Verklaring van Toepasselijkheid

Version: v2.1 **Datum: 09-05-2025**

Versie 2.1 09-05-2025

				Waarom van toepassing?			Waarom niet van toepassing?				
Hoofdstuk & naam	**Omschrijving**	**Van toepassing?**	**Niet van toepassing?**	**Wetgeving**	**Contractueel**	**Risico analyse**	**Waarom niet van toepassing?**	**Interface**	**Uitbesteed**	**Implementatie**	**Volledig geïmplementeerd?**
Onbekend hoofdstuk											
5.01 Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels behoren te 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, te worden beoordeeld.	X				Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02), Beleids-/gedragsregels niet worden nageleefd door geen verantwoordelijke aangewezen voor beleid (03)		N.V.T.	N.V.T.	B01 Informatiebeveiligingsbeleid, B02 Documentbeheer	Ja
5.02 Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	X				Beleids-/gedragsregels niet worden nageleefd door geen verantwoordelijke aangewezen voor beleid (03), Niet compliant aan informatiebeveiligingsnorm door onvoldoende continuïteit SO/ PQS Coördinator (41)		N.V.T.	N.V.T.	B01 Informatiebeveiligingsbeleid	Ja
5.03 Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden behoren te worden gescheiden.	X				Fraude en misbruik van bedrijfsmiddelen (04)		N.V.T.	N.V.T.	B01 Informatiebeveiligingsbeleid	Ja
5.04 Managementverantwoordelijkheden	Het management behoort van al het personeel te eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.	X				Beleids-/gedragsregels niet worden nageleefd door geen verantwoordelijke aangewezen voor beleid (03), Informatiebeveiligingsincidenten veroorzaakt door verkeerd gedrag en/of onvoldoende kennis (08), Niet naleven regels en of taken niet goed uitvoeren (09), Bedrijfsmiddelen die slecht worden beheerd en niet voldoen aan beleid (10)		N.V.T.	N.V.T.	B01 Informatiebeveiligingsbeleid, B09 Veilig personeel	Ja
5.05 Contact met overheidsinstanties	De organisatie behoort contact met de relevante instanties te leggen en te onderhouden.	X				Als organisatie niet adequaat kunnen reageren op calamiteiten en incidenten. (05)		N.V.T.	N.V.T.	B05 Incidentmanagement, B08 Voldoen aan overeenkomsten wet- en regelgeving	Ja
5.06 Contact met speciale belangengroepen	De organisatie behoort contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen te leggen en te onderhouden.	X				Onvoldoende op de hoogte zijn van actuele kwetsbaarheden en nieuwe technologie (01), Virussen/hacking door gebrek inzicht/detectie in technische kwetsbaarheden (28)		N.V.T.	N.V.T.	B08 Voldoen aan overeenkomsten wet- en regelgeving	Ja
5.07 Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen behoort te worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren.	X				Virussen/hacking door gebrek inzicht/detectie in technische kwetsbaarheden (28)		N.V.T.	N.V.T.	B14 ICT beheer	Ja
5.08 Informatiebeveiliging in projectmanagement	Informatiebeveiliging behoort te worden geïntegreerd in projectmanagement.	X				Uitvoering van een project met onvoldoende beveiligingsmaatregelen (06)		N.V.T.	N.V.T.	B04 Risicomanagement, B18 Wijzigingsbeheer	Ja
5.09 Inventarisatie van informatie en andere gerelateerde bedr	Er behoort een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, te worden opgesteld en onderhouden.	X				Bedrijfsmiddelen die slecht worden beheerd en niet voldoen aan beleid (10)		N.V.T.	N.V.T.	B03 Informatieclassificatie en labeling, B09 Veilig personeel, B13 Beheer bedrijfsmiddelen	Ja
5.10 Aanvaardbaar gebruik van informatie en andere gerelateer	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen behoren te worden vastgesteld, gedocumenteerd en geïmplementeerd.	X				Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02), Informatie/bedrijfsmiddelen verkeerd worden behandeld en/of onvoldoende worden beschermd. (13)		N.V.T.	N.V.T.	B03 Informatieclassificatie en labeling	Ja
5.11 Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naargelang de situatie, behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst te retourneren.	X				Informatie kwijtraakt, of in ongeautoriseerde handen valt (11)		N.V.T.	N.V.T.	B09 Veilig personeel, B13 Beheer bedrijfsmiddelen	Ja
