Verklaring van Toepasselijkheid NEN-EN-ISO/IEC 27001:2023

Organisatie: Johan B.V., Debbemeerstraat 25, 2131 HE, Hoofddorp
Versie: 2.1
Datum: 15-1-2025
Classificatie: Openbaar
Norm: NEN-EN-ISO/IEC 27001:2023

Nr.	Hoofdstuk	Onderwerp	Beheersmaatregel	Van toepassing (J/N)	Motivatie voor toepassen	Motivatie voor niet toepassen	Geïmplementeerd (J/N)
Organisatorische beheersmaatregelen							
5.1	Organisatorische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
5.2	Organisatorische beheersmaatregelen	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Ja	Risicoanalyse		Ja
5.3	Organisatorische beheersmaatregelen	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden behoren te worden gescheiden.	Ja	Risicoanalyse		Ja
5.4	Organisatorische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
5.5	Organisatorische beheersmaatregelen	Contact met overheidsinstanties	De organisatie behoort contact met de relevante instanties te leggen en te onderhouden.	Ja	Risicoanalyse		Ja
5.6	Organisatorische beheersmaatregelen	Contact met speciale belangengroepen	De organisatie behoort contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen te leggen en te onderhouden.	Ja	Risicoanalyse		Ja
5.7	Organisatorische beheersmaatregelen	Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen behoort te worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren.	Ja	Risicoanalyse		Ja
5.8	Organisatorische beheersmaatregelen	Informatiebeveiliging in projectmanagement	Informatiebeveiliging behoort te worden geïntegreerd in projectmanagement.	Ja	Risicoanalyse		Ja
5.9	Organisatorische beheersmaatregelen	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Er behoort een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, te worden opgesteld en onderhouden.	Ja	Risicoanalyse		Ja
5.10	Organisatorische beheersmaatregelen	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 behoren te worden vastgesteld, gedocumenteerd en geïmplementeerd.	Ja	Risicoanalyse		Ja
5.11	Organisatorische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
5.12	Organisatorische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
5.13	Organisatorische beheersmaatregelen	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.	Nee		Johan B.V. maakt geen gebruik van gevoelige informatie op fysieke media en/of papier.	

Nr.	Hoofdstuk	Onderwerp	Beheersmaatregel	Van toepassing	Motivatie voor toepassen	Motivatie voor niet toepassen	Geïmplementeerd
5.14	Organisatorische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
5.15	Organisatorische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
5.16	Organisatorische beheersmaatregelen	Identiteitsbeheer	De volledige levenscyclus van identiteiten behoort te worden beheerd.	Ja	Risicoanalyse		Ja
5.17	Organisatorische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
5.18	Organisatorische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
5.19	Organisatorische beheersmaatregelen	Informatiebeveiliging in leveranciersrelaties	Er behoren 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	Risicoanalyse		Ja
5.20	Organisatorische beheersmaatregelen	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	Ja	Risicoanalyse		Ja
5.21	Organisatorische beheersmaatregelen	Beheren van informatiebeveiliging in de ICT-keten	Er behoren processen en procedures te worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheren.	Ja	Risicoanalyse		Ja
5.22	Organisatorische beheersmaatregelen	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie behoort de informatiebeveiligingspraktijken en de leveranciersdiensten regelmatig te monitoren, beoordelen, evalueren en veranderingen daaraan te beheren.	Ja	Risicoanalyse		Ja
5.23	Organisatorische beheersmaatregelen	Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten behoren overeenkomstig de informatiebeveiligingseisen van de organisatie te worden opgesteld.	Ja	Risicoanalyse		Ja
5.24	Organisatorische beheersmaatregelen	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	De organisatie behoort plannen op te stellen voor en zich voor te bereiden op het beheren van informatiebeveiliging-sincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Ja	Risicoanalyse		Ja
5.25	Organisatorische beheersmaatregelen	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie behoort informatiebeveiligingsgebeurtenissen te beoordelen en te beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja	Risicoanalyse		Ja
5.26	Organisatorische beheersmaatregelen	Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Risicoanalyse		Ja
5.27	Organisatorische beheersmaatregelen	Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten behoort te worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Ja	Risicoanalyse		Ja
5.28	Organisatorische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja

