Management Systeem implementatie status (ISO 27001:2022 & ISO9001:2015)

Sectie	Management Systeem vereisten (ISO 27001:2022 & ISO9001:2015)	Volwassenheidsniveau
4	**Context van de organisatie**	
4.1	**Inzicht in de organisatie en haar context**	
4.1	Bepaal de Management Systeem-doelstellingen van de organisatie en eventuele problemen die van invloed kunnen zijn op de	**Beheerst en meetbaar**
4.2	**Stakeholders**	
4.2 (a)	Identificeer stakeholders, inclusief toepasselijke wetgeving, voorschriften, contracten, etc.	**Beheerst en meetbaar**
4.2 (b)	Bepaal de relevante eisen en verplichtingen vanuit de stakeholders	**Beheerst en meetbaar**
4.3	**Management Systeem scope**	
4.3	Bepaal en documenteer de Management Systeem scope	**Beheerst en meetbaar**
4.4	**Management Systeem processen**	
4.4	Opzetten, implementeren, onderhouden en continu verbeteren van het Management Systeem	**Beheerst en meetbaar**
5	**Leiderschap**	
5.1	**Leiderschap & betrokkenheid**	
5.1	Het topmanagement moet leiderschap en betrokkenheid tonen met betrekking tot het Management Systeem	**Beheerst en meetbaar**
5.2	**Beleid**	
5.2	Stel het informatiebeveiliging- en kwaliteitbeleid vast	**Beheerst en meetbaar**
5.3	**Organisatorische rollen, verantwoordelijkheden & bevoegdheden**	
5.3	Wijs rollen en verantwoordelijkheden voor informatiebeveiliging en kwaliteit toe en communiceer deze	**Beheerst en meetbaar**
6	**Planning**	
6.1	**Acties om risico's en kansen aan te pakken**	
6.1.1	Ontwerp het Management Systeem om aan de eisen uit de contextanalyse te voldoen	**Beheerst en meetbaar**
6.1.2	Definieer en pas een risicobeoordelingsproces voor informatiebeveiliging en kwaliteit toe	**Beheerst en meetbaar**

Management Systeem implementatie status (ISO 27001:2022 & ISO9001:2015)

Sectie	Management Systeem vereisten (ISO 27001:2022 & ISO9001:2015)	Volwassenheidsniveau
6.1.3	Documenteer en pas een behandelingsproces voor informatiebeveiliging- en kwaliteitrisico's toe	Beheerst en meetbaar
6.2	**Doelstellingen en plannen voor informatiebeveiliging en kwaliteit**	
6.2	Stel de doelstellingen en plannen voor informatiebeveiliging en kwaliteit vast en documenteer deze	Beheerst en meetbaar
6.3	**Plannen van veranderingen**	
6.3	Substantiële wijzigingen aan het Management Systeem worden gepland en gestructureerd uitgevoerd	Beheerst en meetbaar
7	**Ondersteuning**	
7.1	**Middelen**	
7.1	Bepaal en wijs de benodigde middelen toe voor het Management Systeem	Beheerst en meetbaar
7.2	**Competenties**	
7.2	Bepalen, documenteren en beschikbaar stellen van benodigde competenties	Beheerst en meetbaar
7.3	**Bewustzijn**	
7.3	Opzetten van een security awareness en kwaliteitbewustzijn programma	Beheerst en meetbaar
7.4	**Communicatie**	
7.4	Bepaal de behoefte aan interne en externe communicatie die relevant is voor het Management Systeem	Beheerst en meetbaar
7.5	**Gedocumenteerde informatie**	
7.5.1	Zorg voor documentatie vereist door de norm plus die vereist door de organisatie	Beheerst en meetbaar
7.5.2	Zorg voor documenttitels, auteurs, etc. formatteer ze consistent en bekijk en keur ze goed	Beheerst en meetbaar
7.5.3	Controleer de documentatie goed	Beheerst en meetbaar
8	**Uitvoering**	
8.1	**Operationele planning en beheersing**	
8.1	Stel een risicobehandelingsplan op	Beheerst en meetbaar

Management Systeem implementatie status (ISO 27001:2022 & ISO9001:2015)

