



SCOPE **4** MATION

VERKLARING VAN TOEPASSELIJKHEID

ISO27001:2022 v1.2 06/03/2025



INHOUDSOPGAVE

INLEIDING	3
DIRECTIEVERKLARING	3
SCOPE	3
VERSIE	3
VERKLARING VAN TOEPASSELIJKHEID	4
5 ORGANISATORISCHE BEHEERSMAATREGELEN	4
6 MENS GERICHTE MAATREGELEN	7
7 FYSIEKE BEHEERSMAATREGELEN	8
8 TECHNOLOGISCHE BEHEERSMAATREGELEN	9

INLEIDING

Dit document omvat de Verklaring van Toepasselijkheid (VVT) ten behoeve van de certificering voor de ISO27001-standaard. Het doel van dit document is het identificeren van de toepasselijke beheersmaatregelen welke geïmplementeerd dienen te zijn om de bedreigingen tegen Scope4mation B.V. en bedrijfsprocessen te controleren en te managen.

De van toepassing zijnde beheersmaatregelen zijn geïdentificeerd op basis van de beheersmaatregelen benoemd in de ISO27001 norm Annex 1. Voor de van toepassing zijnde beheersmaatregel wordt verwezen naar de gedefinieerde ISO27002 'best practices' richtlijnen welke specifiek zijn gemaakt voor toepassing in Scope4mation B.V. bedrijfsprocessen. Indien een beheersmaatregel niet van toepassing is, wordt hiervoor een verklaring gegeven.

DIRECTIEVERKLARING

De Directie van Scope4mation B.V. verklaart hierbij de in deze VVT vermelde maatregelen bekrachtigd in relatie tot de uitgevoerde risicoanalyses en accepteert het restrisico van eventuele niet genomen maatregelen.

Ede, 01/11/2025,



J.A.C. Ale

SCOPE

Ontwikkeling, installatie en ondersteuning van software voor data integratie op basis van SaaS en on-premise.

VERSIE

De actuele versie is V1.2

VERKLARING VAN TOEPASSELIJKHEID

5 ORGANISATORISCHE BEHEERSMAATREGELEN

Norm	Omschrijving	Beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag RB: Risicobeoordeling WG: Wetgeving CV: Contractuele Verplichting
5.1	Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en onderwerp specifieke 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		<input checked="" type="checkbox"/> RB <input checked="" type="checkbox"/> WG <input checked="" type="checkbox"/> CV
5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.3	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.4	Management-verantwoordelijkheden	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerp specifieke beleidsregels en procedures van de organisatie.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.5	Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en onderhouden.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.6	Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.7	Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.8	Informatiebeveiliging in projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.13	Labelen van informatie	Om informatie te labelen moet een passende reeks procedures worden vastgesteld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV

Norm	Omschrijving	Beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag RB: Risicobeoordeling WG: Wetgeving CV: Contractuele Verplichting
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.16	Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.17	Beheren van authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie moet worden beheerd door middel van een beheerproces waarvan het informeren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.18	Toegangsrechten	Toegangsrechten met betrekking tot 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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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 beheren.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.20	Adresseren van informatiebeveiliging in leverancierovereenkomsten	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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 daaraan beheren.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	De organisatie moet plannen op stellen 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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.26	Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.29	Informatiebeveiliging tijdens een verstoring	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.30	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input checked="" type="checkbox"/> CV

Norm	Omschrijving	Beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag RB: Risicobeoordeling WG: Wetgeving CV: Contractuele Verplichting
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		<input checked="" type="checkbox"/> RB <input checked="" type="checkbox"/> WG <input checked="" type="checkbox"/> CV
5.32	Intellectuele eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele eigendomsrechten te beschermen.	Ja		<input checked="" type="checkbox"/> RB <input checked="" type="checkbox"/> WG <input checked="" type="checkbox"/> CV
5.33	Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja		<input checked="" type="checkbox"/> RB <input checked="" type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input checked="" type="checkbox"/> WG <input checked="" type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatie verwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar te worden gesteld aan het personeel dat ze nodig heeft.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV

6 MENS GERICHTE MAATREGELEN

Norm	Omschrijving	Beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag RB: Risicobeoordeling WG: Wetgeving CV: Contractuele Verplichting
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input checked="" type="checkbox"/> CV
6.2	Arbeidsovereenkomst	In arbeidsovereenkomsten behoort te worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden behoren 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, te krijgen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
6.4	Disciplinaire procedure	Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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 behoren te worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
6.7	Werken op afstand	Wanneer personeel op afstand werkt, behoren er beveiligingsmaatregelen te worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
6.8	Melden van informatiebeveiligingsgebeurtenissen	De organisatie behoort te voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV

7 FYSIEKE BEHEERSMAATREGELLEN

Norm	Omschrijving	Beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag RB: Risicobeoordeling WG: Wetgeving CV: Contractuele Verplichting
7.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
7.2	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangscontroles en toegangspunten.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
7.4	Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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 geïmplementeerd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
7.8	Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
7.11	Nutsvoorzieningen	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
7.13	Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV

8 TECHNOLOGISCHE BEHEERSMAATREGELEN

Norm	Omschrijving	Beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag RB: Risicobeoordeling WG: Wetgeving CV: Contractuele Verplichting
8.1	'User endpoint devices'	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.2	Speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten moeten worden beperkt en beheerd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.5	Beveiligde authenticatie	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke of aanvullende beleid inzake toegangsbeveiliging.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.6	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd overeenkomstig de huidige en verwachte capaciteitseisen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.7	Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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 moetende passende maatregelen worden getroffen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.10	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer nodig is.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input checked="" type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.14	Redundantie van informatieverwerken de faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.15	Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
Norm	Omschrijving	Beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag RB: Risicobeoordeling WG: Wetgeving

					CV: Contractuele Verplichting
8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden genomen om potentiële informatiebeveiligingsincidenten te evalueren.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.17	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdsbronnen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.18	Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig te worden gecontroleerd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.23	Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.26	Toepassingsbeveiligingseisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.28	Veilig coderen	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.30	Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.31	Scheiding van ontwikkel-, testen productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkingsfaciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
Norm	Omschrijving	Beheersmaatregel	Relevant en geïmplementeerd	Onderboewing uitsluiting	Grondslag RB: Risicobeoordeling WG: Wetgeving CV: Contractuele Verplichting
8.33	Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Ja		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV

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		<input checked="" type="checkbox"/> RB <input type="checkbox"/> WG <input type="checkbox"/> CV
------	---	---	----	--	--