ISO 27001 bijlage A: Beheersdoelstellingen en beheersmaatregelen			Toepasselijkheid	Reden toepasselijkheid				Onderbouwing uitsluiting	Implementatie
2022	Onderwerp	Beheersmaatregelen		wet- en regel-geving	contract / klant	Baseline	risico / eigen eis		
	Betrekking op:	Brooklyn Partners	ja		/ : soms				Lopend On Hold
	Scope:	Informatiebeveiliging gerelateerd aan het verlenen van cyber securitydiensten en advies. Gedrag & cultuurprogramma's op het gebied van informatiebeveiliging, dit in overeenstemming met de verklaring van toepasselijkheid versie 3.0 van 6/1/2026.	nee		x : geheel				Gereed
	Versiedatum/nummer:	3 6/1/2026							Niet van toepassing
A.5	**Organisatorische Beheersmaatregelen**								
A5.1	Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en ***onderwerpspecifieke beleidsregels*** moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en ***erkend*** door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, worden beoordeeld.	**Ja**	x	/		x	**Niet van toepassing**	**Gereed**
A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	**ja**	x	/		x	**Niet van toepassing**	**Gereed**
A.5.3	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	**ja**				x	**Niet van toepassing**	**Gereed**
A.5.4	Management-verantwoordelijkheden	Het ***management*** moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de ***onderwerpspecifieke beleidsregels*** en procedures van de organisatie.	**Ja**		/	x	x	**Niet van toepassing**	**Gereed**
A.5.5	Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties ***leggen*** en onderhouden.	**ja**	x			/	**Niet van toepassing**	**Gereed**
A.5.6	Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen ***leggen*** en onderhouden.	**ja**	x		x		**Niet van toepassing**	**Gereed**
A.5.7	Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	**ja**				x	**Niet van toepassing**	**Gereed**
A.5.8	Informatiebeveiliging in projectmanagement	Informatiebeveiliging moet ***integraal*** onderdeel zijn van het projectmanagement.	**ja**	x	/		x	**Niet van toepassing**	**Gereed**
A.5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.	**ja**	x			x	**Niet van toepassing**	**Gereed**
A.5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	***Regels*** voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden geïdentificeerd, ***gedocumenteerd*** en geïmplementeerd.	**ja**				x	**Niet van toepassing**	**Gereed**
A.5.11	Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.	**ja**				x	**Niet van toepassing**	**Gereed**
A.5.12	Classificeren van informatie	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.	**ja**		/		x	**Niet van toepassing**	**Gereed**
A.5.13	Labelen van informatie	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	**ja**		/	x		**Niet van toepassing**	**Gereed**
A.5.14	Overdragen van informatie	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	**ja**			x	x	**Niet van toepassing**	**Gereed**

ISO 27001 bijlage A: Beheersdoelstellingen en beheersmaatregelen			Toepasselijkheid	Reden toepasselijkheid				Onderbouwing uitsluiting	Implementatie
2022	Onderwerp	Beheersmaatregelen		wet- en regel-geving	contract / klant	Baseline	risico / eigen eis		
A.5.15	Toegangsbeveiliging	Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	ja			x	x	Niet van toepassing	Gereed
A.5.16	Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.	ja	x			x	Niet van toepassing	Gereed
A.5.17	Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	ja			x	x	Niet van toepassing	Gereed
A.5.18	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het ***onderwerpspecifieke beleid*** en de regels inzake toegangsbeveiliging van de organisatie.	ja			x	x	Niet van toepassing	Gereed
A.5.19	Informatiebeveiliging in leveranciersrelaties	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.	ja	x			x	Niet van toepassing	Gereed
A.5.20	Adresseren van informatiebeveiliging in leveranciers-overeenkomsten	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	ja	x		x	x	Niet van toepassing	Gereed
A.5.21	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Er moeten processen en procedures worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen	ja			x	x	Niet van toepassing	Gereed
A.5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.	ja			x	x	Niet van toepassing	Gereed
A.5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	ja				x	Niet van toepassing	Gereed
A.5.24	Plannen en voorbereiden van het beheer van informatiebeveiligings-incidenten	De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, ***rollen en verantwoordelijkheden voor het beheer van informatie- beveiligingsincidenten te definiëren, vast te stellen en te communiceren.***	ja	x			x	Niet van toepassing	Gereed
A.5.25	Beoordelen van en besluiten over informatiebeveiligings-gebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	ja	/	/	x	x	Niet van toepassing	Gereed
