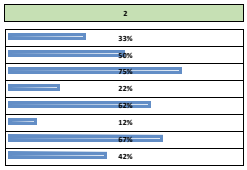
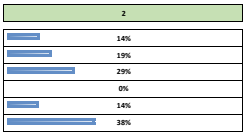
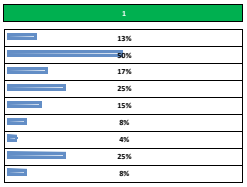
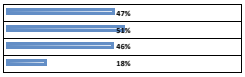
M365, Active Directory, Azure Active Directory og Microsoft Baseline Dashboard V1.2 Jan 2022 © Dediko A/S 2022

Dashboard - M365 Sikkerhed	Dashboard - Active Directory	Dashboard - Azure Active Directory	Samlet score	Microsoft Azure Security Benchmark
45%	19%	18%	28%	40%









Se mere om vores services og modenhedsmodeller på www.dediko.dk
Kontakt Christian Schmidt direkte på mail: chr@dediko.dk

Dediko A/S
Your Security is our Passion

45%	Dashboard - M365 Sikkerhed	Compliance
	CIS Benchmark	33%
	Account/Authentication politikker	50%
	Applikationstilladelser/adgang	75%
	Dataadministration	22%
	Email sikkerhed/Exchange Online	62%
	Audtpolitikker	12%
	Lagringspolitikker	67%
	Mobile device administration	42%

Dediko A/S
Your Security is our Passion

Vælg først ønsket status herunder (D13)...

	Målsat risikoprofil (1,2,3) --->>>		2		

Fortsæt derefter med at udfylde nuværende status herunder (C16)...

