ISO27002:2022 foranstaltninger						
Foranstaltning nummer	Foranstaltning titel	foranstaltningstype	informationssikkerhedsegenskaber	cybersikkerhedsbegreber	driftsmæssige kapaciteter	sikkerhedsdomæner
5.10	Acceptabel brug af information og understøttende aktiver	#Forbyggende	#Fortrolighed #Integritet #Tilgængelighed	#Beskyt	#Asset_management #Information_protection	#Governance_and_Ecosystem #Protection
5.21	Styring af informationssikkerhed i IKT-forsyningskæden	#Forebyggende	#Fortrolighed #Integritet #Tilgængelighed	#Identificer	#Sikring_af_leverandørforhold	#Ledelse_og_Økosystem #Beskyttelse
5.32	Intellektuelle ejendomsrettigheder	#Forebyggende	#Fortrolighed #Integritet #Tilgængelighed	#Identificer	#Legal_and_compli-ance	#Governance_and_Ecosystem
6.6	Hemmeligholdelses- og fortrolighedsaftale	#Forebyggende	#Fortrolighed	#Beskyt	#Medarbejdersikkerhed #Beskyttelse_af_information #Leverandørforhold	#Ledelse_og_Økosystem
7.9	Sikring af aktiver uden for organisationens områder	#Forebyggende	#Fortrolighed #Integritet #Tilgængelighed	#Beskyt	#Physical_security #Asset_management	#Protection
8.6	Kapacitetsstyring	#Forebyggende #Opdagende	#Integrity #Availability	#Identify #Protect #Detect	#Continuity	#Governance_and_Ecosystem #Protection
8.17	Synkronisering af ure	#Opdagende	#Integritet	#Beskyt #Opdag	#Styring_af_informa- tionssikkerheds- hændelser	#Beskyttelse #Forsvar
8.28	Sikker programmering	#Forebyggende	#Fortrolighed #Integritet #Tilgængelighed	#Beskyt	#Applikationssikkerhed #System_og_netværks- sikkerhed	#Beskyttelse

CIS-18 V8.1 Kontroller			
Kontrol nummer	Kontrol titel	Antal safeguards	Sammenhæng med ISO27002:2022 foranstaltning
CONTROL 1	Inventory and Control of Enterprise Assets	5	Foranstaltningens formål er at sikre, at information og understøttende aktiver beskyttes, anvendes og håndteres på behørig vis. Kontrollens formål er at "Actively manage all enterprise assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate"
CONTROL 4	Secure Configuration of Enterprise Assets and Software	12	ISO 5.32
CONTROL 3 Safeguard 3.7	Data Protection Establish and Maintain a Data Classification Scheme	14	ISO 6.6
CONTROL 8 Safeguard 8.4	Audit Log Management Standardize Time Synchronization	12	ISO 8.17 Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack. Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported
CIS Control 16	Application Software Security	7	CIS Safeguard 16.1: Establish and Maintain a Secure Application Development Process

Gruppe nummer: 10
Gruppe medlemmer: Medlem: 1, 2, 3 og 4
Senest redigeret: 23/09/2025
Version: V0.1