A.5.26	Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de ***gedocumenteerde*** procedures.	ja			x	x	Niet van toepassing	Gereed
A.5.27	Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	ja	/			x	Niet van toepassing	Gereed
A.5.28	Verzamelen van bewijsmateriaal	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	ja	/			x	Niet van toepassing	Gereed
A.5.29	Informatiebeveiliging tijdens een verstoring	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Nee	x		x	x	De organisatie heeft ervoor gekozen maatregel A.5.29 uit te sluiten op basis van de aard van de dienstverlening en de risico-acceptatie. Onze dienstverlening (Cyber Security Awareness) betreft geen real-time kritische infrastructuur.	Niet van toepassing

ISO 27001 bijlage A: Beheersdoelstellingen en beheersmaatregelen			Toepasselijkheid	Reden toepasselijkheid				Onderbouwing uitsluiting	Implementatie
2022	Onderwerp	Beheersmaatregelen		wet- en regel-gevin g	contract / klant	Baseline	risico / eigen eis		
A.5.30	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoel- stellingen en ICT-continuïteitseisen.	**Nee**	x			x	Uit onze Business Impact Analyse (BIA) blijkt dat er geen bedrijfsprocessen zijn die onmiddellijke ICT-herstelacties vereisen om onacceptabele schade te voorkomen. Onze dienstverlening (Cyber Security Awareness) is niet 'mission critical' of real-time van aard. Een tijdelijke uitval van systemen (tot enkele dagen) leidt niet tot levensbedreigende situaties of onoverkomelijke financiële schade.	**Niet van toepassing**
A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, moeten worden geïdentificeerd, ***gedocumenteerd*** en actueel gehouden.	**ja**	x			x	**Niet van toepassing**	**Gereed**
A.5.32	Intellectuele-eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.	**ja**	x			x	**Niet van toepassing**	**Gereed**
A.5.33	Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ***ongeoorloofde*** vrijgave.	**ja**	x			x	**Niet van toepassing**	**Gereed**
A.5.34	Privacy en bescherming van persoonsgegevens	De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen ***identificeren*** en eraan voldoen.	**ja**	x			x	**Niet van toepassing**	**Gereed**
A.5.35	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, moeten onafhankelijk en met geplande tussenpozen ***of zodra zich belangrijke veranderingen voordoen***, worden beoordeeld.	**ja**			x	x	**Niet van toepassing**	**Gereed**
A.5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het ***onderwerpspecifieke beleid***, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	**ja**	x	x		x	**Niet van toepassing**	**Gereed**
A.5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden ***gedocumenteerd*** en beschikbaar worden gesteld aan ***het personeel*** dat ze nodig heeft.	**ja**	x			x	**Niet van toepassing**	**Gereed**
A.6	**Mensgerichte Beheersmaatregelen**								
A.6.1	Screening	De achtergrond van alle kandidaten voor een dienstverband moet worden gecontroleerd voordat ze bij de organisatie in dienst treden ***en daarna op gezette tijden worden herhaald.*** Hierbij moet rekening worden gehouden met de toepasselijke wet- en regelgeving en ethische overwegingen, en deze controle moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	**ja**				x	**Niet van toepassing**	**Gereed**
A.6.2	Arbeidsovereenkomst	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	**ja**		/		x	**Niet van toepassing**	**Gereed**
A.6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, ***onderwerpspecifieke beleidsregels*** en procedures van de organisatie, voor zover relevant voor hun functie, krijgen.	**ja**	/	/	x	x	**Niet van toepassing**	**Gereed**

ISO 27001 bijlage A: Beheersdoelstellingen en beheersmaatregelen			Toepasselijkheid	Reden toepasselijkheid				Onderbouwing uitsluiting	Implementatie
2022	Onderwerp	Beheersmaatregelen		wet- en regel-geving	contract / klant	Baseline	risico / eigen eis		
A.6.4	Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen personeel ***en andere belanghebbenden*** die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.	**ja**				x	**Niet van toepassing**	**Gereed**
A.6.5	Verantwoordelijkheden na beëindiging of wijziging vanhet dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, moeten worden gedefinieerd, ***gehandhaafd*** en gecommuniceerd aan relevant personeel en andere belanghebbenden.	**ja**		/		x	**Niet van toepassing**	**Gereed**
A.6.6	Vertrouwlijkheids- of geheimhoudings-overeenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, ***gedocumenteerd***, regelmatig worden beoordeeld ***en ondertekend door personeel en andere relevante belanghebbenden.***	**ja**	/	/		x	**Niet van toepassing**	**Gereed**
A.6.7	Werken op afstand	***Wanneer personeel op afstand werkt,*** moeten er beveiligingsmaatregelen worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	**ja**				x	**Niet van toepassing**	**Gereed**
