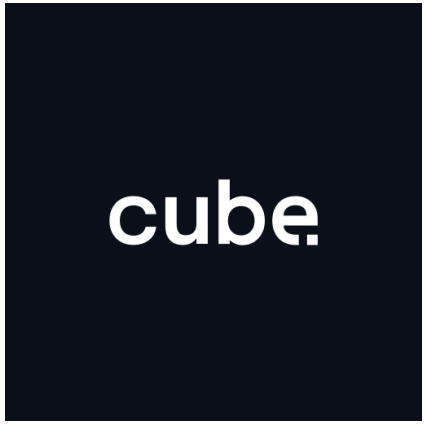
Verklaring van Toepasselijkheid (VvT) van Cube B.V.



Datum	03-28-2024
Norm	ISO/IEC 27001:2023
Versie	1.0
Inleiding	Dit document omvat de Verklaring van Toepasselijkheid (VVT) ten behoeve van de ISO 27001 Annex A beheersmaatregelen die door Cube B.V. worden toegepast. De doelstelling van dit document is het identificeren van de toepasselijke beheersmaatregelen die geïmplementeerd dienen te zijn om de bedreigingen te controleren en te managen. De beheersmaatregelen zijn geïdentificeerd op basis van de opgenomen beheersmaatregelen.
Directieverklaring	De Directie verklaart hierbij de in deze VVT vermelde beheersmaatregelen bekrachtigd in relatie tot de uitgevoerde doelstellingen en risicoanalyses en accepteert eventuele restrisico's van eventuele niet genomen maatregelen.
Toelichting	De reden van selectie of indien de beheersmaatregel niet van toepassing is wordt weergegeven alsmede de relatie met doelstelling en/of risico. De getoonde doelstellingen, baselines en risico's zijn te openen vanuit de CyberManager en/of zijn er verwijzingen gemaakt naar contract of wetgeving die een relatie hebben met de beheersmaatregel. De mate van implementatie van de benoemde maatregelen kan worden nagezien in het geautomatiseerd managementsysteem dat is vastgelegd in de CyberManager.

Domein - A Beheersmaatregelen					
Subdomein	Control		v.T.	Reden	Implementatie
A.5 Organisatorische beheersmaatregelen	A.5.1 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 of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	Ja	Risico	Ja
	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	Risico	Ja
	A.5.3 Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	Ja	Risico	Ja
	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	Risico	Ja
	A.5.5 Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en onderhouden.	Ja	Risico	Ja
	A.5.6 Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	Ja	Risico	Ja
	A.5.7 Informatie en analyses over dreigingen (Nieuw)	Informatie met betrekking tot informatiebeveiligingsdreigingen moeten worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren.	Ja	Risico	Ja
	A.5.8 Informatiebeveiliging in projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	Ja	Risico	Ja

	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	Risico	Ja
	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 vastgesteld, gedocumenteerd en geïmplementeerd.	Ja	Risico	Ja
	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 te retourneren.	Ja	Risico	Ja
	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 belanghebbenden.	Ja	Risico	Ja
	A.5.13 Labelen van informatie	Om informatie te labelen moet een passende reeks procedures worden vastgesteld en geïmplementeerd in overeenstemming met het informatie classificatieschema dat is vastgesteld door de organisatie.	Ja	Risico	Ja
	A.5.14 Overdragen van informatie	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn vastgesteld voor alle soorten van overdracht binnen de organisatie en tussen de organisatie en andere partijen.	Ja	Risico	Ja
	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	Risico	Ja
	A.5.16 Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.	Ja	Risico	Ja
	A.5.17 Beheren van authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheerproces waarvan het informeren	Ja	Risico	Ja

		van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.			
	A.5.18 Toegangsrechten	Toegangsrechten met betrekking tot informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerp specifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.	Ja	Risico	Ja
	A.5.19 Informatiebeveiliging in leveranciersrelaties	Er moeten processen en procedures te worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheren.	Ja	Risico	Ja
	A.5.20 Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	Ja	Risico	Ja
	A.5.21 Beheren van informatiebeveiliging in de ICT-keten	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheren.	Ja	Risico	Ja
	A.5.22 Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie moet de informatiebeveiligingspraktijken en de leveranciersdiensten regelmatig monitoren, beoordelen, evalueren en veranderingen daarin beheren.	Ja	Risico	Ja
	A.5.23 Informatiebeveiliging voor het gebruik van clouddiensten (Nieuw)	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	Ja	Risico	Ja
	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 informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Ja	Risico	Ja

	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	Risico	Ja
	A.5.26 Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Risico	Ja
	A.5.27 Leren van informatiebeveiligings-incidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Ja	Risico	Ja
	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	Risico	Ja
	A.5.29 Informatiebeveiliging tijdens een verstoring	De organisatie moet plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja	Risico	Ja
	A.5.30 ICT-gereedheid voor bedrijfscontinuïteit (Nieuw)	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja	Risico	Ja
	A.5.31 Wettelijke, statutaire, regelgevende en contractuele eisen	Eisen van 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 vastgesteld, gedocumenteerd en actueel gehouden.	Ja	Risico	Ja
	A.5.32 Intellectuele-eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele eigendomsrechten te beschermen.	Ja	Risico	Ja
	A.5.33 Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja	Risico	Ja
	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	Risico	Ja

