Handreiking BIO2.0-opmaat

De kolomkoppen met rechts bovenin een rode driehoek bevatten een toelichting.

Control-nr.	Control-soort	BBN van control	Control-titel	Control	Doel	Control-nr. BIO 1.0.4zv	Maatregelnr. BIO 1.0.4zv	Maatregel-nummer	BBN van maatregel	Overheidsmaatregel	Verantwoordelijke(n)	Type control	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligingsdomeinen
5.1	Organisatorisch	1	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 en als zich significante wijzigingen voordoen, te worden beoordeeld.	De voortdurende geschiktheid, toereikendheid, doeltreffendheid van de sturing en ondersteuning door het management overeenkomstig de bedrijfseisen en de eisen van wet- en regelgeving, statutaire en contractuele eisen bewerkstelligen.	05.1.1	05.1.1.1	5.01.1	1	De organisatie heeft een informatiebeveiligingsbeleid opgesteld. Dit beleid is vastgesteld door de leiding van de organisatie en bevat ten minste de volgende punten: (a) De strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. (b) De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. (c) De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers. (d) De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn. (e) De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd.	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_en_Ecosysteem #Veerkracht
5.1	Organisatorisch	1	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 en als zich significante wijzigingen voordoen, te worden beoordeeld.	De voortdurende geschiktheid, toereikendheid, doeltreffendheid van de sturing en ondersteuning door het management overeenkomstig de bedrijfseisen en de eisen van wet- en regelgeving, statutaire en contractuele eisen bewerkstelligen.	05.1.2	05.1.2.1	5.01.2	1	Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en Planning & Control (P&C)-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_en_Ecosysteem #Veerkracht
5.2	Organisatorisch	1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Een gedefinieerde, goedgekeurde en duidelijk te begrijpen structuur voor de implementatie, uitvoering en het beheer van informatiebeveiliging binnen de organisatie inrichten.	06.1.1	06.1.1.1	5.02.1	1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_en_Ecosysteem #Bescherming #Veerkracht
5.2	Organisatorisch	1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Een gedefinieerde, goedgekeurde en duidelijk te begrijpen structuur voor de implementatie, uitvoering en het beheer van informatiebeveiliging binnen de organisatie inrichten.	06.1.1	06.1.1.2	5.02.2	1	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_en_Ecosysteem #Bescherming #Veerkracht
5.2	Organisatorisch	1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Een gedefinieerde, goedgekeurde en duidelijk te begrijpen structuur voor de implementatie, uitvoering en het beheer van informatiebeveiliging binnen de organisatie inrichten.	06.1.1	06.1.1.3	5.02.3	1	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_en_Ecosysteem #Bescherming #Veerkracht
5.2	Organisatorisch	1	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Een gedefinieerde, goedgekeurde en duidelijk te begrijpen structuur voor de implementatie, uitvoering en het beheer van informatiebeveiliging binnen de organisatie inrichten.	06.1.1	06.1.1.4	5.02.4	1	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_en_Ecosysteem #Bescherming #Veerkracht
5.3	Organisatorisch	1	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden behoren te worden gescheiden.	Het risico op fraude, fouten en het omzeilen van beheersmaatregelen voor informatiebeveiliging verminderen.	06.1.2	06.1.2.1	5.03.1	1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Governance #Identiteits-_en_toegangsbeheer	#Governance_en_Ecosysteem
5.4	Organisatorisch	1	Managementverantwoordelijkheden	Het management behoort van al het personeel te eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en	Bewerkstelligen dat het management zijn rol bij informatiebeveiliging begrijpt en maatregelen neemt om ervoor te zorgen dat al het personeel zich bewust is van zijn verantwoordelijkheden op het gebied van informatiebeveiliging en deze ook nakomt.	07.2.1	07.2.1.1	5.04.1	1	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen anoniem en veilig beveiligingsissues kan melden.	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Governance	#Governance_en_Ecosysteem
5.5	Organisatorisch	2	Contact met overheidsinstanties	De organisatie behoort contact met de relevante instanties te leggen en te onderhouden.	Een passende stroom van informatie met betrekking tot informatiebeveiliging tussen de organisatie en relevante juridische, regelgevende en toezichthoudende instanties bewerkstelligen.	06.1.3	06.1.3.1	5.05.1	2	De organisatie heeft uitgewerkt wie met welke (overheids)instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen #Reageren #Herstellen	#Governance	#Verdediging #Veerkracht
5.5	Organisatorisch	2	Contact met overheidsinstanties	De organisatie behoort contact met de relevante instanties te leggen en te onderhouden.	Een passende stroom van informatie met betrekking tot informatiebeveiliging tussen de organisatie en relevante juridische, regelgevende en toezichthoudende instanties bewerkstelligen.	06.1.3	06.1.3.2	5.05.2	2	Het contactoverzicht wordt jaarlijks geactualiseerd.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen #Reageren #Herstellen	#Governance	#Verdediging #Veerkracht
5.6	Organisatorisch	-	Contact met speciale belangengroepen	De organisatie behoort contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen te leggen en te onderhouden.	Een passende stroom van informatie met betrekking tot informatiebeveiliging bewerkstelligen.	06.1.4	/	/	/	/	-	#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Reageren #Herstellen	#Governance	#Verdediging
5.7	Organisatorisch	2	Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen behoort te worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren.	Bewustwording bieden van de mogelijke dreigingen voor de organisatie zodat de passende mitigerende maatregelen kunnen worden getroffen.	/	/	/	/	Dit is een nieuwe control. Er zijn geen overheidsmaatregelen nodig. De richtlijnen uit de NEN-EN-ISO/IEC 27002:2022 geven voldoende houvast.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief #Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Detecteren #Reageren	#Beheer_van_bedreigingen_en_kwetsbaarheden	#Verdediging #Veerkracht
5.8	Organisatorisch	2	Informatiebeveiliging in projectmanagement	Informatiebeveiliging behoort te worden geïntegreerd in projectmanagement.	Ervoor zorgen dat informatiebeveiligingsrisico's binnen projecten en te leveren producten en diensten gedurende de gehele levenscyclus van het project op doeltreffende wijze binnen het projectmanagement worden	06.1.5	/	/	/	/	Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Governance	#Governance_en_Ecosysteem #Bescherming