Sectie	Management Systeem vereisten (ISO 27001:2022 & ISO9001:2015)	Volwassenheidsniveau
8.2	**Risicobeoordeling van informatiebeveiliging**	
8.2	(Her)beoordeel en documenteer informatiebeveiligingsrisico's regelmatig en bij wijzigingen	**Beheerst en meetbaar**
8.3	**Informatiebeveiligingrisico's behandelen**	
8.3	Voer het risicobehandelingsplan uit en documenteer de resultaten	**Beheerst en meetbaar**
8.2	**Eisen voor producten en diensten**	
8.2	Met klanten wordt duidelijk gecommuniceerd over de specificaties van producten en diensten.	**Beheerst en meetbaar**
8.3	**Ontwerp en ontwikkeling van producten en diensten**	
8.3	Er is een ontwerp- en ontwikkelproces vastgesteld, geïmplementeerd en deze wordt onderhouden zodat het aansluit bij de	**Geoptimaliseerd**
8.4	**Beheersing van extern geleverde processen, producten en diensten**	
8.4	Door derde partijen geleverde processen, producten en diensten moeten aan vooraf opgestelde eisen voldoen.	**Geoptimaliseerd**
8.5	**Productie en het leveren van diensten**	
8.5	Het productieproces en leveren van diensten moeten duidelijk in kaart zijn gebracht en aan vooraf opgestelde vereisten	**Geoptimaliseerd**
8.6	**Vrijgave van producten en diensten**	
8.6	Er wordt, voordat het product of de dienst geleverd wordt, actief gecontroleerd of de producten en diensten aan de vooraf	**Geoptimaliseerd**
8.7	**Beheersing van afwijkende outputs**	
8.7	Er worden passende maatregelen genomen op afwijkingen die geconstateerd worden in producten en/of diensten.	**Geoptimaliseerd**
9	**Evaluatie van de prestaties**	
9.1	**Monitoren, meten, analyseren en evalueren**	
9.1	Bewaak, meet, analyseer en evalueer het Management Systeem en de beveiligingsmaatregelen	**Beheerst en meetbaar**
9.2	**Interne audit**	
9.2	Plan en voer interne audits van het Management Systeem uit	**Beheerst en meetbaar**
9.3	**Directiebeoordeling**	

Management Systeem implementatie status (ISO 27001:2022 & ISO9001:2015)

Sectie	Management Systeem vereisten (ISO 27001:2022 & ISO9001:2015)	Volwassenheidsniveau
9.3	Zorg voor regelmatige directiebeoordelingen van het Management Systeem	Beheerst en meetbaar
10	**Verbetering**	
10.1	**Continue verbetering**	
10.1	Verbeter het Management Systeem continu	Beheerst en meetbaar
10.2	**Afwijkingen en corrigerende maatregelen**	
10.2	Identificeren, documenteren, oplossen en actie ondernemen om herhaling van afwijkingen te voorkomen	Beheerst en meetbaar

34

Verklaring van Toepasselijkheid & informatiebeveiliging beheersmaatregelen implementatie status (Annex A vanuit ISO 27001:2022)

Sectie		Toelichting op de informatiebeveiliging beheersmaatregelen	Van toepassing?	Reden voor insluiting / uitsluiting	Geïmplementeerd?	Volwassenheidsniveau
A5	Organisatorische beheersmaatregelen					
A.5.1	Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels moeten worden Herhaalbaar, 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	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden Herhaalbaar en toegewezen overeenkomstig de behoeften van de organisatie.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.5.3	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheidsgebieden moeten te worden gescheiden.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.5.4	Managementverantwoordelijkheden	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.	Ja	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.5.5	Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en te onderhouden.	Ja	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.5.6	Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en te onderhouden.	Ja	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.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	Risicoanalyse	Ja	Beheerst en meetbaar
A.5.8	Informatiebeveiliging in projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	Ja	Best practices / bedrijfsvereisten	Ja	Initieel
A.5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.5.10	Aanvaard gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moet worden vastgesteld en geïmplementeerd.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.5.11	Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.5.12	Classificeren van informatie	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante belanghebbenden.	Ja	Best practices / bedrijfsvereisten	Ja	Herhaalbaar
A.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	Best practices / bedrijfsvereisten	Ja	Herhaalbaar
A.5.14	Overdragen van informatie	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn vastgesteld voor alle soorten van overdracht binnen de organisatie en tussen de organisatie en andere partijen.	Ja	Best practices / bedrijfsvereisten	Ja	Herhaalbaar
A.5.15	Toegangsbeveiliging	Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.5.16	Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.5.17	Beheren van authenticatie informatie	De toewijzing en het beheer van authenticatie-informatie moet worden Beheerst en meetbaar door middel van een beheerproces waarvan het informeren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.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	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.5.19	Informatiebeveiliging in leveranciersrelaties	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheren.	Ja	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	Ja	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.5.21	Beheren van informatiebeveiliging in de ICT-keten	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheren.	Ja	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie moet de informatiebeveiligingspraktijken en de leveranciersdiensten regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan te beheren.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd

Verklaring van Toepasselijkheid & informatiebeveiliging beheersmaatregelen implementatie status (Annex A vanuit ISO 27001:2022)

Sectie		Toelichting op de informatiebeveiliging beheersmaatregelen	Van toepassing?	Reden voor insluiting / uitsluiting	Geïmplementeerd?	Volwassenheidsniveau
A.5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	Ja	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	De organisatie moet plannen opstellen voor, en zich voor te bereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar
A.5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en te beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar
A.5.26	Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar
A.5.27	Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar
A.5.28	Verzamelen van bewijsmateriaal	De organisatie moet procedures vaststellen en te implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar
A.5.29	Informatiebeveiliging tijdens een verstoring	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar
A.5.30	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.	Ja	Risicoanalyse	Ja	Herhaalbaar
A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Eisen van wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen moeten worden vastgesteld, gedocumenteerd en actueel gehouden.	Ja	Wet- en regelgeving	Ja	Geoptimaliseerd
A.5.32	Intellectuele eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele eigendomsrechten te beschermen.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.5.33	Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.5.34	Privacy en bescherming van persoonsgegevens	De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan te voldoen.	Ja	Wet- en regelgeving	Ja	Beheerst en meetbaar
A.5.35	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	Ja	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	Ja	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar te worden gesteld aan het personeel dat ze nodig heeft.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A6	**Mensgerichte beheersmaatregelen**					
A.6.1	Screening	De achtergrond van alle kandidaten die in aanmerking komen voor posities binnen de organisatie moet worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden 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	Beheerst en meetbaar
A.6.2	Arbeidsovereenkomst	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Ja	Best practices / bedrijfsvereisten	Ja	Gedefinieerd
A.6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden moet 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, krijgen.	Ja	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.6.4	Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.	Ja	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden Herhaalbaar, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar

Verklaring van Toepasselijkheid & informatiebeveiliging beheersmaatregelen implementatie status (Annex A vanuit ISO 27001:2022)

Sectie		Toelichting op de informatiebeveiliging beheersmaatregelen	Van toepassing?	Reden voor insluiting / uitsluiting	Geïmplementeerd?	Volwassenheidsniveau
A.6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.6.7	Werken op afstand	Wanneer personeel op afstand werkt, moeten er beveiligingsmaatregelen worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.6.8	Melden van informatiebeveiligingsgebeurtenissen	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar
A7	**Fysieke beheersmaatregelen**					
A.7.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.7.2	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangscontroles en toegangspunten.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.7.4	Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.7.5	Beschermen tegen fysieke en omgevingsdreigingen	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen van de infrastructuur, worden ontworpen en geïmplementeerd.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	Nee	Onze medewerkers komen niet in het datacenter. Dit is uitbesteedt als onderdeel van de Clouddienst oplossing die afgenomen wordt bij een derde partij.	NVT	Niet van toepassing
A.7.7	'Clear desk' en 'clear screen'	Er moeten 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten worden Herhaalbaar en op passende wijze ten uitvoer worden gebracht.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar
A.7.8	Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar
A.7.10	Opslagmedia	Opslagmedia moet worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar
A.7.11	Nutsvoorzieningen	Informatieverwerkende faciliteiten moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.7.12	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.7.13	Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.7.14	Veilig verwijderen of hergebruiken van apparatuur	Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A8	**Technische beheersmaatregelen**					
A.8.1	User endpoint devices	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	Ja	Risicoanalyse	Ja	Gedefinieerd
A.8.2	Speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.8.3	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja	Risicoanalyse	Ja	Geoptimaliseerd

Verklaring van Toepasselijkheid & informatiebeveiliging beheersmaatregelen implementatie status (Annex A vanuit ISO 27001:2022)