33%	CIS Benchmark	Status	Ønsket status	Delta	Bemærkning
SPG: #01	Er der kørt et benchmark mod M365 tennant	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #02	Er dette benchmark mitigeret?	1. Delvist implementeret	3. Fuldt implementeret	2	
50%	**Account/Authentication politikker**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #03	**Implementer fler-faktor godkendelse (2FA) for alle brugere med administrative roller**	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
SPG: #04	**Implementer fler-faktor (2FA) godkendelse for alle brugere I alle roller**	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #05	**Håndhæv at der er defineret mellem 2 og 4 global admins**	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #06	Implementer at self-service password reset er aktiveret	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #07	Håndhæv at moderne godkendelse for Exchange Online er aktiveret	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #08	Håndhæv at moderne godkendelse for SharePoint applications er aktiveret	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #09	Håndhæv at moderne godkendelse for Skype for Business Online er aktiveret	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #10	Implementer at Office 365 Passwords ikke udløber	3. Fuldt implementeret	3. Fuldt implementeret	0	
75%	**Applikationstilladelser/adgang**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #11	Håndhv at tredieparts integrerede applikationer ikke er tilladt (User Settings > No App Registrations).	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #12	Håndhæv at deling af kalenderdetaljer ikke er tilladt med tredjepart / udenfor virksomheden	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #13	Implementer at O365 ATP SafeLinks til Office applikationer er aktiveret	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #14	Håndhæv at Office 365 ATP for SharePoint, OneDrive og Microsoft Teams er aktiveret (blokerer ondsindede filer).	3. Fuldt implementeret	3. Fuldt implementeret	0	
22%	**Dataadministration**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #15	Håndhæv at customer lockbox funktionen er aktiveret	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #16	Håndhæv at SharePoint Online data klassifikationspolitikker er implementerede og i aktiv anvendelse	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #17	Håndhæv at eksterne domæner ikke er tilladt I Skype eller Teams	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #18	Håndhæv DLP politikker er aktiverede og i aktiv anvendelse	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #19	Håndhæv at eksterne brugere ikke kan dele filer, foldere eller hjemmesider de ikke er ejere af	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #20	Håndhæv at kun autriserede vloud lagrings tjenester er tilladt til deling i teams	0. Ikke implementeret	3. Fuldt implementeret	3	
62%	**Email sikkerhed/Exchange Online**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #21	Håndhæv at "Common Attachment Types Filter" er aktiveret	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #22	Håndhæv at Exchange Online Spam politikker er aktiveret og implementeret korrekt	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #23	Håndhæv at mail transportregler ikke forwarder mails til ekstern email adresser	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #24	Håndhæv at mailtransportregler ikke hvidliter specifikke domæner	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #25	Håndhæv at "Client Rules Forwarding" blokering er aktiveret	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #26	Håndhæv at "Advanced Threat Protection Safe Links" politikken er aktiveret	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #27	Håndhæv at "Advanced Threat Protection Safe Attachments" politikken er aktiveret	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #28	Håndhæv at basal authentication for Exchange Online er deaktiveret	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #29	Håndhæv at der er oprettet og implementeret en anti-phishing politik	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
SPG: #30	Håndhæv at DKIM er aktiveret for alle Exchange Online Domæner	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #31	Håndhæv at SPF records er publiseret for alle Exchange Domains.	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #32	Håndhæv at DMARC Records er publiseret for alle Exchange Online domæner	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #33	Håndhæv at notifikation om at interne brugere sender malware er aktiveret	1. Delvist implementeret	3. Fuldt implementeret	2	
12%	**Audtpolitikker**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #34	Håndhæv at Microsoft 365 audit log søgning er aktiveret	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #35	Håndhæv at mailbox auditing for alle brugere er aktiveret	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #36	Håndhæv at "Azure AD Risky sign-ins" reporten bliver læst og mitigeret mindst ugentligt	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #37	Håndhæv at "Application Usage" reporten bliver læst og mitigeret mindst ugentligt	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #38	Håndhæv at "self-service password reset" aktivitetsrapporten bliver læst og mitigeret mindst ugentligt	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #39	Håndhæv at "user role group"ændringer bliver læst og mitigeret mindst ugentligt	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #40	Håndhæv at mail forwarding regler bliver vurderet og mitigeret mindst ugentligt	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #41	Håndhæv at "Mailbox Access by Non-Owners" rapporten bliver læst og mitigeret mindst hver anden uge	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #42	Håndhæv at "Malware Detections" rapporten bliver læst og mitigeret mindst ugentligt	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #43	Håndhæv at "Account Provisioning Activity" rapporten bliver læst og mitigeret mindst ugentligt	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #44	Håndhæv at alle "ikke global administrator rollle gruppe tildelinger" bliver læst og mitigeret mindst ugentligt	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #45	Håndhæv at "spoofed domains" rapporten bliver læst og mitigeret mindst ugentligt	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #46	**Håndhæv at Microsoft 365 Cloud App Security er aktiveret**	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #47	Håndhæv om brugere der har fået deres privilegier begrænset pga. Spam bliver læst og mitigeret	1. Delvist implementeret	3. Fuldt implementeret	2	
67%	**Lagringspolitikker**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #48	Håndhæv at dokumentdeling bliver kontrolleret og administreret pr. Domæne med hvid- og sortlistning	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #49	Håndhæv at "expiration time for external sharing links" er aktiveret	3. Fuldt implementeret	3. Fuldt implementeret	0	
42%	**Mobile device administration**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #50	Håndhæv at "mobile device management polices" er aktiveret til at kræve avancerede sikkerhedskonfigurationer til at beskytte mod basale internetbaserede angreb	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
SPG: #51	Håndhæv at mobile device password genrbug er forhindret/forbudt	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
SPG: #52	Håndhæv at mobile devices har passwords sat til aldrig at udløbe	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #53	Håndhæv at brugene ikke kan forbinde fra mobile devices som er "jail broken" eller "rooted"	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #54	Håndhæv at mobile devices er aktiverede til at auto-slette alt indhold ved gentage fejlede loginforsøg for at forbundre et brute force angreb med følgende kompromittering	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #55	Håndhæv indstillingerne der låser flere mobile devices efter en priode med inaktivitet for at forhindre uautoriseret adgang	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #56	Håndhæv at mobile device kryptering er aktiveret for at forhindre uautoriseret adgang tl lmobile data	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #57	Håndhæv at mobile deviceskræve komplekse passwords for at forhindre brute force angreb	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #58	Håndhæv at mobile devices som forbinder til netværket har antivius og lokal firewall aktiveret (Windows 10).	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #59	Håndhæv at mobile device administrationspolitikker er krævet for email profiler	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #60	Håndhæv at mobile devices kræver brugen af et password	3. Fuldt implementeret	3. Fuldt implementeret	0	

	Dashboard - Active Directory	Compliance
19%	Sikring af Domain Controllerne efter CIS kontrollerne	14%
	Opsætning af AD	19%
	Overvåges AD for tegn på ondsindet kode og adfærd	29%
	Mitigering af klassiske angrebsteknikker	0%
	Er følgende grupper i AD under streng kontrol, administration, overvågning og mitigering efter principperne om mindste privilegier (PoLP)	14%
	Identity Access Management (IAM) og Active Directory	38%

Dediko A/S
Your Security is our Passion

Vælg først ønsket status herunder (D11)...