5.8	Organisatorisch	2	Informatiebeveiliging in projectmanagement	Informatiebeveiliging behoort te worden geïntegreerd in projectmanagement.	Ervoor zorgen dat informatiebeveiligingsrisico's binnen projecten en te leveren producten en diensten gedurende de gehele levenscyclus van het project op doeltreffende wijze binnen het projectmanagement worden	14.1.1	14.1.1.1	5.08.1	1	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO.	Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Governance	#Governance_en_Ecosysteem #Bescherming
5.9	Organisatorisch	1	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.	De informatie en andere gerelateerde bedrijfsmiddelen van de organisatie identificeren om de informatiebeveiliging ervan te behouden en passend	08.1.1	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beheer_van_bedrijfsmiddelen	#Governance_en_Ecosysteem #Bescherming
5.9	Organisatorisch	1	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.	De informatie en andere gerelateerde bedrijfsmiddelen van de organisatie identificeren om de informatiebeveiliging ervan te behouden en passend	08.1.2	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beheer_van_bedrijfsmiddelen	#Governance_en_Ecosysteem #Bescherming
5.10	Organisatorisch	1	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 behoren te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen passend worden beschermd, gebruikt en behandeld.	08.1.3	08.1.3.1	5.10.1	1	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Governance_en_Ecosysteem #Bescherming
5.10	Organisatorisch	1	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 behoren te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen passend worden beschermd, gebruikt en behandeld.	08.1.3	08.1.3.2	5.10.2	1	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Governance_en_Ecosysteem #Bescherming
5.10	Organisatorisch	1	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 behoren te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen passend worden beschermd, gebruikt en behandeld.	08.2.3	/	/	/	/	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Governance_en_Ecosysteem #Bescherming

5.11	Organisatorisch	1	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.	De bedrijfsmiddelen van de organisatie beschermen als onderdeel van de procedure voor het wijzigen of beëindigen van het dienstverband, het contract of de overeenkomst.	08.1.4	/	/	/	/	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen	#Bescherming
5.12	Organisatorisch	1	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 eisen van belanghebbenden.	Bewerkstelligen dat het identificeren van en het inzicht in de beschermingsbehoeften voor informatie in overeenstemming zijn met het belang ervan voor de organisatie.	08.2.1	08.2.1.1	5.12.1	1	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Informatiebescherming	#Bescherming #Verdediging
5.13	Organisatorisch	1	Labelen van informatie	Om informatie te labelen, behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Het communiceren van de classificatie van informatie mogelijk maken en het automatiseren van informatieverwerking en -beheer ondersteunen.	08.2.2	/	/	/	/	Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Informatiebescherming	#Verdediging #Bescherming
5.14	Organisatorisch	1	Overdragen van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe belanghebbende.	13.2.3	13.2.3.1	5.14.1	1	Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en afluisteren op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. Voor beveiliging van websiteverkeer gelden de open standaarden tegen afluisteren op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Bescherming
5.14	Organisatorisch	1	Overdragen van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe belanghebbende.	13.2.3	13.2.3.2	5.14.2	2	Voor veilige berichtenuitwisseling met basisregistraties wordt, conform de 'pas toe of leg uit'-lijst van het Forum Standaardisatie, gebruik gemaakt van de actuele versie van Digikoppeling.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Bescherming
5.14	Organisatorisch	1	Overdragen van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe belanghebbende.	13.2.3	13.2.3.3	5.14.3	2	Maak bij openbaar webverkeer van gevoelige gegevens gebruik van ten minste publiek vertrouwde Organization Validated-certificaten. Maak bij intern webverkeer voor gevoelige gegevens gebruik van ten minste publieke vertrouwde OV-certificaten of private PKIo-certificaten. Hogere eisen aan certificaten kunnen voortvloeien uit een risicoanalyse, aansluitvoorwaarden of wetgeving.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Bescherming
5.14	Organisatorisch	1	Overdragen van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe belanghebbende.	13.2.3	/	5.14.4	2	Verzend gevoelige gegevens via e-mail alleen over onvertrouwde netwerken als de keten tussen verzender en ontvanger voldoende beveiligd is zoals door het toepassen van maatregel 5.14.1.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Bescherming
5.14	Organisatorisch	1	Overdragen van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe belanghebbende.	13.2.3	13.2.3.4	5.14.5	2	Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Bescherming
5.14	Organisatorisch	1	Overdragen van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe belanghebbende.	13.2.1	/	/	/	/	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Bescherming
5.14	Organisatorisch	1	Overdragen van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe belanghebbende.	13.2.2	/	/	/	/	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Bescherming
5.15	Organisatorisch	1	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.	Toegang voor bevoegden bewerkstelligen en toegang voor onbevoegden tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen.	09.1.1	/	/	/	/	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.15	Organisatorisch	1	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.	Toegang voor bevoegden bewerkstelligen en toegang voor onbevoegden tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen.	09.1.2	09.1.2.1	5.15.1	1	Alleen geauthentiseerde apparatuur kan toegang krijgen tot een vertrouwde zone.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.15	Organisatorisch	1	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.	Toegang voor bevoegden bewerkstelligen en toegang voor onbevoegden tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen.	09.1.2	09.1.2.2	5.15.2	1	Gebruikers met eigen of ongeauthentiseerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.16	Organisatorisch	1	Identiteitsbeheer	De volledige levenscyclus van identiteiten behoort te worden beheerd.	De unieke identificatie van personen en systemen die toegang hebben tot de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie, en een juiste toewijzing van toegangsrechten ondersteunen.	09.2.1	09.2.1.1	5.16.1	1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.16	Organisatorisch	1	Identiteitsbeheer	De volledige levenscyclus van identiteiten behoort te worden beheerd.	De unieke identificatie van personen en systemen die toegang hebben tot de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie, en een juiste toewijzing van toegangsrechten ondersteunen.	