5.12 Classificeren van informatie	Informatie behoort te worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante belanghebbenden.	X				Informatie verkeerd wordt behandeld en/of onvoldoende wordt beschermd. (12)		N.V.T.	N.V.T.	B03 Informatieclassificatie en labeling	Ja
5.13 Labelen van informatie	Om informatie te labelen behoort een passende reeks procedures te worden vastgesteld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	X				Informatie verkeerd wordt behandeld en/of onvoldoende wordt beschermd. (12)		N.V.T.	N.V.T.	B03 Informatieclassificatie en labeling	Ja
5.14 Overdragen van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn vastgesteld voor alle soorten van overdracht binnen de organisatie en tussen de organisatie en andere partijen.	X			X	Onveilig transport van informatie en onveilige toegang tot informatie in toepassingsdiensten via net (30), Onderzoeksresultaten in verkeerde handen vallen (47)		N.V.T.	N.V.T.	B12 Leveranciersmanagement, Communicatieblad	Ja
5.15 Toegangsbeveiliging	Er behoren regels op basis van bedrijfs- en informatiebeveiligingseisen te worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	X				Ongeautoriseerde toegang of toegang die breder is dan het 'need tot know' principe. (14)		N.V.T.	N.V.T.	B11 Autorisatiebeheer	Ja
5.16 Identiteitsbeheer	De volledige levenscyclus van identiteiten behoort te worden beheerd.	X				Ongeautoriseerde toegang of toegang die breder is dan het 'need tot know' principe. (14)		N.V.T.	N.V.T.	B11 Autorisatiebeheer	Ja
5.17 Beheren van authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het informeren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	X				Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02), Ongeautoriseerde toegang of toegang die breder is dan het 'need tot know' principe. (14), Ongeautoriseerde toegang door ontbreken inlogbeveiliging (16)		N.V.T.	N.V.T.	B11 Autorisatiebeheer	Ja

5.18 Toegangsrechten	Toegangsrechten met betrekking tot informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.	X				Ongeautoriseerde toegang of toegang die breder is dan het 'need tot know' principe. (14)		N.V.T.	N.V.T.	B09 Veilig personeel, B11 Autorisatiebeheer	Ja
5.19 Informatiebeveiliging in leveranciersrelaties	Er behoren processen en procedures te worden vastgesteld en geimplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheren.	X				Inadequate leveranciers en aanschaf slechte ICT-middelen (33)		N.V.T.	N.V.T.	B12 Leveranciersmanagement	Ja
5.20 Adresseren van informatiebeveiliging in leveranciersovere	Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	X				Inadequate leveranciers en aanschaf slechte ICT-middelen (33)		N.V.T.	N.V.T.	B12 Leveranciersmanagement	Ja
5.21 Beheren van informatiebeveiliging in de ICT-keten	Er behoren processen en procedures te worden vastgesteld en geimplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheren.	X				Inadequate leveranciers en aanschaf slechte ICT-middelen (33)		N.V.T.	N.V.T.	B12 Leveranciersmanagement	Ja
5.22 Monitoren beoordelen en het beheren van wijzigingen var	De organisatie behoort de informatiebeveiligingspraktijken en de leveranciersdiensten regelmatig te monitoren, beoordelen, evalueren en veranderingen daaraan te beheren.	X				Gewenst beveiligingsniveau daalt door slechte sturing leveranciers bij uitbesteden van diensten (34)		N.V.T.	N.V.T.	B12 Leveranciersmanagement	Ja
5.23 Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beeindigen van clouddiensten behoren overeenkomstig de informatiebeveiligingseisen van de organisatie te worden opgesteld.	X				Inadequate leveranciers en aanschaf slechte ICT-middelen (33)		N.V.T.	N.V.T.	B12 Leveranciersmanagement	Ja
5.24 Plannen en voorbereiden van het beheer van informatiebe	De organisatie behoort plannen op te stellen voor, en zich voor te bereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definieren, vast te stellen en te communiceren.	X		X	X	Beveiligingsniveau daalt door slechte afhandeling van informatiebeveiligingsincidenten (35)		N.V.T.	N.V.T.	B05 Incidentmanagement	Ja