A.6.8	Melden van informatiebeveiligings-gebeurtenissen	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligings- gebeurtenissen tijdig via passende kanalen kan melden.	**ja**	x	/	x	x	**Niet van toepassing**	**Gereed**
A.7	**Fysieke Beheersmaatregelen**								
A.7.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.	**ja**				x	**Niet van toepassing**	**Gereed**
A.7.2	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.	**ja**				x	**Niet van toepassing**	**Gereed**
A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	**ja**				x	**Niet van toepassing**	**Gereed**
A.7.4	Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	**ja**				x	**Niet van toepassing**	**Gereed**
A.7.5	Beschermen tegen fysieke en omgevingsdreigingen	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd.	**Nee**	x			x	Op ons eigen kantoor is de beveiliging gericht op de veiligheid van medewerkers en endpoints (laptops). Wij mitigeren risico's door: - Inbraakbeveiliging (deugdelijk hang- en sluitwerk conform bouwbesluit). - Brandveiligheid (aanwezigheid brandblussers/rookmelders conform eisen verhuurder/brandweer). - Clean Desk Policy (geen gevoelige data onbeheerd achterlaten).	**Niet van toepassing**
A.7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	**Nee**	x			x	De organisatie heeft maatregel A.7.6 uitgesloten omdat er binnen de fysieke locatie (het gehuurde kantoor) geen ruimtes zijn gedefinieerd als "Beveiligde Zone" (Secure Area) zoals bedoeld in de ISO 27001 norm.	**Niet van toepassing**
A.7.7	Clean desk' en 'clear screen'	Er moeten 'clear desk'-***regels*** voor papieren documenten en verwijderbare opslagmedia en 'clean screen'-***regels*** voor informatieverwerkende faciliteiten worden ***gedefinieerd en op passende wijze worden afgedwongen.***	**ja**	/			x	**Niet van toepassing**	**Gereed**

ISO 27001 bijlage A: Beheersdoelstellingen en beheersmaatregelen			Toepasselijkheid	Reden toepasselijkheid				Onderbouwing uitsluiting	Implementatie
2022	Onderwerp	Beheersmaatregelen		wet- en regel-geving	contract / klant	Baseline	risico / eigen eis		
A.7.8	Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	**Nee**	x			x	De fysieke omgeving en voorzieningen (zoals stroomvoorziening en klimaatbeheersing) worden beheerd door de verhuurder van het kantoorpand. De organisatie heeft geen invloed op de installatietechnische plaatsing van voorzieningen.	**Niet van toepassing**
A.7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	**ja**				x	**Niet van toepassing**	**Gereed**
A.7.10	Opslagmedia	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	**ja**				x	**Niet van toepassing**	**Gereed**
A.7.11	Nutsvoorzieningen	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	**Nee**	x			x	De organisatie heeft deze maatregel uitgesloten omdat de fysieke locatie (het kantoor) geen kritieke informatieverwerkende faciliteiten huisvest die continue stroomvoorziening of specifieke klimaatbeheersing vereisen.	**Niet van toepassing**
A.7.12	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	**Nee**	x			x	De organisatie is gevestigd in een gehuurd pand (bedrijfsverzamelgebouw). De aanleg, het onderhoud en de bescherming van de vaste bekabeling in muren, vloeren en plafonds (stroom en internet) vallen onder de verantwoordelijkheid van de verhuurder. De organisatie heeft geen bevoegdheid of mogelijkheid om bouwkundige beschermingsmaatregelen aan deze bekabeling te treffen.	**Niet van toepassing**
A.7.13	Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en ***betrouwbaarheid*** van informatie te garanderen.	**ja**				x	**Niet van toepassing**	**Gereed**
A.7.14	Veilig verwijderen of hergebruiken van apparatuur	Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	**ja**			x	x	**Niet van toepassing**	**Gereed**
A.8	**Technologische Beheersmaatregelen**								
A.8.1	User endpoint devices'	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	**ja**			x	x	**Niet van toepassing**	**Gereed**
A.8.2	Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	**ja**			x	x	**Niet van toepassing**	**Gereed**
A.8.3	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde ***onderwerpspecifieke beleid*** inzake toegangsbeveiliging.	**ja**			x	x	**Niet van toepassing**	**Gereed**
A.8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ***ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.***	**Ja**				x	**Niet van toepassing**	**Gereed**
A.8.5	Beveiligde authenticatie	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het ***onderwerpspecifieke beleid*** inzake toegangsbeveiliging.	**ja**			x	x	**Niet van toepassing**	**Gereed**
A.8.6	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	**ja**	x			x	**Niet van toepassing**	**Gereed**