09.2.1	09.2.1.2	5.16.2	1	Het gebruiken van groepsaccounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.17	Organisatorisch	1	Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Goede authenticatie bewerkstelligen en fouten van authenticatieprocessen voorkomen.	09.4.3	09.4.3.1 09.4.3.2 09.4.3.5	5.17.1	1	Bij het aanloggen op een vertrouwde zone: (a) is het gebruik van tweefactor-authenticatie altijd verplicht; (b) is de minimale wachtwoordlengte 12 posities en wordt het wachtwoord minimaal halfjaarlijks vernieuwd als geen tweefactor-authenticatie mogelijk is (zie ook 8.5.1); (c) mogen wachtwoorden niet worden hergebruikt; (d) zijn de tekens van een wachtwoord zo willekeurig mogelijk gekozen dat individuele tekens of combinaties van tekens geen voorspellende waarde hebben voor de rest van het wachtwoord; (e) is het aantal inlogpogingen maximaal 5; (f) is de tijdsduur vastgelegd dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen; (g) wordt in het bewustwordingsprogramma en de gedragsregels ingegaan op het belang van het hebben van goede wachtwoorden 45). 45) Vanuit een vertrouwde zone mag op basis van een risicoafweging afgeweken worden van bovenstaande regels.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.17	Organisatorisch	1	Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Goede authenticatie bewerkstelligen en fouten van authenticatieprocessen voorkomen.	09.3.1	09.3.1.1	5.17.2	2	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordmanager of een vergelijkbaar systeem.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.17	Organisatorisch	1	Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Goede authenticatie bewerkstelligen en fouten van authenticatieprocessen voorkomen.	09.3.1	/	5.17.3	2	Een wachtwoordmanager is in staat om een waarschuwing te geven als de combinatie van account en wachtwoord voorkomt op lijsten met gecompromitteerde wachtwoorden of het vermoeden bestaat dat het wachtwoord gecompromitteerd is. In dat geval moet het wachtwoord worden gewijzigd.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming

5.17	Organisatorisch	1	Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Goede authenticatie bewerkstelligen en fouten van authenticatieprocessen voorkomen.	09.4.3	09.4.3.3	5.17.4	2	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.17	Organisatorisch	1	Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Goede authenticatie bewerkstelligen en fouten van authenticatieprocessen voorkomen.	09.4.3	09.4.3.4	5.17.5	2	Van initiële wachtwoorden en wachtwoorden die gereset zijn, wordt automatisch afgedwongen dat deze bij het eerste gebruik worden gewijzigd.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.17	Organisatorisch	1	Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Goede authenticatie bewerkstelligen en fouten van authenticatieprocessen voorkomen.	09.2.4	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.18	Organisatorisch	1	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de	Bewerkstelligen dat de toegang tot informatie en andere gerelateerde bedrijfsmiddelen wordt vastgesteld en goedgekeurd overeenkomstig de bedrijfseisen.	09.2.2	09.2.2.1	5.18.1	1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.18	Organisatorisch	1	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de	Bewerkstelligen dat de toegang tot informatie en andere gerelateerde bedrijfsmiddelen wordt vastgesteld en goedgekeurd overeenkomstig de bedrijfseisen.	09.2.2	09.2.2.2	5.18.2	1	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.18	Organisatorisch	1	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de	Bewerkstelligen dat de toegang tot informatie en andere gerelateerde bedrijfsmiddelen wordt vastgesteld en goedgekeurd overeenkomstig de bedrijfseisen.	09.2.5	09.2.5.1	5.18.4	1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.18	Organisatorisch	1	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de	Bewerkstelligen dat de toegang tot informatie en andere gerelateerde bedrijfsmiddelen wordt vastgesteld en goedgekeurd overeenkomstig de bedrijfseisen.	09.2.5	09.2.5.2	5.18.6	1	Ongeautoriseerde afwijkingen op of ongeautoriseerde aanpassingen aan uitgegeven toegangsrechten worden beschouwd als beveiligingsgebeurtenis en als zodanig vastgelegd en afgehandeld.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.18	Organisatorisch	1	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de	Bewerkstelligen dat de toegang tot informatie en andere gerelateerde bedrijfsmiddelen wordt vastgesteld en goedgekeurd overeenkomstig de bedrijfseisen.	09.2.2	09.2.2.3	5.18.3	2	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.18	Organisatorisch	1	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de	Bewerkstelligen dat de toegang tot informatie en andere gerelateerde bedrijfsmiddelen wordt vastgesteld en goedgekeurd overeenkomstig de bedrijfseisen.	09.2.5	09.2.5.3	5.18.5	2	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.18	Organisatorisch	1	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen behoren te worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de	Bewerkstelligen dat de toegang tot informatie en andere gerelateerde bedrijfsmiddelen wordt vastgesteld en goedgekeurd overeenkomstig de bedrijfseisen.	09.2.6	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
5.19	Organisatorisch	1	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 beheersen.	Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.	15.1.1	15.1.1.1	5.19.1	1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden inkoopeisen ten aanzien van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging. Bijvoorbeeld kan gebruik gemaakt worden van de maatregelset uit de Inkoopeisen Cybersecurity Overheid (ICO).	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming
5.19	Organisatorisch	1	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 beheersen.	Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.	15.1.1	15.1.1.2	5.19.2	2	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekking tot leverancierstoegang tot bedrijfsinformatie vastgesteld.	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming
5.19	Organisatorisch	1	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 beheersen.	Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.	15.1.1	15.1.1.3	5.19.3	2	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming
5.20	Organisatorisch	1	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.	15.1.2	15.1.2.1	5.20.1	1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar de verwerking van informatie een rol speelt.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming
5.20	Organisatorisch	1	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.	15.1.2	15.1.2.2	5.20.2	1	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming
5.20	Organisatorisch	1	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.	15.1.2	15.1.2.3	5.20.3	1	In situaties waarin contractvoorwaarden worden opgelegd door leveranciers, is voorafgaand aan het tekenen van het contract met een risicoafweging helder gemaakt wat de consequenties hiervan zijn voor de organisatie. Expliciet is gemaakt welke consequenties geaccepteerd worden, welke gemitigeerd moeten zijn en welke voorwaarden niet of nooit geaccepteerd mogen worden bij het	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming
5.20	Organisatorisch	1	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.	15.1.2	15.1.2.4	5.20.4	1	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaardvoorwaarden voor inkoop gehanteerd.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming
5.20	Organisatorisch	1	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.	15.1.2	15.1.2.5	5.20.5	2	Voordat een contract wordt afgesloten, wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming
5.20	Organisatorisch	1	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen behoren te worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.	15.1.2	15.1.2.6	5.20.6	2	In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst. Een audit is niet nodig als de contractant door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming
5.21	Organisatorisch	1	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Er behoren processen en procedures te worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.	Een overeengekomen niveau van informatiebeveiliging in leveranciersrelaties in stand houden.	15.1.3	15.1.3.1	5.21.1	2	Leveranciers moeten gedurende de looptijd van het contract: (a) hun keten van toeleveranciers bekendmaken; (b) transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers; (c) transparant zijn over de resultaten van de controle bij toeleveranciers over de aan hen opgelegde maatregelen, zie ook paragraaf 4.4;	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming

5.22	Organisatorisch	1	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie behoort de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig te monitoren, beoordelen, evalueren en veranderingen daaraan te beheren.	Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.	15.2.1	15.2.1.1	5.22.1	2	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.	Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_leveranciersrelaties #Borging_van_informatiebeveiliging	#Governance_en_Ecosysteem #Bescherming #Verdediging
5.22	Organisatorisch	1	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie behoort de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig te monitoren, beoordelen, evalueren en veranderingen daaraan te beheren.	Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.	15.2.2	/	/	/	/	Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Beveiliging_in_leveranciersrelaties #Borging_van_informatiebeveiliging	#Governance_en_Ecosysteem #Bescherming #Verdediging
5.23	Organisatorisch	1	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.	Informatiebeveiliging voor het gebruik van clouddiensten specificeren en beheren.	/	/	/	/	Dit is een nieuwe control. Er zijn geen overheidsmaatregelen nodig. De richtlijnen uit de NEN-EN-ISO/IEC 27002:2022 geven voldoende houvast.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming
5.24	Organisatorisch	1	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 informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Een snelle, doeltreffende, consistente en geordende reactie op informatiebeveiligingsincidenten, met inbegrip van communicatie over informatiebeveiligingsgebeurtenissen, bewerkstelligen.	16.1.1	/	/	/	/	Secretaris/Algemeen directeur Proceseigenaar Dienstleverancier	#Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Reageren #Herstellen	#Governance #Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
5.24	Organisatorisch	1	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 informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Een snelle, doeltreffende, consistente en geordende reactie op informatiebeveiligingsincidenten, met inbegrip van communicatie over informatiebeveiligingsgebeurtenissen, bewerkstelligen.	16.1.2	16.1.2.1	5.24.1	1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.	Secretaris/Algemeen directeur Proceseigenaar Dienstleverancier	#Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Reageren #Herstellen	#Governance #Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
5.24	Organisatorisch	1	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 informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Een snelle, doeltreffende, consistente en geordende reactie op informatiebeveiligingsincidenten, met inbegrip van communicatie over informatiebeveiligingsgebeurtenissen, bewerkstelligen.	16.1.2	16.1.2.2	5.24.2	1	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	Secretaris/Algemeen directeur Proceseigenaar Dienstverlener	#Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Reageren #Herstellen	#Governance #Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
5.24	Organisatorisch	1	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 informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Een snelle, doeltreffende, consistente en geordende reactie op informatiebeveiligingsincidenten, met inbegrip van communicatie over informatiebeveiligingsgebeurtenissen, bewerkstelligen.	16.1.2	16.1.2.5	5.24.3	1	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	Secretaris/Algemeen directeur Proceseigenaar Dienstverlener	#Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Reageren #Herstellen	#Governance #Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
5.24	Organisatorisch	1	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 informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Een snelle, doeltreffende, consistente en geordende reactie op informatiebeveiligingsincidenten, met inbegrip van communicatie over informatiebeveiligingsgebeurtenissen, bewerkstelligen.	16.1.2	16.1.2.6	5.24.4	1	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.	Secretaris/Algemeen directeur Proceseigenaar Dienstverlener	#Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Reageren #Herstellen	#Governance #Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
5.24	Organisatorisch	1	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 informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Een snelle, doeltreffende, consistente en geordende reactie op informatiebeveiligingsincidenten, met inbegrip van communicatie over informatiebeveiligingsgebeurtenissen, bewerkstelligen.	16.1.3	16.1.3.1	5.24.5	1	Een Coordinated Vulnerability Disclosure (CVD)-procedure is gepubliceerd en ingericht, inclusief de opvolging 46). 46) Voorheen werd Coordinated Vulnerability Disclosure (CVD) responsible disclosure genoemd.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Reageren #Herstellen	#Governance #Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
5.24	Organisatorisch	1	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 informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Een snelle, doeltreffende, consistente en geordende reactie op informatiebeveiligingsincidenten, met inbegrip van communicatie over informatiebeveiligingsgebeurtenissen, bewerkstelligen.	16.1.2	16.1.2.7	5.24.6	1	Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD)-procedure is onderdeel van de incidentrapportage.	Secretaris/Algemeen directeur Proceseigenaar Dienstverlener	#Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Reageren #Herstellen	#Governance #Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