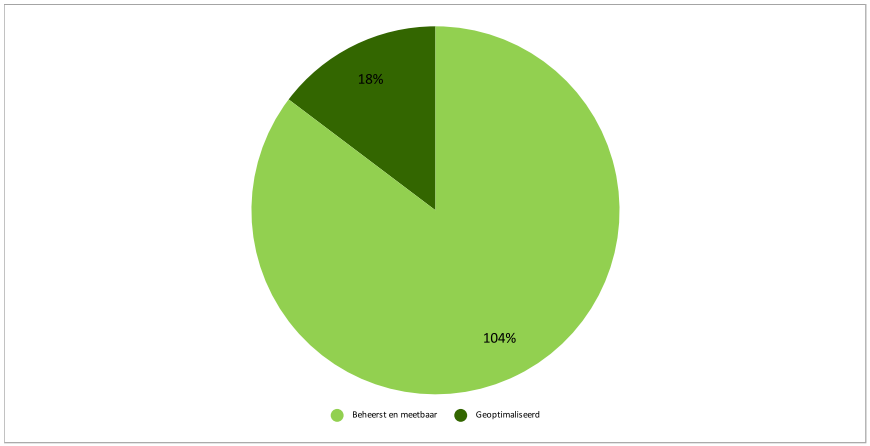
Sectie		Toelichting op de informatiebeveiliging beheersmaatregelen	Van toepassing?	Reden voor insluiting / uitsluiting	Geïmplementeerd?	Volwassenheidsniveau
A.8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.8.5	Beveiligde authenticatie	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke of aanvullende beleid inzake toegangsbeveiliging.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.8.6	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd overeenkomstig de huidige en verwachte capaciteitseisen.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.8.7	Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.8.8	Beheer van technische kwetsbaarheden	Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er behorende passende maatregelen te worden getroffen.	Ja	Best practices / bedrijfsvereisten	Ja	Beheerst en meetbaar
A.8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.8.10	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer nodig is.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.8.11	Maskeren van gegevens	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	Ja	Wet- en regelgeving	Ja	Geoptimaliseerd
A.8.12	Voorkomen van gegevenslekken (Data leakage prevention)	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.8.13	Back-up van informatie	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig te worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.8.14	Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar
A.8.15	Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja	Risicoanalyse	Ja	Gedefinieerd
A.8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden genomen om potentiële informatiebeveiligingsincidenten te evalueren.	Ja	Risicoanalyse	Ja	Gedefinieerd
A.8.17	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdsbronnen.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.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	Risicoanalyse	Ja	Geoptimaliseerd
A.8.19	Installeren van software op operationele systemen	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en Beheerst en meetbaar om informatie in systemen en toepassingen te beschermen.	Ja	Risicoanalyse	Ja	Gedefinieerd
A.8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja	Risicoanalyse	Ja	Gedefinieerd
A.8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Ja	Risicoanalyse	Ja	Gedefinieerd
A.8.23	Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja	Risicoanalyse	Ja	Gedefinieerd
A.8.24	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd	Ja	Risicoanalyse	Ja	Geoptimaliseerd

Verklaring van Toepasselijkheid & informatiebeveiliging beheersmaatregelen implementatie status (Annex A vanuit ISO 27001:2022)

Sectie		Toelichting op de informatiebeveiliging beheersmaatregelen	Van toepassing?	Reden voor insluiting / uitsluiting	Geïmplementeerd?	Volwassenheidsniveau
A.8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Ja	Contractuele verplichtingen	Ja	Herhaalbaar
A.8.26	Applicatie-beveiligingseisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja	Risicoanalyse	Ja	Beheerst en meetbaar
A.8.27	Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	Ja	Contractuele verplichtingen	Ja	Herhaalbaar
A.8.28	Veilig coderen	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	Ja	Contractuele verplichtingen	Ja	Herhaalbaar
A.8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging moeten worden Herhaalbaar en geïmplementeerd in de ontwikkelcyclus.	Ja	Contractuele verplichtingen	Ja	Herhaalbaar
A.8.30	Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Nee	Software-ontwikkeling wordt alleen intern gedaan.	NVT	Niet van toepassing
A.8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Ja	Risicoanalyse	Ja	Geoptimaliseerd
A.8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkingsfaciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	Ja	Best practices / bedrijfsvereisten	Ja	Geoptimaliseerd
A.8.33	Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Ja	Wet- en regelgeving	Ja	Geoptimaliseerd
A.8.34	Bescherming van informatiesystemen tijdens audits	Audits en andere borgingsactiviteiten waarbij operationele systemen worden beoordeeld moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Ja	Risicoanalyse	Ja	Geoptimaliseerd