5.25 Beoordelen van en besluiten over informatiebeveiligingsge	De organisatie behoort informatiebeveiligingsgebeurtenissen te beoordelen en te beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	X		X	X	Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02), Beveiligingsniveau daalt door slechte afhandeling van informatiebeveiligingsincidenten (35)		N.V.T.	N.V.T.	B05 Incidentmanagement	Ja
5.26 Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	X		X	X	Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02), Beveiligingsniveau daalt door slechte afhandeling van informatiebeveiligingsincidenten (35)		N.V.T.	N.V.T.	B05 Incidentmanagement, B12 Leveranciersmanagement	Ja
5.27 Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten behoort te worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	X		X	X	Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02), Beveiligingsniveau daalt door slechte afhandeling van informatiebeveiligingsincidenten (35)		N.V.T.	N.V.T.	B05 Incidentmanagement	Ja
5.28 Verzamelen van bewijsmateriaal	De organisatie behoort procedures vast te stellen en te implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	X		X	X	Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02), Geen detectie en geen bewijsmateriaal door ontbreken regels omtrent logging en monitoring (26), Beveiligingsniveau daalt door slechte afhandeling van informatiebeveiligingsincidenten (35)		N.V.T.	N.V.T.	B05 Incidentmanagement	Ja
5.29 Informatiebeveiliging tijdens een verstoring	De organisatie behoort plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	X			X	Verstoring primaire bedrijfsprocessen als gevolg van calamiteit (36)		N.V.T.	N.V.T.	B18 Continuiteit informatiebeveiliging	Ja
5.30 ICT-gereedheid voor bedrijfscontinuiteit	De ICT-gereedheid behoort te worden gepland, geimplementeerd, onderhouden en getest op basis van bedrijfscontinuiteitsdoelstellingen en ICT-continuiteitseisen.	X				Verstoring primaire bedrijfsprocessen als gevolg van calamiteit (36)		N.V.T.	N.V.T.	B18 Continuiteit informatiebeveiliging	Ja
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 behoren te worden vastgesteld, gedocumenteerd en actueel gehouden.	X		X	X	Niet voldoen aan geldende wet- en regelgeving (37)		N.V.T.	N.V.T.	B08 Voldoen aan overeenkomsten wet- en regelgeving	Ja
5.32 Intellectuele-eigendomsrechten	De organisatie behoort passende procedures te implementeren om intellectuele eigendomsrechten te beschermen.	X		X	X	Niet voldoen aan geldende wet- en regelgeving (37)		N.V.T.	N.V.T.	B08 Voldoen aan overeenkomsten wet- en regelgeving	Ja
5.33 Beschermen van registraties	Registraties behoren te worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	X				Datalek,of juridische procedures door het niet voldoen aan verplichte registraties (38)		N.V.T.	N.V.T.	B02 Documentbeheer	Ja
5.34 Privacy en bescherming van persoonsgegevens	De organisatie behoort de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen te identificeren en eraan te voldoen.	X		X	X	Niet voldoen aan geldende wet- en regelgeving (37)		N.V.T.	N.V.T.	B08 Voldoen aan overeenkomsten wet- en regelgeving	Ja
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 technologieen, behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.	X				Beleids-/gedragsregels niet worden nageleefd door geen verantwoordelijke aangewezen voor beleid (03), Datalek door ontbreken periodieke toetsing van het ISMS (39)		N.V.T.	N.V.T.	B06 Bewustwording, B07 Interne audit	Ja
5.36 Naleving van beleid regels en normen voor informatiebeve	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie behoort regelmatig te worden beoordeeld.	X				Beleids-/gedragsregels niet worden nageleefd door geen verantwoordelijke aangewezen voor beleid (03), Datalek door ontbreken periodieke toetsing van het ISMS (39)		N.V.T.	N.V.T.	B06 Bewustwording	Ja