5.25	Organisatorisch	1	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie behoort informatiebeveiligingsgebeurtenissen te beoordelen en te beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Doeltreffende categorisering en prioritering van informatiebeveiligingsgebeurtenissen bewerkstelligen.	16.1.4	16.1.4.1	5.25.1	2	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.	Proceseigenaar Dienstenleverancier	#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren #Reageren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
5.26	Organisatorisch	1	Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Een doelmatige en doeltreffende reactie op informatiebeveiligingsincidenten bewerkstelligen.	16.1.5	/	/	/	/	Proceseigenaar Dienstenleverancier	#Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Reageren #Herstellen	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
5.27	Organisatorisch	2	Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten behoort te worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	De waarschijnlijkheid of de gevolgen van toekomstige incidenten verminderen.	16.1.6	16.1.6.1	5.27.1	2	Beveiligingsincidenten worden geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
5.27	Organisatorisch	2	Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten behoort te worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	De waarschijnlijkheid of de gevolgen van toekomstige incidenten verminderen.	16.1.6	16.1.6.2	5.27.2	2	De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
5.28	Organisatorisch	2	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.	In het kader van disciplinaire en gerechtelijke stappen consistent en doeltreffend beheer bewerkstelligen van bewijsmateriaal in verband met informatiebeveiligingsincidenten.	16.1.7	16.1.7.1	5.28.1	2	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren #Reageren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
5.29	Organisatorisch	1	Informatiebeveiliging tijdens een verstoring	De organisatie behoort plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Informatie en andere gerelateerde bedrijfsmiddelen tijdens een verstoring beschermen.	17.1.3	17.1.3.1	5.29.1	2	Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.	Proceseigenaar Dienstenleverancier	#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Reageren	#Continuïteit	#Bescherming #Veerkracht
5.29	Organisatorisch	1	Informatiebeveiliging tijdens een verstoring	De organisatie behoort plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Informatie en andere gerelateerde bedrijfsmiddelen tijdens een verstoring beschermen.	17.1.3	17.1.3.2	5.29.2	2	Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.	Proceseigenaar Dienstenleverancier	#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Reageren	#Continuïteit	#Bescherming #Veerkracht
5.29	Organisatorisch	1	Informatiebeveiliging tijdens een verstoring	De organisatie behoort plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Informatie en andere gerelateerde bedrijfsmiddelen tijdens een verstoring beschermen.	17.1.3	17.1.3.3	5.29.3	2	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten uiterlijk binnen een week hersteld.	Proceseigenaar Dienstenleverancier	#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Reageren	#Continuïteit	#Bescherming #Veerkracht
5.29	Organisatorisch	1	Informatiebeveiliging tijdens een verstoring	De organisatie behoort plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Informatie en andere gerelateerde bedrijfsmiddelen tijdens een verstoring beschermen.	17.1.1	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Reageren	#Continuïteit	#Bescherming #Veerkracht
5.29	Organisatorisch	1	Informatiebeveiliging tijdens een verstoring	De organisatie behoort plannen te maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Informatie en andere gerelateerde bedrijfsmiddelen tijdens een verstoring beschermen.	17.1.2	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Reageren	#Continuïteit	#Bescherming #Veerkracht

5.30	Organisatorisch	1	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid behoort te worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.	De beschikbaarheid van de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie tijdens een verstoring waarborgen.	/	/	/	/	Dit is een nieuwe control. Er zijn geen overheidsmaatregelen nodig. De richtlijnen uit de NEN-EN-ISO/IEC 27002:2022 geven voldoende houvast.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Corrigerend	#Beschikbaarheid	#Reageren	#Continuïteit	#Veerkracht
5.31	Organisatorisch	1	Wettelijke, statutaire, regelgevende en contractuele eisen	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 geïdentificeerd, gedocumenteerd en actueel gehouden.	De naleving bewerkstelligen van wettelijke, statutaire, regelgevende en contractuele eisen in verband met informatiebeveiliging.	18.1.5	18.1.5.1	5.31.1	1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie.	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Juridisch_en_compliance	#Governance_en_Ecosysteem #Bescherming
5.31	Organisatorisch	1	Wettelijke, statutaire, regelgevende en contractuele eisen	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 geïdentificeerd, gedocumenteerd en actueel gehouden.	De naleving bewerkstelligen van wettelijke, statutaire, regelgevende en contractuele eisen in verband met informatiebeveiliging.	18.1.5	/	5.31.2	2	Zie overheidsmaatregel 8.24.1.	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Juridisch_en_compliance	#Governance_en_Ecosysteem #Bescherming
5.31	Organisatorisch	1	Wettelijke, statutaire, regelgevende en contractuele eisen	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 geïdentificeerd, gedocumenteerd en actueel gehouden.	De naleving bewerkstelligen van wettelijke, statutaire, regelgevende en contractuele eisen in verband met informatiebeveiliging.	18.1.1	/	/	/	/	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Juridisch_en_compliance	#Governance_en_Ecosysteem #Bescherming
5.32	Organisatorisch	1	Intellectuele-eigendomsrechten	De organisatie behoort passende procedures te implementeren om intellectuele-eigendomsrechten te beschermen.	De naleving bewerkstelligen van eisen van wet- en regelgeving, statutaire en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van propriëtaire producten.	18.1.2	/	/	/	/	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Juridisch_en_compliance	#Governance_en_Ecosysteem
5.33	Organisatorisch	2	Beschermen van registraties	Registraties behoren te worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	De naleving bewerkstelligen van wet- en regelgeving, statutaire en contractuele eisen, alsmede gemeenschaps- of maatschappelijke verwachtingen, met betrekking tot de bescherming en beschikbaarheid van registraties.	18.1.3	18.1.3.1	5.33.1	2	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Juridisch_en_compliance #Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Verdediging