Målsat risikoprofil (1,2,3) --->>> 2

Fortsæt derefter med at udfylde nuværende status herunder (C14)...

14%	Sikring af Domain Controllerne efter CIS kontrollerne	Status	Ønsket status	Delta	Bemærkning
SPG: #01	Er der installeret et bedst i klasse anti-malware system på DC'erne	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #02	Er der implementeret et sekundært anti-malware system fx via VMWare / Hyper-V	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #03	Sårbarhedsscannes DC'erne kontinuerligt	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #04	Mitigeres de fundne sårbarheder rettidigt efter risiko	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #05	Er der implementeres application whitelisting på DC'erne	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #06	Anvendes kun sikre autoriserede applikationer på DC'erne I specifikt tilladte versioner	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #07	Er DC'erne segmenteret fra det øvrige netværk	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #08	Er ALLE DC'erne beskyttet af en firewall med en default deny politik	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
SPG: #09	Er OS indbyggede sikkerhedsfunktioner slået til hvor det er muligt (fx UAC)	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #10	Bruges sikre dedikerede klienter til at administrere DC'erne	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #11	Tilgås DC'erne efter sikker bedste praksis - restriktiv RDP med jump servere	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #12	Er DC'erne holdt kontinuerligt op mod CIS Benchmarks	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #13	Mitigeres afvigelser fra CIS Benchmarks rettidigt efter risiko	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #14	Er DC'erne skærmet mod Internettet	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #15	Anvendes sikre browsere på DC'erne	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #16	Er DC'ernes OS opgraderet til seneste (N-1) nye OS	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
SPG: #17	Er der implementeret en OS lifecycle management for DC'erne	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #18	Er fysiske Domain Controllere tilstrækkelgt beskyttede	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #19	Er virtuelle Domain Controller (i det virtuelle miljø) tilstrækkeligt beskyttet mod uautoriseret adgang	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #20	Kører virtuelle Domain Controller på separate fysiske hypervisor hosts	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #21	Er der implementeret Bitlocker på Domain Controllerne	0. Ikke implementeret	3. Fuldt implementeret	3	
19%	**Opsætning af AD**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #22	Er der afviklet en vurdering af modenheden i opsætningen af AD	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #23	Mitigeres drift væk fra bedste praksis kontinuerligt	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #24	Er det muligt at restore specifikke AD objekter	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #25	Er AD særligt beskyttet med "backup"	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
SPG: #26	Testes AD restore live regelmæssigt	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #27	Er GPO opsat efter bedste praksis	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #28	Er ændringer af disse GPO under regelmæssig audit og aktiv overvågning (eller automatisk mitigering)	0. Ikke implementeret	3. Fuldt implementeret	3	
29%	**Overvåges AD for tegn på ondsindet kode og adfærd**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #29	Er audit politikker opsat efter bedste påraksis på alle Domain Controllere	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
SPG: #30	Opsamles DC logs fra ALLE DC'erne til et centralt system	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #31	Overvåges disse logs for tegn på compromise eller ond-sindet adfærd	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #32	Er der implementeret use-cases baseret på MITRE ATT&CK	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #33	Er der et velfungerende SOC med aktiv Incident Resonse tilknyttet denne overvågning	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #34	Er der en særlig IR plan for at mitigere et angreb på AD/DC?	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #35	Er der en særlig plan for at vurdere sikkerheden på AD/DC ved sammenlægning og opkøb af virksomheder	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #36	Følger du målrettede blogs og website om AD (Fx https://adsecurity.org/ og https://ultimatewindowssecurity.com)	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
0%	**Mitigering af klassiske angrebsteknikker**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #37	Er følgende teknik mulig at opdage og mitigere: Pass-The-Hash og Mimikatz	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #38	Er følgende teknik mulig at opdage og mitigere: GPO Præference og Passwordudtræk	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #39	Er følgende teknik mulig at opdage og mitigere: AdminSDHolder og SDProp	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #40	Er følgende teknik mulig at opdage og mitigere: Ntdis.dit kompromittering og password udtræk	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #41	Er følgende teknik mulig at opdage og mitigere: LDAP undersøgelser	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #42	Er følgende teknik mulig at opdage og mitigere: DCShadow angreb	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #43	Er følgende teknik mulig at opdage og mitigere: Password Spray	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #44	Er følgende teknik mulig at opdage og mitigere: Kerberos Silver Ticket	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #45	Er følgende teknik mulig at opdage og mitigere: Golden Ticket	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #46	Er følgende teknik mulig at opdage og mitigere: Kerberoasting	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #47	Er følgende teknik mulig at opdage og mitigere: Misbrug af AD attributter	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #48	Er følgende teknik mulig at opdage og mitigere: Pass-the-cookie	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #49	Er følgende teknik mulig at opdage og mitigere: Lateral bevægelse	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #50	Er følgende teknik mulig at opdage og mitigere: Andre mimikatz teknikker	0. Ikke implementeret	3. Fuldt implementeret	3	
14%	**Er følgende grupper i AD under streng kontrol, administration, overvågning og mitigering efter principperne om mindste privilegier (PoLP)**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #51	Administrators	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
SPG: #52	DHCP Administrators	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #53	DnsAdmins	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #54	Domain Admins	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #55	Enterprise Admins	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #56	Schema Admins	3. Fuldt implementeret	3. Fuldt implementeret	0	
SPG: #57	Account Operators	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #58	Backup Operators	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #59	Cryptographic Operators	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #60	Distributed COM Users	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #61	Incoming Forest Trust Builders	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #62	Network Configuration Operators	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #63	Performance Log Users	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #64	Performance Monitor Users	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #65	Print Operators	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #66	Remote Desktop Users	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #67	Replicator	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #68	Server Operators	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #69	Windows Authorization Access Group	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #70	Cert Publishers	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #71	DnsUpdateProxy	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #72	Domain Controllers	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #73	Enterprise Read-only Domain Controllers	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #74	Group Policy Creator Owners	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #75	RAS and IAS Servers	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #76	Read-only Domain Controllers	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #77	Er egne tilsvarende grupper (fx SQL Admins/Vmware admins under samme kontrol?	0. Ikke implementeret	3. Fuldt implementeret	3	
38%	**Identity Access Management (IAM) og Active Directory**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #78	Er der impleenteret et PAM system efter bedste praksis?	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #79	Er der implementeret en robust IAM for Service konti	0. Ikke implementeret	3. Fuldt implementeret	3	
SPG: #80	Er der implementeret en robust IAM for Administrative konti	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
SPG: #81	Er der implementeret en robust IAM for Konsulent konti	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
SPG: #82	Er der implementeret en robust IAM for Bruger konti	2. Næsten fuldt implementeret	3. Fuldt implementeret	1	
SPG: #83	Er alle relevante konti under regelmæssig audit	1. Delvist implementeret	3. Fuldt implementeret	2	
SPG: #84	Er Microsoft (eller lignende) 3-tier admin modellen implementeret?	0. Ikke implementeret	3. Fuldt implementeret	3	