Nr.	Hoofdstuk	Onderwerp	Beheersmaatregel	Van toepassing	Motivatie voor toepassen	Motivatie voor niet toepassen	Geïmplementeerd
5.29	Organisatorische beheersmaatregelen	Informatiebeveiliging tijdens een verstoring	De organisatie behoort plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja	Risicoanalyse		Ja
5.30	Organisatorische beheersmaatregelen	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid behoort te worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfs-continuïteitsdoelstellingen en ICT-continuïteitseisen.	Ja	Risicoanalyse		Ja
5.31	Organisatorische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
5.32	Organisatorische beheersmaatregelen	Intellectuele-eigendomsrechten	De organisatie behoort passende procedures te implementeren om intellectuele eigendomsrechten te beschermen.	Ja	Risicoanalyse		Ja
5.33	Organisatorische beheersmaatregelen	Beschermen van registraties	Registraties behoren te worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja	Risicoanalyse		Ja
5.34	Organisatorische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
5.35	Organisatorische beheersmaatregelen	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, behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.	Ja	Risicoanalyse		Ja
5.36	Organisatorische beheersmaatregelen	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie behoort regelmatig te worden beoordeeld.	Ja	Risicoanalyse		Ja
5.37	Organisatorische beheersmaatregelen	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan het personeel dat ze nodig heeft.	Ja	Risicoanalyse		Ja
Mensgerichte beheersmaatregelen							
6.1	Mensgerichte beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
6.2	Mensgerichte beheersmaatregelen	Arbeidsovereenkomst	In arbeidsovereenkomsten behoort te worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Ja	Risicoanalyse		Ja
6.3	Mensgerichte beheersmaatregelen	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden behoren een passende 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.	Ja	Risicoanalyse		Ja
6.4	Mensgerichte beheersmaatregelen	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	Risicoanalyse		Ja

Nr.	Hoofdstuk	Onderwerp	Beheersmaatregel	Van toepassing	Motivatie voor toepassen	Motivatie voor niet toepassen	Geïmplementeerd
6.5	Mensgerichte beheersmaatregelen	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	Risicoanalyse		Ja
6.6	Mensgerichte beheersmaatregelen	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, behoren te worden geïdentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	Ja	Risicoanalyse		Ja
6.7	Mensgerichte beheersmaatregelen	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	Risicoanalyse		
6.8	Mensgerichte beheersmaatregelen	Melden van informatiebeveiligingsgebeurtenissen	De organisatie behoort te voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Ja	Risicoanalyse		Ja
Fysieke beheersmaatregelen							
7.1	Fysieke beheersmaatregelen	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, behoren te worden beschermd door beveiligingszones te definiëren en te gebruiken.	Ja	Risicoanalyse		Ja
7.2	Fysieke beheersmaatregelen	Fysieke toegangsbeveiliging	Beveiligde zones behoren te worden beschermd door passende toegangscontroles en toegangspunten.	Ja	Risicoanalyse		Ja
7.3	Fysieke beheersmaatregelen	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en geïmplementeerd.	Ja	Risicoanalyse		Ja
7.4	Fysieke beheersmaatregelen	Monitoren van de fysieke beveiliging	Het gebouw en terrein behoort voortdurend te worden gemonitord op onbevoegde fysieke toegang.	Ja	Risicoanalyse		Ja
7.5	Fysieke beheersmaatregelen	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 geïmplementeerd.	Ja	Risicoanalyse		Ja
7.6	Fysieke beheersmaatregelen	Werken in beveiligde zones	Voor het werken in beveiligde zones behoren beveiligingsmaatregelen te worden ontwikkeld en geïmplementeerd.	Ja	Risicoanalyse		Ja
7.7	Fysieke beheersmaatregelen	‘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.	Ja	Risicoanalyse		Ja
7.8	Fysieke beheersmaatregelen	Plaatsen en beschermen van apparatuur	Apparatuur behoort veilig te worden geplaatst en beschermd.	Ja	Risicoanalyse		Ja
7.9	Fysieke beheersmaatregelen	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein behoren te worden beschermd.	Ja	Risicoanalyse		Ja
7.10	Fysieke beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
7.11	Fysieke beheersmaatregelen	Nutsvoorzieningen	Informatieverwerkende faciliteiten behoren te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja	Risicoanalyse		Ja
7.12	Fysieke beheersmaatregelen	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen onderschepping, interferentie of beschadiging.	Ja	Risicoanalyse		Ja
7.13	Fysieke beheersmaatregelen	Onderhoud van apparatuur	Apparatuur behoort op de juiste wijze te worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	Ja	Risicoanalyse		Ja