Overzicht Management Systeem implementatiestatus

Volwassenheidsniveau	Betekenis	#	%
? Onbekend	Dit onderdeel is nog niet beoordeeld.	0	0%
Niet bestaand	Er is (nog) geen invulling gegeven aan dit onderdeel.	0	0%
Initieel	De organisatie is pas net begonnen met het inrichten van dit onderdeel. Er zijn misschien enkele ad-hoc maatregelen getroffen, maar over het algemeen is de aanpak informeel en ontbreekt het aan een gestructureerd kader.	0	0%
Gedefinieerd	De organisatie heeft formele beleidsdocumenten en procedures vastgesteld voor dit onderdeel. Er zijn basismaatregelen getroffen, maar er zijn nog inconsistenties en hiaten in de uitvoering daarvan.	0	0%
Herhaalbaar	De organisatie heeft formele beleidsdocumenten en procedures vastgesteld voor dit onderdeel, waarbij de vastgestelde maatregelen ook volgens de gemaakte afspraken worden uitgevoerd.	0	0%
Beheerst en meetbaar	De organisatie heeft formele beleidsdocumenten en procedures vastgesteld voor dit onderdeel, waarbij de vastgestelde maatregelen ook volgens de gemaakte afspraken worden uitgevoerd. Daarbij is er substantieel bewijs aanwezig om dit aan te tonen.	29	104%
Geoptimaliseerd	De organisatie heeft formele beleidsdocumenten en procedures vastgesteld voor dit onderdeel, waarbij de vastgestelde maatregelen ook aantoonbaar volgens de gemaakte afspraken worden uitgevoerd. Daarbij wordt ook regelmatig aandacht besteedt om dit onderdeel te verbeteren.	5	18%
Niet van toepassing	Alle vereisten vanuit de Harmonized Structure (HS) zijn verplicht om de ISO-certificering te behalen, maar specifieke maatregelen kunnen worden uitgesloten als er een passende reden wordt opgegeven.	0	0%
	Totaal	34	121%



Overzicht informatiebeveiligingsmaatregelen implementatiestatus

Volwassenheidsniveau	Betekenis	#	%
? Onbekend	Dit onderdeel is nog niet beoordeeld.	0	0%
Niet bestaand	Er is (nog) geen invulling gegeven aan dit onderdeel.	0	0%
Initieel	De organisatie is pas net begonnen met het inrichten van dit onderdeel. Er zijn misschien enkele ad-hoc maatregelen getroffen, maar over het algemeen is de aanpak informeel en ontbreekt het aan een gestructureerd kader.	1	1%
Gedefinieerd	De organisatie heeft formele beleidsdocumenten en procedures vastgesteld voor dit onderdeel. Er zijn basismaatregelen getroffen, maar er zijn nog inconsistenties en hiaten in de uitvoering daarvan.	8	9%
Herhaalbaar	De organisatie heeft formele beleidsdocumenten en procedures vastgesteld voor dit onderdeel, waarbij de vastgestelde maatregelen ook volgens de gemaakte afspraken worden uitgevoerd.	8	9%
Beheerst en meetbaar	De organisatie heeft formele beleidsdocumenten en procedures vastgesteld voor dit onderdeel, waarbij de vastgestelde maatregelen ook volgens de gemaakte afspraken worden uitgevoerd. Daarbij is er substantieel bewijs aanwezig om dit aan te tonen.	29	31%
Geoptimaliseerd	De organisatie heeft formele beleidsdocumenten en procedures vastgesteld voor dit onderdeel, waarbij de vastgestelde maatregelen ook aantoonbaar volgens de gemaakte afspraken worden uitgevoerd. Daarbij wordt ook regelmatig aandacht besteedt om dit onderdeel te verbeteren.	45	48%
Niet van toepassing	Alle vereisten vanuit de Harmonized Structure (HS) zijn verplicht om de ISO-certificering te behalen, maar specifieke maatregelen kunnen worden uitgesloten als er een passende reden wordt opgegeven.	2	2%
	Totaal	93	100%