	Dashboard - Azure Active Directory	Compliance
	CIS Benchmark	13%
	Centraliseret identitetsstyring	50%
	Password administration og fler-faktor godkendelse	17%
18%	Overvågning af uautoriseret / ondsindet adfærd	25%
	Microsoft Defender for Cloud (Se CIS Benchmark for et komplet Audit set)	15%
	Lager (Storage) konti (Se CIS Benchmark for et komplet Audit set)	8%
	MS SQL Server (Se CIS Benchmark for et komplet Audit set)	4%
	Microsoft Defender for Cloud (Se CIS Benchmark for et komplet Audit set)	25%
	Netværk (Se CIS Benchmark for et komplet Audit set)	8%

Dediko A/S
Your Security is our Passion

Vælg først ønsket status herunder (D14)...

	Målsat risikoprofil (1,2,3) --->>>	1	

Fortsæt derefter med at udfylde nuværende status herunder (C17)...

13%	CIS Benchmark	Status	Ønsket status	Delta	Bemærkning
SPG: #01	**Er der afviklet et CIS Benchmark mod Azure AD**	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #02	**Bruges Azure Security Benchmark aktivt**	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #03	Er resultaterne fra denne benchmark scanning mitigeret	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #04	Undersøges det kontinuerlit om denne status drifter væk fra bedste praksis	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
50%	**Centraliseret identitetsstyring**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #05	Behandler du identitetsstyring som den vigtigste perimeter (bruger du Azure AD til identitetsstyring?)	3. Fuldt implementeret	4. Fuldt implementeret og vedligeholdt	1	
SPG: #06	Bruger du et enkelt Azure AD som fundamet for identitetsstyring iet et hybrid miljø?	2. Næsten fuldt implementeret	4. Fuldt implementeret og vedligeholdt	2	
SPG: #07	Bruger du Azure AD connecttil at synkronisere on-prem ad identiteter til Azure AD?	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #08	Undgår du at synkronisere on-prem konti mere høje privilegier (filtreret væk som standard)	3. Fuldt implementeret	4. Fuldt implementeret og vedligeholdt	1	
SPG: #09	Er Password Hash synkroniseret aktiveret (beskytter mod lækkede rettigheder)	3. Fuldt implementeret	4. Fuldt implementeret og vedligeholdt	1	
SPG: #10	Bruges Azure AD korrekt I udvikling af nye applikationer (Azure AD, Azure AD, B2B og Azure AD B2C)	3. Fuldt implementeret	4. Fuldt implementeret og vedligeholdt	1	
SPG: #11	Er single sign on (SSO) aktiveret og udvidet fra on-pre AD I et hybrid miljø?	3. Fuldt implementeret	4. Fuldt implementeret og vedligeholdt	1	
SPG: #12	Er Azure AD Application Proxy implementeret korrekt	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #13	Er gamle og unødvendige (Legacy) protokoller deaktiverede (relateret til betinget adgang)?	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #14	Er betinget adgangs politikker implementeret korrekt relateret til grupper, lokation og (SaaS) applikation(er)	3. Fuldt implementeret	4. Fuldt implementeret og vedligeholdt	1	
SPG: #15	Har du implementeret regelmæssige audits af cybersikkerheds status for at forbedre scoren?	2. Næsten fuldt implementeret	4. Fuldt implementeret og vedligeholdt	2	
17%	**Password administration og fler-faktor godkendelse**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #16	Er self-service passwords SSFR aktiveret (og virker det I tilstrækkeligt grad)?	3. Fuldt implementeret	4. Fuldt implementeret og vedligeholdt	1	
SPG: #17	Overvåges SSPR funktionen for uautoriseret adfærd?	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #18	Er password beskyttelsen I Azure AD (eller lignende tredieparts funktion) udvidet tilogså at dække on-prem AD passwords	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #19	Er fler-faktor godkendelse for alle brugere aktivret	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #20	**Bruges rolle baseret adgangsstyring baseret på PoLP**	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #21	Bruges indbyggede Azure Roller til rolle basret adgangsstyring (Funktionsadskillelse)	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #22	Er medlemskabet af disse roller under regelmæssigt audit	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #23	Overvåges medlemmer af specifikke roller med høje pprivilegier for uautoriseret adfærd?	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #24	Hvis virksomheden har et sikkerhedsteam har de så fået Security Reader rollen	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #25	Har Microsoft Defender (hvis den bruges) fået adgang til de nødvendige sikkerhedsroller	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #26	Er Microsoft PIM (eller lignende tredieparts funktionalitet) aktiveret	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #27	Har alle administrative roller separat konti for forskellige administrative opgaver	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #28	Er særlig Global Admin brugt efter bedste praksis (2-4 brugere under regelmæssigt audit og alarmering)	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #29	Er der implementeret Just In Time adgang til roller hvor det er relevant	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #30	Er MFA aktiveret for alle administrative konti	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #31	Er der implementeret privilegerede arbejdsstationer (PAW)	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #32	Er der implementeret en IAM proces for administrative konti	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #33	Er administrative konti en del af er regelmæssigt IR test scanarie	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #34	Er administrative konti testet mod de mest almindelige angrebsmetoder/tenikker	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