ISO 27001 bijlage A: Beheersdoelstellingen en beheersmaatregelen			Toepasselijkheid	Reden toepasselijkheid				Onderbouwing uitsluiting	Implementatie
2022	Onderwerp	Beheersmaatregelen		wet- en regel-geving	contract / klant	Baseline	risico / eigen eis		
A.8.7	Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebuikersbewustzijn.	ja				x	Niet van toepassing	Gereed
A.8.8	Beheer van technische kwetsbaarheden	Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten passende maatregelen worden getroffen.	ja			x	x	Niet van toepassing	Gereed
A.8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, ***gedocumenteerd***, geïmplementeerd, gemonitord en beoordeeld.	ja				x	Niet van toepassing	Gereed
A.8.10	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.	ja				x	Niet van toepassing	Gereed
A.8.11	Maskeren van gegevens	Gegevens moeten worden gemaskeerd overeenkomstig het ***onderwerpspecifieke beleid*** inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	ja				x	Niet van toepassing	Gereed
A.8.12	Voorkomen van gegevenslekken (data leakage prevention)	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	ja	x			x	Niet van toepassing	Gereed
A.8.13	Back-up van informatie	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen ***onderwerpspecifieke beleid*** inzake back-ups.	ja	x		x	x	Niet van toepassing	Gereed
A.8.14	Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	ja			x	x	Niet van toepassing	Gereed
A.8.15	Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	ja			x	x	Niet van toepassing	Gereed
A.8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	ja				x	Niet van toepassing	Gereed
A.8.17	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.	ja				x	Niet van toepassing	Gereed
A.8.18	Gebruik van speciale hulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.	ja				x	Niet van toepassing	Gereed
A.8.19	Installeren van software op operationele systemen	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	ja				x	Niet van toepassing	Gereed
A.8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	ja			x	x	Niet van toepassing	Gereed
A.8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en ***gemonitord***.	ja				x	Niet van toepassing	Gereed
A.8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	ja			x	x	Niet van toepassing	Gereed

ISO 27001 bijlage A: Beheersdoelstellingen en beheersmaatregelen			Toepasselijkheid	Reden toepasselijkheid				Onderbouwing uitsluiting	Implementatie
2022	Onderwerp	Beheersmaatregelen		wet- en regel-geving	contract / klant	Baseline	risico / eigen eis		
A.8.23	Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	**Nee**				x	Als Cyber Security Awareness-specialist omvatten onze werkzaamheden het onderzoeken van actuele dreigingen, het analyseren van phishing-voorbeelden en het ontwikkelen van simulaties. Dit vereist ongehinderde toegang tot het internet, inclusief websites die door standaard filters als 'kwaadaardig', 'uncategorized' of 'suspicious' zouden worden geblokkeerd. Het implementeren van strenge webfilters zou onze operationele slagkracht belemmeren.	**Niet van toepassing**
A.8.24	Gebruik van cryptografie	***Regels*** voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden ***gedefinieerd*** en geïmplementeerd.	**ja**	/		x	x	**Niet van toepassing**	**Gereed**
A.8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	**Ja**				x	**Niet van toepassing**	**Gereed**
A.8.26	Toepassingsbeveiligingseisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	**ja**				x	**Niet van toepassing**	**Gereed**
A.8.27	Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, ***gedocumenteerd***, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	**Ja**				x	**Niet van toepassing**	**Gereed**
A.8.28	Veilig coderen	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	**ja**				x	**Niet van toepassing**	**Gereed**
A.8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	**Ja**				x	**Niet van toepassing**	**Gereed**
A.8.30	Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	**Nee**	x	x	x	x	De organisatie heeft maatregel A.8.30 uitgesloten omdat er geen sprake is van uitbesteding van softwareontwikkelingstaken aan externe partijen.	**Niet van toepassing**
A.8.31	Scheiding van ontwikkel-, test- en productomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	**Ja**				x	**Niet van toepassing**	**Gereed**
A.8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	**ja**	x		x	x	**Niet van toepassing**	**Gereed**
A.8.33	Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en ***beheerd***.	**Ja**				x	**Niet van toepassing**	**Gereed**
A.8.34	Bescherming van informatiesystemen tijdens audits	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en ***overeengekomen tussen de tester en het verantwoordelijke management.***	**ja**	x			x	**Niet van toepassing**	**Gereed**