5.37 Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan het personeel dat ze nodig heeft.	X				Datalek door ontbreken regels omtrent beheer en audits informatiesystemen (25), Niet integere uitkomsten onderzoek (49)		N.V.T.	N.V.T.	Werkprocedures en afspraken.	Ja
6.01 Screening	De achtergrond van alle kandidaten die in aanmerking komen voor posities binnen de organisatie behoort te worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden te worden herhaald. Hierbij behoort rekening te worden gehouden met de toepasselijke wet- en regelgeving, voorschriften en ethische overwegingen, en deze controle behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	X		X		Informatiebeveiligingsincidenten veroorzaakt door verkeerd gedrag en/of onvoldoende kennis (08)		N.V.T.	N.V.T.	B09 Veilig personeel	Ja

6.02 Arbeidsovereenkomst	In arbeidsovereenkomsten behoort te worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	X				Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02)		N.V.T.	N.V.T.	B09 Veilig personeel	Ja
6.03 Bewustwording van opleiding en training in informatiebev	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, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, te krijgen.	X				Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02), Informatiebeveiligingsincidenten veroorzaakt door verkeerd gedrag en/of onvoldoende kennis (08)		N.V.T.	N.V.T.	B06 Bewustwording, B09 Veilig personeel	Ja
6.04 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.	X				Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02)		N.V.T.	N.V.T.	P09 Disciplinaire procedure	Ja
6.05 Verantwoordelijkheden na beeindiging of wijziging van he	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beeindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	X				Niet naleven regels en of taken niet goed uitvoeren (09)		N.V.T.	N.V.T.	B09 Veilig personeel	Ja
6.06 Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, behoren te worden geidentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	X			X	Onveilig transport van informatie en onveilige toegang tot informatie in toepassingsdiensten via net (30), Niet integere uitkomsten onderzoek (49)		N.V.T.	N.V.T.	B12 Leveranciersmanagement	Ja
6.07 Werken op afstand	Wanneer personeel op afstand werkt, behoren er beveiligingsmaatregelen te worden geimplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	X				Informatiebeveiligingsincidenten door niet passende regels omtrent telewerken (07)		N.V.T.	N.V.T.	B03 Informatieclassificatie en labeling, B13 Beheer bedrijfsmiddelen	Ja
6.08 Melden van informatiebeveiligingsgebeurtenissen	De organisatie behoort te voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	X		X	X	Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02), Beveiligingsniveau daalt door slechte afhandeling van informatiebeveiligingsincidenten (35)		N.V.T.	N.V.T.	B05 Incidentmanagement	Ja
7.01 Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, behoren te worden beschermd door beveiligingszones te definieren en te gebruiken.	X				Ongeautoriseerde toegang tot informatie door diefstal, brand, of vandalisme (20)		N.V.T.	N.V.T.	B10 Fysieke toegangsbeveiliging	Ja
7.02 Fysieke toegangsbeveiliging	Beveiligde zones behoren te worden beschermd door passende toegangscontroles en toegangspunten.	X				Ongeautoriseerde toegang tot informatie door diefstal, brand, of vandalisme (20)		N.V.T.	N.V.T.	B10 Fysieke toegangsbeveiliging	Ja
7.03 Beveiligen van kantoren ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en geimplementeerd.	X				Ongeautoriseerde toegang tot informatie door diefstal, brand, of vandalisme (20)		N.V.T.	N.V.T.	B10 Fysieke toegangsbeveiliging	Ja
7.04 Monitoren van de fysieke beveiliging	Het gebouw en terrein behoort voortdurend te worden gemonitord op onbevoegde fysieke toegang.	X				Vernietiging/onbruikbaar raken van bedrijfsmiddelen in beveiligde gebieden (22)		N.V.T.	N.V.T.	B10 Fysieke toegangsbeveiliging	Ja
7.05 Beschermen tegen fysieke en omgevingsdreigingen	Er behoort bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen van de infrastructuur, te worden ontworpen en geimplementeerd.	X				Vernietiging/onbruikbaar raken van bedrijfsmiddelen door bedreigingen van buitenaf (21)		N.V.T.	N.V.T.	B10 Fysieke toegangsbeveiliging	Ja