5.34	Organisatorisch	1	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.	De naleving bewerkstelligen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot de informatiebeveiligingsaspecten voor de bescherming van persoonsgegevens.	18.1.4	18.1.4.1	5.34.1	1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Informatiebescherming #Juridisch_en_compliance	#Bescherming
5.34	Organisatorisch	1	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.	De naleving bewerkstelligen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot de informatiebeveiligingsaspecten voor de bescherming van persoonsgegevens.	18.1.4	18.1.4.2	5.34.2	2	Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Informatiebescherming #Juridisch_en_compliance	#Bescherming
5.35	Organisatorisch	1	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	Waarborgen dat de organisatie continu een geschikte, toereikende en doeltreffende aanpak voor het beheer van informatiebeveiliging hanteert.	18.2.1	18.2.1.1	5.35.1	2	Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Borging_van_informatiebeveiliging	#Governance_en_Ecosysteem
5.35	Organisatorisch	1	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	Waarborgen dat de organisatie continu een geschikte, toereikende en doeltreffende aanpak voor het beheer van informatiebeveiliging hanteert.	18.2.1	18.2.1.2	5.35.2	2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Borging_van_informatiebeveiliging	#Governance_en_Ecosysteem
5.36	Organisatorisch	1	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie behoren regelmatig te worden beoordeeld.	Bewerkstelligen dat informatiebeveiliging in overeenstemming met het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en normen van de organisatie wordt geïmplementeerd en uitgevoerd.	18.2.2	18.2.2.1	5.36.1	1	In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Juridisch_en_compliance #Borging_van_informatiebeveiliging	#Governance_en_Ecosysteem
5.36	Organisatorisch	1	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie behoren regelmatig te worden beoordeeld.	Bewerkstelligen dat informatiebeveiliging in overeenstemming met het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en normen van de organisatie wordt geïmplementeerd en uitgevoerd.	18.2.3	/	/	/	/	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Juridisch_en_compliance #Borging_van_informatiebeveiliging	#Governance_en_Ecosysteem
5.37	Organisatorisch	1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan het personeel dat ze nodig heeft.	De correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.	12.1.1	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Herstellen	#Beheer_van_bedrijfsmiddelen #Fysieke_beveiliging #Systeem-_en_netwerkbeveiliging #Toepassingsbeveiliging #Veilige_configuratie #Identiteits-_en_toegangsbeheer #Beheer_van_bedreigingen_en_kwetsbaarheden #Continuïteit #Beheer_van_informatiebeveiligingsgebeurtenissen	#Governance_en_Ecosysteem #Bescherming #Verdediging
6.1	Mensgericht	1	Screening	De achtergrond van alle kandidaten voor een dienstverband 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 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.	Bewerkstelligen dat al het personeel in aanmerking komt en geschikt is voor de functies waarvoor zij worden overwogen en dat zij hiervoor gedurende hun dienstverband in aanmerking blijven komen en geschikt blijven.	07.1.1	07.1.1.1	6.01.1	1	Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan een Verklaring Omtrent het Gedrag (VOG) gevraagd worden.	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Personeelsbeveiliging	#Governance_en_Ecosysteem
6.2	Mensgericht	1	Arbeidsovereenkomst	In arbeidsovereenkomsten behoort te worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Bewerkstelligen dat personeel begrijpt wat hun verantwoordelijkheden zijn op het gebied van informatiebeveiliging voor de rollen waarvoor zij mogelijk in aanmerking komen.	07.1.2	07.1.2.1	6.02.1	1	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Personeelsbeveiliging	#Governance_en_Ecosysteem
6.3	Mensgericht	1	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden behoren een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, te krijgen.	Ervoor zorgen dat personeel en relevante belanghebbenden zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.	07.2.2	07.2.2.1	6.03.1	1	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Personeelsbeveiliging	#Governance_en_Ecosysteem
6.3	Mensgericht	1	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden behoren een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, te krijgen.	Ervoor zorgen dat personeel en relevante belanghebbenden zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.	07.2.2	07.2.2.2	6.03.2	1	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Personeelsbeveiliging	#Governance_en_Ecosysteem

6.3	Mensgericht	1	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden behoren een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, te krijgen.	Ervoor zorgen dat personeel en relevante belanghebbenden zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.	07.2.2	07.2.2.3	6.03.3	1	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Personeelsbeveiliging	#Governance_en_Ecosysteem
6.4	Mensgericht	1	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.	Bewerkstelligen dat personeel en andere relevante belanghebbenden de gevolgen begrijpen van schending van het informatiebeveiligingsbeleid, personeel en andere relevante belanghebbenden ervan weerhouden zich schuldig te maken aan een schending, en personeel en andere relevante belanghebbenden die zich schuldig hebben gemaakt aan een schending op de juiste manier aanpakken.	07.2.3	/	/	/	/	Secretaris/Algemeen directeur	#Preventief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Reageren	#Personeelsbeveiliging	#Governance_en_Ecosysteem
6.5	Mensgericht	1	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.	De belangen van de organisatie beschermen als onderdeel van de wijzigings- of beëindigingsprocedure van dienstverband of contracten.	07.3.1	/	/	/	/	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Personeelsbeveiliging #Beheer_van_bedrijfsmiddelen	#Governance_en_Ecosysteem
6.6	Mensgericht	1	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.	De vertrouwelijkheid van informatie waartoe personeel of externe partijen toegang hebben, handhaven.	13.2.4	/	/	/	/	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid	#Beschermen	#Personeelsbeveiliging #Informatiebescherming #Leveranciersrelaties	#Governance_en_Ecosysteem
6.7	Mensgericht	2	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.	De beveiliging van informatie waarborgen wanneer personeel op afstand werkt.	06.2.2	/	/	/	/	Secretaris/Algemeen directeur Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming #Fysieke_beveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
6.8	Mensgericht	1	Melden van informatiebeveiligingsgebeurtenissen	De organisatie behoort te voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Tijdige, consistente en doeltreffende melding ondersteunen van informatiebeveiligingsgebeurtenissen die door personeel kunnen worden geïdentificeerd.	16.1.2	16.1.2.3	6.08.1	1	Alle medewerkers en contractanten hebben aantoonbaar kennisgenomen van de meldingsprocedure van incidenten.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