25%	**Overvågning af uautoriseret / ondsindet adfærd**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #35	Tegn på adgang uden adgangskontrol	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #36	Brute Force angreb	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #37	Forsøg på login fra flere lokationer på samme sid ("impossible travel")	3. Fuldt implementeret	4. Fuldt implementeret og vedligeholdt	1	
SPG: #38	Tegn på devices som er angrebet af malware	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
15%	**Microsoft Defender for Cloud (Se CIS Benchmark for et komplet Audit set)**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #39	Er Defender for servere aktiveret	3. Fuldt implementeret	4. Fuldt implementeret og vedligeholdt	1	
SPG: #40	Er Defender for app services aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #41	Er Defender for Azure SQL aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #42	Er Defender for lager (Storage) aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #43	Er Defender for Key Valut aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #44	Er Defender for klienter (WDATP) aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #45	Er Defender for Cloud Apps Integration (MCAS) aktiveret	3. Fuldt implementeret	4. Fuldt implementeret og vedligeholdt	1	
SPG: #46	Er Defender for klienter (WDATP) aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #47	Er Defender for klienter (WDATP) aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #48	Er Defender for klienter (WDATP) aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
8%	**Lager (Storage) konti (Se CIS Benchmark for et komplet Audit set)**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #49	Er "Secure Transfer required" aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #50	Lager konto keys er regelmæssigt fornyet	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #51	Er lager logning for for "Queue Service" aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #52	Er standard networks adgang for lager konti sat til "Deny"	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #53	Er "Soft Delete" aktiveret for Azure lagerplads	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #54	Er minimum TLS service version sat til 1.2	2. Næsten fuldt implementeret	4. Fuldt implementeret og vedligeholdt	2	
4%	**MS SQL Server (Se CIS Benchmark for et komplet Audit set)**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #55	Er "auditing" aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #56	Er datakryptering aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #57	Er ATP for SQL aktiveret	1. Delvist implementeret	4. Fuldt implementeret og vedligeholdt	3	
SPG: #58	Er sårbarhedsvurdering aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #59	Er sårbarhedsvurdering aktiveret til periodisk genscan	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #60	Er sårbarhedsvurderings scan rapporter aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
25%	**Logning og overvågning (Se CIS Benchmark for et komplet Audit set)**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #61	Håndhæv at "Diagnostics settings" findes	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #62	Håndhæv af diagnostics settings fanger relevante kategorier	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #63	Håndhæv at Azure logging for KeyVault er aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #64	Håndhæv en aktivitetslog for "Delete Policy"	3. Fuldt implementeret	4. Fuldt implementeret og vedligeholdt	1	
SPG: #65	Håndhæv en aktivitetslog for "Create Policy"	3. Fuldt implementeret	4. Fuldt implementeret og vedligeholdt	1	
SPG: #66	Håndhæv en aktivitetslog for "Delete Security Solution"	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
8%	**Netværk (Se CIS Benchmark for et komplet Audit set)**	**Status**	**Ønsket status**	**Delta**	**Bemærkning**
SPG: #67	Er RDP adgang fra Internettet begrænset	2. Næsten fuldt implementeret	4. Fuldt implementeret og vedligeholdt	2	
SPG: #68	Er SSH adgang fra Internettet begrænset	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #69	Er UDP Services fra Internettet begrænset	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #70	Er SQL Database Aloow ingress deaktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #71	Er network flow log retention sat til mere end 90 dage	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	
SPG: #72	Er Network Watcher aktiveret	0. Ikke implementeret	4. Fuldt implementeret og vedligeholdt	4	