	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	Risico	Ja
	A.5.36 Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerp specifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	Ja	Risico	Ja
	A.5.37 Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.	Ja	Risico	Ja
A.6 Mensgerichte beheersmaatregelen	A.6.1 Screening	De achtergrond van alle kandidaten die in aanmerking komen voor posities binnen de organisatie 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, voorschriften 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	Risico	Ja
	A.6.2 Arbeidsovereenkomst	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Ja	Risico	Ja
	A.6.3 Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden moeten een passend(e) bewustwording van, opleiding, training en bijscholing in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerp specifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen.	Ja	Risico	Ja
	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	Ja	Risico	Ja

		schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.			
	A.6.5 Verantwoordelijkheden na beëindiging of wijziging van het 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	Risico	Ja
	A.6.6 Vertrouwelijkheids- of geheimhoudingsovereen komsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geeïdentificeerd, gedocumenteerd, regelmatig worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	Ja	Risico	Ja
	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	Risico	Ja
	A.6.8 Melden van informatiebeveiligingsgeb eurtenissen	De organisatie moet zorgen voor een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Ja	Risico	Ja
A.7 Fysieke beheersmaatregelen	A.7.1 Fysieke beheersmaatregelen	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definieren en te gebruiken.	Ja	Risico	Ja
	A.7.2 Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangscontroles en toegangspunten.	Ja	Risico	Ja
	A.7.3 Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja	Risico	Ja
	A.7.4 Monitoren van de fysieke beveiliging (Nieuw)	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Ja	Risico	Ja

	A.7.5 Beschermen tegen fysieke en omgevingsdreigingen	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen van de infrastructuur, worden ontworpen en geiuml;mplementeerd.	Ja	Risico	Ja
	A.7.6 Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geiuml;mplementeerd.	Ja	Risico	Ja
	A.7.7 ‘Clear desk’ en ‘clear screen’	Er moeten clear desk-regels voor papieren documenten en verwijderbare opslagmedia en clear screen-regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze ten uitvoer worden gebracht.	Ja	Risico	Ja
	A.7.8 Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	Ja	Risico	Ja
	A.7.9 Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	Ja	Risico	Ja
	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	Risico	Ja
	A.7.11 Nutsvoorzieningen	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja	Risico	Ja
	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.	Ja	Risico	Ja
	A.7.13 Onderhoud van apparatuur	Apparatuur behoort op de juiste wijze te worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	Ja	Risico	Ja
	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	Ja	Risico	Ja

		gelicenseerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.			
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	Risico	Ja
	A.8.2 Speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	Ja	Risico	Ja
	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	Risico	Ja
	A.8.4 Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en software bibliotheken moet op passende wijze worden beheerd.	Ja	Risico	Ja
	A.8.5 Beveiligde authenticatie	Er moeten beveiligde authenticatie technologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerp specifieke of aanvullende beleid inzake toegangsbeveiliging.	Ja	Risico	Ja
	A.8.6 Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd overeenkomstig de huidige en verwachte capaciteitseisen.	Ja	Risico	Ja
	A.8.7 Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikers bewustzijn.	Ja	Risico	Ja
	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	Risico	Ja
	A.8.9 Configuratiebeheer (Nieuw)	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja	Risico	Ja

	A.8.10 Wissen van informatie (Nieuw)	In informatiesystemen, apparaten of andere opslagmedia, moet opgeslagen informatie worden gewist als deze niet langer nodig is.	Ja	Risico	Ja
	A.8.11 Maskeren van gegevens (Nieuw)	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	Risico	Ja
	A.8.12 Voorkomen van gegevenslekken (Data leakage prevention) (Nieuw)	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	Risico	Ja
	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	Risico	Ja
	A.8.14 Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Risico	Ja
	A.8.15 Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja	Risico	Ja
	A.8.16 Monitoren van activiteiten (Nieuw)	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden genomen om potentiële informatiebeveiligingsincidenten te evalueren.	Ja	Risico	Ja
	A.8.17 Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdsbronnen.	Ja	Risico	Ja
	A.8.18 Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moeten worden beperkt en nauwkeurig worden gecontroleerd.	Ja	Risico	Ja

	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	Risico	Ja
	A.8.20 Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Risico	Nee
	A.8.21 Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverlening eisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja	Risico	Ja
	A.8.22 Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Ja	Risico	Ja
	A.8.23 Toepassen van webfilters (Nieuw)	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja	Risico	Ja
	A.8.24 Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moet worden gedefinieerd en geïmplementeerd.	Ja	Risico	Ja
	A.8.25 Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Ja	Risico	Ja
	A.8.26 Toepassings beveiligingseisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja	Risico	Ja
	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	Risico	Ja
	A.8.28 Veilig coderen (Nieuw)	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	Ja	Risico	Ja
	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	Risico	Ja

	A.8.30 Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Nee	Niet van toepassing, Cube besteedt geen softwareontwikkeling uit.	n.v.t.
	A.8.31 Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moet worden gescheiden en beveiligd.	Ja	Risico	Ja
	A.8.32 Wijzigingsbeheer	Wijzigingen in informatieverwerkingsfaciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	Ja	Risico	Ja
	A.8.33 Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Ja	Risico	Ja
	A.8.34 Bescherming van informatiesystemen tijdens audits	Audits en andere borgingsactiviteiten waarbij operationele systemen worden beoordeeld moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management	Ja	Risico	Ja