7.06 Werken in beveiligde zones	Voor het werken in beveiligde zones behoren beveiligingsmaatregelen te worden ontwikkeld en geimplementeerd.	X				Vernietiging/onbruikbaar raken van bedrijfsmiddelen in beveiligde gebieden (22)		N.V.T.	N.V.T.	B03 Informatieclassificatie en labeling, B10 Fysieke toegangsbeveiliging	Ja
7.07 'Clear desk' en 'clear screen'	Er behoren 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten te worden gedefinieerd en op passende wijze ten uitvoer worden gebracht.	X				Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02)		N.V.T.	N.V.T.	B03 Informatieclassificatie en labeling	Ja
7.08 Plaatsen en beschermen van apparatuur	Apparatuur behoort veilig te worden geplaatst en beschermd.	X				Netwerk, apparatuur of nutsvoorziening gecompromitteerd, onbruikbaar of niet beschikbaar (23)		N.V.T.	N.V.T.	B10 Fysieke toegangsbeveiliging	Ja
7.09 Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein behoren te worden beschermd.	X				Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02), Informatiebeveiligingsincidenten door niet passende regels omtrent telewerken (07)		N.V.T.	N.V.T.	B10 Fysieke toegangsbeveiliging, B13 Beheer bedrijfsmiddelen	Ja
7.10 Opslagmedia	Opslagmedia behoren te worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	X				Informatie/bedrijfsmiddelen verkeerd worden behandeld en/of onvoldoende worden beschermd. (13)		N.V.T.	N.V.T.	B13 Beheer bedrijfsmiddelen	Ja
7.11 Nutsvoorzieningen	Informatieverwerkende faciliteiten behoren te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	X				Netwerk, apparatuur of nutsvoorziening gecompromitteerd, onbruikbaar of niet beschikbaar (23)		N.V.T.	N.V.T.	B10 Fysieke toegangsbeveiliging	Ja
7.12 Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen onderschepping, interferentie of beschadiging.	X				Netwerk, apparatuur of nutsvoorziening gecompromitteerd, onbruikbaar of niet beschikbaar (23)		N.V.T.	N.V.T.	B10 Fysieke toegangsbeveiliging	Ja
7.13 Onderhoud van apparatuur	Apparatuur behoort op de juiste wijze te worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	X				Netwerk, apparatuur of nutsvoorziening gecompromitteerd, onbruikbaar of niet beschikbaar (23)		N.V.T.	N.V.T.	B10 Fysieke toegangsbeveiliging	Ja
7.14 Veilig verwijderen of hergebruiken van apparatuur	Onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	X				Informatie/bedrijfsmiddelen verkeerd worden behandeld en/of onvoldoende worden beschermd. (13), Ongeautoriseerde toegang tot informatie door ontbreken regels opslagmedia (24)		N.V.T.	N.V.T.	B13 Beheer bedrijfsmiddelen	Ja
8.01 'User endpoint devices'	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' behoort te worden beschermd.	X				Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02), Informatiebeveiligingsincidenten door niet passende regels omtrent telewerken (07), Onbevoegde toegang tot klantinformatie op telefoon en er een datalek ontstaat (50)		N.V.T.	N.V.T.	B13 Beheer bedrijfsmiddelen	Ja
8.02 Speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerd.	X				Ongeautoriseerde toegang door bijvoorbeeld beheerders en externen. (15)		N.V.T.	N.V.T.	B11 Autorisatiebeheer	Ja

8.03 Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen behoort te worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	X				Ongeautoriseerde toegang of toegang die breder is dan het 'need tot know' principe. (14)		N.V.T.	N.V.T.	B11 Autorisatiebeheer	Ja
8.04 Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken behoort op passende wijze te worden beheerd.	X				Diefstal van programmabroncode of ongeautoriseerd wijziging (18)		N.V.T.	N.V.T.	B11 Autorisatiebeheer	Ja
8.05 Beveiligde authenticatie	Er behoren beveiligde authenticatietechnologieen en -procedures te worden geimplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke of aanvullende beleid inzake toegangsbeveiliging.	X				Ongeautoriseerde toegang door ontbreken inlogbeveiliging (16)		N.V.T.	N.V.T.	B11 Autorisatiebeheer	Ja