Nr.	Hoofdstuk	Onderwerp	Beheersmaatregel	Van toepassing	Motivatie voor toepassen	Motivatie voor niet toepassen	Geïmplementeerd
7.14	Fysieke beheersmaatregelen	Veilig verwijderen of hergebruiken van apparatuur	Onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicenseerde software zijn verwijderd of veilig zijn overschreven, voordat ze worden verwijderd of hergebruikt.	Ja	Risicoanalyse		Ja
Technologische beheersmaatregelen							
8.1	Technologische beheersmaatregelen	User endpoint devices	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via user endpoint devices behoort te worden beschermd.	Ja	Risicoanalyse		Ja
8.2	Technologische beheersmaatregelen	Speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerd.	Ja	Risicoanalyse		Ja
8.3	Technologische beheersmaatregelen	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen behoort te worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja	Risicoanalyse		Ja
8.4	Technologische beheersmaatregelen	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en software-bibliotheken behoort op passende wijze te worden beheerd.	Ja	Risicoanalyse		Ja
8.5	Technologische beheersmaatregelen	Beveiligde authenticatie	Er behoren beveiligde authenticatie-technologieën en -procedures te worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke of aanvullende beleid inzake toegangsbeveiliging.	Ja	Risicoanalyse		Ja
8.6	Technologische beheersmaatregelen	Capaciteitsbeheer	Het gebruik van middelen behoort te worden gemonitord en afgestemd overeenkomstig de huidige en verwachte capaciteitseisen.	Ja	Risicoanalyse		Ja
8.7	Technologische beheersmaatregelen	Bescherming tegen malware	Bescherming tegen malware behoort te worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn	Ja	Risicoanalyse		Ja
8.8	Technologische beheersmaatregelen	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 geëvalueerd en er behorende passende maatregelen te worden getroffen.	Ja	Risicoanalyse		Ja
8.9	Technologische beheersmaatregelen	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken behoren te worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja	Risicoanalyse		Ja
8.10	Technologische beheersmaatregelen	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie behoort te worden gewist als deze niet langer nodig is.	Ja	Risicoanalyse		Ja
8.11	Technologische beheersmaatregelen	Maskeren van gegevens	Gegevens behoren te worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerp-specifieke beleidsregels en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	Ja	Risicoanalyse		Ja
8.12	Technologische beheersmaatregelen	Voorkomen van gegevenslekken (Data leakage prevention)	Maatregelen om gegevens-lekken te voorkomen behoren te worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	Ja	Risicoanalyse		Ja
8.13	Technologische beheersmaatregelen	Back-up van informatie	Backups van informatie, software en systemen behoren te worden bewaard en regelmatig te worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	Ja	Risicoanalyse		Ja
8.14	Technologische beheersmaatregelen	Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheids-eisen te voldoen.	Ja	Risicoanalyse		Ja
8.15	Technologische beheersmaatregelen	Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja	Risicoanalyse		Ja

Nr.	Hoofdstuk	Onderwerp	Beheersmaatregel	Van toepassing	Motivatie voor toepassen	Motivatie voor niet toepassen	Geïmplementeerd
8.16	Technologische beheersmaatregelen	Monitoren van activiteiten	Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden genomen om potentiële informatiebeveiligingsincidenten te evalueren.	Ja	Risicoanalyse		Ja
8.17	Technologische beheersmaatregelen	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, behoren te worden gesynchroniseerd met goedgekeurde tijdsbronnen.	Ja	Risicoanalyse		Ja
8.18	Technologische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
8.19	Technologische beheersmaatregelen	Installeren van software op operationele systemen	Er behoren procedures en maatregelen te worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	Ja	Risicoanalyse		Ja
8.20	Technologische beheersmaatregelen	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten behoren te worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Risicoanalyse		Ja
8.21	Technologische beheersmaatregelen	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten behoren te worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja	Risicoanalyse		Ja
8.22	Technologische beheersmaatregelen	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen behoren in de netwerken van de organisatie te worden gesegmenteerd.	Ja	Risicoanalyse		Ja
8.23	Technologische beheersmaatregelen	Toepassen van webfilters	De toegang tot externe websites behoort te worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja	Risicoanalyse		Ja
8.24	Technologische beheersmaatregelen	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.	Ja	Risicoanalyse		Ja
8.25	Technologische beheersmaatregelen	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen behoren regels te worden vastgesteld en toegepast.	Ja	Risicoanalyse		Ja
8.26	Technologische beheersmaatregelen	Toepassingsbeveiligingseisen	Er behoren eisen aan de informatiebeveiliging te worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja	Risicoanalyse		Ja
8.27	Technologische beheersmaatregelen	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.	Ja	Risicoanalyse		Ja
8.28	Technologische beheersmaatregelen	Veilig coderen	Er behoren principes voor veilig coderen te worden toegepast op softwareontwikkeling.	Ja	Risicoanalyse		Ja
8.29	Technologische beheersmaatregelen	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging behoren te worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Ja	Risicoanalyse		Ja
8.30	Technologische beheersmaatregelen	Uitbestede systeemontwikkeling	De organisatie behoort de activiteiten in verband met uitbestede systeemontwikkeling te sturen, bewaken en beoordelen.	Ja	Risicoanalyse		Ja
8.31	Technologische beheersmaatregelen	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden en beveiligd.	Ja	Risicoanalyse		Ja
8.32	Technologische beheersmaatregelen	Wijzigingsbeheer	Wijzigingen in informatieverwerkingsfaciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer.	Ja	Risicoanalyse		Ja
8.33	Technologische beheersmaatregelen	Testgegevens	Testgegevens behoren op passende wijze te worden geselecteerd, beschermd en beheerd.	Ja	Risicoanalyse		Ja
8.34	Technologische beheersmaatregelen	Bescherming van informatiesystemen tijdens audits	Audits en andere borgings-activiteiten waarbij operationele systemen worden beoordeeld behoren te worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Ja	Risicoanalyse		Ja