Microsoft Azure Security Benchmark

Baseline	Relevans	Efterlevelse
Azure Bot Service	✓	75%
Azure Bastion	✓	22%
Azure Backup	✓	32%
Azure Arc-aktiverede servere	✗	20%
Azure App Konfiguration	✓	50%
Azure Advisor	✓	75%
Azure AD Domain Services	✓	75%
Azure AD	✓	33%
Automatisering	✓	30%
Applikations gateway	✓	50%
App service	✓	50%
API Administration	✓	20%
Samlet vurdering af Baseline		47%

Level 1	Relevans	Efterlevelse
Network Security	✓	50%
Logging & Monitoring	✓	65%
Identity & Access Control	✓	75%
Data Protection	✓	45%
Vulnerability Management	✓	55%
Identity & Access Management	✓	55%
Secure Configuration	✓	35%
Malware Defence	✓	85%
Data Recovery	✓	45%
Incident response	✓	35%
Pentest & Red team Excersise	✓	15%
Samlet vurdering af Level 1		51%

Level 2	Relevans	Efterlevelse
Network Security	✓	50%
Identity Management	✓	55%
Privileged Access	✓	55%
Data Protection	✓	35%
Asset Manageent	✓	35%
Logging & Threat Detection	✓	55%
Incident Response	✓	25%
Posture & Vulnerability Management	✓	5%
Endpoint Security	✓	95%
Backup & Recovery	✓	85%
Governance & Strategy	✓	15%
Samlet vurdering af Level 2		46%

Level 3	Relevans	Efterlevelse
Network Security	✓	50%
Identity Management	✓	5%
Privileged Access	✓	5%
Data Protection	✓	5%
Asset Manageent	✓	5%
Logging & Threat Detection	✓	5%
Incident Response	✓	5%
Posture & Vulnerability Management	✓	5%
Endpoint Security	✓	55%
Backup & Recovery	✓	55%
DevOps Security	✓	
Governance & Strategy	✓	15%
Samlet vurdering af Level 3		18%

Start med at udfylde Relevans og efterlevelse i C4...