8.06 Capaciteitsbeheer	Het gebruik van middelen behoort te worden gemonitord en afgestemd overeenkomstig de huidige en verwachte capaciteitseisen.	X				Geen detectie en geen bewijsmateriaal door ontbreken regels omtrent logging en monitoring (26)		N.V.T.	N.V.T.	B14 ICT beheer	Ja
8.07 Bescherming tegen malware	Bescherming tegen malware behoort te worden geimplementeerd en ondersteund door een passend gebruikersbewustzijn.	X				Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02), Malware en datalekken (40)		N.V.T.	N.V.T.	B14 ICT beheer, B15 Netwerkbeheer	Ja
8.08 Beheer van technische kwetsbaarheden	Er behoort informatie te worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden behoort te worden geevalueerd en er behorende passende maatregelen te worden getroffen.	X				Onvoldoende op de hoogte zijn van actuele kwetsbaarheden en nieuwe technologie (01), Virussen/hacking door gebrek inzicht/detectie in technische kwetsbaarheden (28)		N.V.T.	N.V.T.	B05 Incidentmanagement, B14 ICT beheer, B15 Netwerkbeheer	Ja
8.09 Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken behoren te worden vastgesteld, gedocumenteerd, geimplementeerd, gemonitord en beoordeeld.	X				Onvoldoende configuratiebeheer (42)		N.V.T.	N.V.T.	B14 ICT beheer	Ja
8.10 Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie behoort te worden gewist als deze niet langer nodig is.	X				Niet tijdig wissen van informatie (46)		N.V.T.	N.V.T.	B14 ICT beheer	Ja
8.11 Maskeren van gegevens	Gegevens behoren te worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	X				Niet voldoen aan wetgeving en overeenkomsten (43)		N.V.T.	N.V.T.	B19 Beveiligde ontwikkeling	Ja
8.12 Voorkomen van gegevenslekken (Data leakage prevention	Maatregelen om gegevenslekken te voorkomen behoren te worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	X				Onvoldoende maatregelen Data Leakage Prevention (44)		N.V.T.	N.V.T.	B14 ICT beheer	Ja
8.13 Back-up van informatie	Back-ups van informatie, software en systemen behoren te worden bewaard en regelmatig te worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	X			X	Datalek door ontbreken regels omtrent beheer en audits informatiesystemen (25), Verlies data waardoor het werk stil komt te liggen met faillissement tot gevolg (51)		N.V.T.	N.V.T.	B14 ICT beheer	Ja
8.14 Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geimplementeerd om aan beschikbaarheidseisen te voldoen.	X				Verstoring primaire bedrijfsprocessen als gevolg van calamiteit (36), Verlies data waardoor het werk stil komt te liggen met faillissement tot gevolg (51)		N.V.T.	N.V.T.	B14 ICT beheer, B18 Continuiteit informatiebeveiliging	Ja
8.15 Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	X				Geen detectie en geen bewijsmateriaal door ontbreken regels omtrent logging en monitoring (26)		N.V.T.	N.V.T.	B14 ICT beheer	Ja
8.16 Monitoren van activiteiten	Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden genomen om potentiele informatiebeveiligingsincidenten te evalueren.	X				Geen detectie en geen bewijsmateriaal door ontbreken regels omtrent logging en monitoring (26)		N.V.T.	N.V.T.	B14 ICT beheer, B15 Netwerkbeheer	Ja
8.17 Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, behoren te worden gesynchroniseerd met goedgekeurde tijdsbronnen.	X				Bewijsmateriaal niet bruikbaar door ontbreken regels kloksynchronisatie (27)		N.V.T.	N.V.T.	B14 ICT beheer	Ja
8.18 Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	X				Oneigenlijk gebruik van hulpmiddelen en dus ongeautoriseerde toegang of onzorgvuldig beheer (17)		N.V.T.	N.V.T.	B11 Autorisatiebeheer, B14 ICT beheer	Ja
8.19 Installeren van software op operationele systemen	Er behoren procedures en maatregelen te worden geimplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	X				Beleids-/gedragsregels niet worden nageleefd en het ISMS niet effectief is. (02)		N.V.T.	N.V.T.	B03 Informatieclassificatie en labeling	Ja
8.20 Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten behoren te worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	X				Ongeautoriseerde toegang tot informatie door gebrek beveiligingsmaatregelen en procedures (29), Niet werkende VPN beveiliging (48)		N.V.T.	N.V.T.	B15 Netwerkbeheer	Ja
8.21 Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten behoren te worden geidentificeerd, geimplementeerd en gemonitord.	X				Ongeautoriseerde toegang tot informatie door gebrek beveiligingsmaatregelen en procedures (29)		N.V.T.	N.V.T.	B15 Netwerkbeheer	Ja
8.22 Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen behoren in de netwerken van de organisatie te worden gesegmenteerd.	X				Ongeautoriseerde toegang tot informatie door gebrek beveiligingsmaatregelen en procedures (29)		N.V.T.	N.V.T.	B15 Netwerkbeheer	Ja
8.23 Toepassen van webfilters	De toegang tot externe websites behoort te worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.		X			Onvoldoende toepassen van webfilters (45)	Bij het bezoeken van websites wordt malicious content geblokkeerd. Uitgaand is er geen blokkade van websites, door de aard van het werk is toegang tot alle websites noodzakelijk. In het beleid is wel vastgelegd dat bezoek van bepaalde websites niet wenselijk is en zoveel mogelijk beperkt moet worden.	N.V.T.	N.V.T.	B15 Netwerkbeheer	Nee

8.24 Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.	X				Ongeautoriseerde toegang tot informatie en/of verlies van informatie en verkeerde routering van info (19)		N.V.T.	N.V.T.	B14 ICT beheer	Ja
8.25 Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen behoren regels te worden vastgesteld en toegepast.	X				Onveilig ontwikkelen van (onveilige) software (31), Gewenst beveiligingsniveau daalt door slechte sturing leveranciers bij uitbesteden van diensten (34)		N.V.T.	N.V.T.	B19 Beveiligde ontwikkeling	Ja
8.26 Toepassingsbeveiligingseisen	Er behoren eisen aan de informatiebeveiliging te worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	X				Onveilig ontwikkelen van (onveilige) software (31), De software niet voldoet aan de gestelde (beveiligings)eisen. (32)		N.V.T.	N.V.T.	B19 Beveiligde ontwikkeling	Ja
8.27 Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	X				Onveilig ontwikkelen van (onveilige) software (31)		N.V.T.	N.V.T.	B19 Beveiligde ontwikkeling	Ja
8.28 Veilig coderen	Er behoren principes voor veilig coderen te worden toegepast op softwareontwikkeling.	X				Onveilig ontwikkelen van (onveilige) software (31)		N.V.T.	N.V.T.	B19 Beveiligde ontwikkeling	Ja
8.29 Testen van de beveiliging tijdens ontwikkeling en acceptat	Processen voor het testen van de beveiliging behoren te worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	X				Onveilig ontwikkelen van (onveilige) software (31)		N.V.T.	N.V.T.	B19 Beveiligde ontwikkeling	Ja
8.30 Uitbestede systeemontwikkeling	De organisatie behoort de activiteiten in verband met uitbestede systeemontwikkeling te sturen, bewaken en beoordelen.	X				De software niet voldoet aan de gestelde (beveiligings)eisen. (32)		N.V.T.	N.V.T.	B19 Beveiligde ontwikkeling	Ja
8.31 Scheiding van ontwikkel- test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden en beveiligd.	X				Onveilig ontwikkelen van (onveilige) software (31)		N.V.T.	N.V.T.	B19 Beveiligde ontwikkeling	Ja
8.32 Wijzigingsbeheer	Wijzigingen in informatieverwerkingsfaciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer.	X				Datalek door ontbreken regels omtrent beheer en audits informatiesystemen (25)		N.V.T.	N.V.T.	B04 Risicomanagement, B18 Wijzigingsbeheer	Ja
8.33 Testgegevens	Testgegevens behoren op passende wijze te worden geselecteerd, beschermd en beheerd.	X				Onveilig ontwikkelen van (onveilige) software (31), De software niet voldoet aan de gestelde (beveiligings)eisen. (32)		N.V.T.	N.V.T.	B19 Beveiligde ontwikkeling	Ja
8.34 Bescherming van informatiesystemen tijdens audits	Audits en andere borgingsactiviteiten waarbij operationele systemen worden beoordeeld behoren te worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	X				Datalek door ontbreken regels omtrent beheer en audits informatiesystemen (25)		N.V.T.	N.V.T.	B16 Technische audits	Ja