6.8	Mensgericht	1	Melden van informatiebeveiligingsgebeurtenissen	De organisatie behoort te voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Tijdige, consistente en doeltreffende melding ondersteunen van informatiebeveiligingsgebeurtenissen die door personeel kunnen worden geïdentificeerd.	16.1.2	16.1.2.4	6.08.2	1	Incidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
6.8	Mensgericht	1	Melden van informatiebeveiligingsgebeurtenissen	De organisatie behoort te voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Tijdige, consistente en doeltreffende melding ondersteunen van informatiebeveiligingsgebeurtenissen die door personeel kunnen worden geïdentificeerd.	16.1.3	16.1.3.1	6.08.3	1	Een Coordinated Vulnerability Disclosure (CVD)-procedure is gepubliceerd en ingericht.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
7.1	Fysiek	1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, behoren te worden beschermd door beveiligingszones te definiëren en te gebruiken.	Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en andere gerelateerde bedrijfsmiddelen van de organisatie voorkomen.	11.1.1	11.1.1.1	7.01.1	1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.2	Fysiek	1	Fysieke toegangsbeveiliging	Beveiligde zones behoren te worden beschermd door passende toegangsbeveiligings-maatregelen en toegangspunten.	Bewerkstelligen dat er alleen bevoegde fysieke toegang tot de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie plaatsvindt.	11.1.2	11.1.2.1	7.02.1	2	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Identiteits-_en_toegangsbeheer	#Bescherming
7.2	Fysiek	1	Fysieke toegangsbeveiliging	Beveiligde zones behoren te worden beschermd door passende toegangsbeveiligings-maatregelen en toegangspunten.	Bewerkstelligen dat er alleen bevoegde fysieke toegang tot de informatie en andere gerelateerde bedrijfsmiddelen van de organisatie plaatsvindt.	11.1.6	/	/	/	/	Secretaris/Algemeen directeur	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Identiteits-_en_toegangsbeheer	#Bescherming
7.3	Fysiek	1	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en geïmplementeerd.	Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en andere gerelateerde bedrijfsmiddelen van de organisatie in kantoren, ruimten en faciliteiten voorkomen.	11.1.3	11.1.3.1	7.03.1	1	Sleutelbeheer is ingericht op basis van een sleutelplan.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming
7.4	Fysiek	1	Monitoren van de fysieke beveiliging	Het gebouw en terrein behoort voortdurend te worden gemonitord op onbevoegde fysieke toegang.	Onbevoegde fysieke toegang detecteren en ontmoedigen.	/	/	/	/	Dit is een nieuwe control. Er zijn geen overheidsmaatregelen nodig. De richtlijnen uit de NEN-EN-ISO/IEC 27002:2022 geven voldoende houvast.	Secretaris/Algemeen directeur	#Preventief #Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Fysieke_beveiliging	#Bescherming #Verdediging
7.5	Fysiek	1	Beschermen tegen fysieke en omgevingsdreigingen	Er behoort bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, te worden ontworpen en geïmplementeerd.	De gevolgen van gebeurtenissen die voortvloeien uit fysieke en omgevingsdreigingen, voorkomen of beperken.	11.1.4	11.1.4.1	7.05.1	1	De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.5	Fysiek	1	Beschermen tegen fysieke en omgevingsdreigingen	Er behoort bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, te worden ontworpen en geïmplementeerd.	De gevolgen van gebeurtenissen die voortvloeien uit fysieke en omgevingsdreigingen, voorkomen of beperken.	11.1.4	11.1.4.2	7.05.2	1	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.6	Fysiek	2	Werken in beveiligde zones	Voor het werken in beveiligde zones behoren beveiligingsmaatregelen te worden ontwikkeld en geïmplementeerd.	Informatie en andere gerelateerde bedrijfsmiddelen in beveiligde zones beschermen tegen schade en onbevoegde verstoring door personeel dat in deze zones aan het werk is.	11.1.5	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.7	Fysiek	1	'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 te worden afgedwongen.	De risico's op onbevoegde toegang tot, verlies van en schade aan informatie op bureaus, schermen en op andere toegankelijke plaatsen tijdens en buiten de gebruikelijke werkuren beperken.	11.2.9	11.2.9.1	7.07.1	2	Een onbemenste werkplek is altijd vergrendeld.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.7	Fysiek	1	'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 te worden afgedwongen.	De risico's op onbevoegde toegang tot, verlies van en schade aan informatie op bureaus, schermen en op andere toegankelijke plaatsen tijdens en buiten de gebruikelijke werkuren beperken.	11.2.9	11.2.9.2	7.07.2	2	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.7	Fysiek	1	'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 te worden afgedwongen.	De risico's op onbevoegde toegang tot, verlies van en schade aan informatie op bureaus, schermen en op andere toegankelijke plaatsen tijdens en buiten de gebruikelijke werkuren beperken.	11.2.9	11.2.9.3	7.07.3	2	Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.7	Fysiek	1	'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 te worden afgedwongen.	De risico's op onbevoegde toegang tot, verlies van en schade aan informatie op bureaus, schermen en op andere toegankelijke plaatsen tijdens en buiten de gebruikelijke werkuren beperken.	11.2.9	11.2.9.4	7.07.4	2	Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.7	Fysiek	1	'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 te worden afgedwongen.	De risico's op onbevoegde toegang tot, verlies van en schade aan informatie op bureaus, schermen en op andere toegankelijke plaatsen tijdens en buiten de gebruikelijke werkuren beperken.	11.2.9	11.2.9.5	7.07.5	2	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingsvergrendeling automatisch geactiveerd.	Secretaris/Algemeen directeur Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.8	Fysiek	1	Plaatsen en beschermen van apparatuur	Apparatuur behoort veilig te worden geplaatst en beschermd.	De risico's op fysieke en omgevingsdreigingen en op toegang door onbevoegden en schade beperken.	11.2.1	/	/	/	/	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming

7.9	Fysiek	1	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein behoren te worden beschermd.	Verlies, schade, diefstal of compromittering van bedrijfsmiddelen buiten het gebouw en/of terrein en onderbreking van de bedrijfsvoering van de organisatie voorkomen.	11.2.6	/	/	/	/	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming
7.10	Fysiek	2	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.	Uitsluitend geoorloofde openbaarmaking, wijziging, verwijdering of vernietiging van informatie op opslagmedia bewerkstelligen.	08.3.1	08.3.1.1	7.10.1	2	Er is een verwijderinstructie waarin is opgenomen dat van verwijderbare media die herbruikbaar zijn en die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd is.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming
7.10	Fysiek	2	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.	Uitsluitend geoorloofde openbaarmaking, wijziging, verwijdering of vernietiging van informatie op opslagmedia bewerkstelligen.	08.3.2	08.3.2.1	7.10.2	2	Media die vertrouwelijke informatie bevatten, zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming
7.10	Fysiek	2	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.	Uitsluitend geoorloofde openbaarmaking, wijziging, verwijdering of vernietiging van informatie op opslagmedia bewerkstelligen.	08.3.3	08.3.3.1	7.10.3	2	Er is een vastgestelde procedure voor het fysiek transport van media.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming
7.10	Fysiek	2	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.	Uitsluitend geoorloofde openbaarmaking, wijziging, verwijdering of vernietiging van informatie op opslagmedia bewerkstelligen.	08.3.3	08.3.3.2	7.10.4	2	Het gebruik van koeriers of transporteurs voor transport van op BBN2 of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming
7.10	Fysiek	2	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.	Uitsluitend geoorloofde openbaarmaking, wijziging, verwijdering of vernietiging van informatie op opslagmedia bewerkstelligen.	08.3.2	08.3.2.2	7.10.5	2	Verwijdering vindt plaats op een veilige manier, bijvoorbeeld door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming
7.10	Fysiek	2	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.	Uitsluitend geoorloofde openbaarmaking, wijziging, verwijdering of vernietiging van informatie op opslagmedia bewerkstelligen.	08.3.2	08.3.2.3	7.10.6	2	Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is en er wordt verslag van gemaakt.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming
7.10	Fysiek	2	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.	Uitsluitend geoorloofde openbaarmaking, wijziging, verwijdering of vernietiging van informatie op opslagmedia bewerkstelligen.	11.2.5	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming
7.11	Fysiek	1	Nutsvoorzieningen	Informatieverwerkende faciliteiten behoren te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Verlies, schade of compromittering van informatie en andere gerelateerde bedrijfsmiddelen of onderbreking van de bedrijfsvoering van de organisatie vanwege verstoring en ontregeling van ondersteunende nutsvoorzieningen voorkomen.	11.2.2	/	/	/	/	Dienstenleverancier	#Preventief #Detectief	#Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Fysieke_beveiliging	#Bescherming
7.12	Fysiek	1	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen onderschepping, interferentie of beschadiging.	Verlies, schade, diefstal of compromittering van informatie en andere gerelateerde bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie in verband met voedings- en communicatiekabels voorkomen.	11.2.3	/	/	/	/	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging	#Bescherming
7.13	Fysiek	1	Onderhoud van apparatuur	Apparatuur behoort op de juiste wijze te worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	Verlies, schade, diefstal of compromittering van informatie en andere gerelateerde bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie door gebrekkig onderhoud voorkomen.	11.2.4	/	/	/	/	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming #Veerkracht
7.14	Fysiek	1	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.	Het lekken van informatie via af te voeren of te hergebruiken apparatuur voorkomen.	11.2.7	/	7.14.1	2	Zie overheidsmaatregelen van 7.10 (7.10.2, 7.10.5 en 7.10.6).	Dienstenleverancier	#Preventief	#Vertrouwelijkheid	#Beschermen	#Fysieke_beveiliging #Beheer_van_bedrijfsmiddelen	#Bescherming
8.1	Technologisch	1	'User endpoint devices'	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' behoort te worden beschermd.	Informatie beschermen tegen de risico's als gevolg van het gebruik van 'user endpoint devices'.	06.2.1	06.2.1.1	8.01.1	2	Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Bescherming
8.1	Technologisch	1	'User endpoint devices'	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' behoort te worden beschermd.	Informatie beschermen tegen de risico's als gevolg van het gebruik van 'user endpoint devices'.	06.2.1	06.2.1.2	8.01.2	2	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: (a) In bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde. (b) Het apparaat maakt deel uit van patchmanagement en hardening. (c) Er wordt gebruik gemaakt van Mobile Device Management (MDM) of van Mobile Application Management (MAM)-oplossingen. (d) Gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt. (e) Periodiek wordt getoetst of de punten in lid a), b) en c) worden nageleefd.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Bescherming
8.1	Technologisch	1	'User endpoint devices'	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' behoort te worden beschermd.	Informatie beschermen tegen de risico's als gevolg van het gebruik van 'user endpoint devices'.	11.2.8	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Beheer_van_bedrijfsmiddelen #Informatiebescherming	#Bescherming
8.2	Technologisch	1	Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten behoren te worden beperkt en beheerd.	Bewerkstelligen dat alleen bevoegde gebruikers, softwarecomponenten en diensten speciale toegangsrechten krijgen.	09.2.3	09.2.3.1	8.02.1	2	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
8.3	Technologisch	1	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen behoren te worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	Uitsluitend bevoegde toegang bewerkstelligen en onbevoegde toegang tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen.	09.4.1	09.4.1.1	8.03.1	2	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
8.3	Technologisch	1	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen behoren te worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	Uitsluitend bevoegde toegang bewerkstelligen en onbevoegde toegang tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen.	09.4.1	09.4.1.2	8.03.2	2	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
8.4	Technologisch	1	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken behoren op passende wijze te worden beheerd.	Voorkomen dat er ongeoorloofde functionaliteit wordt geïntroduceerd, vermijden dat onbedoelde of kwaadwillige wijzigingen plaatsvinden en de vertrouwelijkheid behouden van waardevol intellectueel eigendom.	09.4.5	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer #Toepassingsbeveiliging #Veilige_configuratie	#Bescherming

8.5	Technologisch	1	Beveiligde authenticatie	Er behoren beveiligde authenticatietechnologieën en -procedures te worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.	Bewerkstelligen dat een gebruiker of een entiteit veilig wordt geauthentiseerde wanneer toegang tot systemen, toepassingen en diensten wordt verleend.	09.4.2	09.4.2.1	8.05.1	1	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal tweefactor-authenticatie.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
8.5	Technologisch	1	Beveiligde authenticatie	Er behoren beveiligde authenticatietechnologieën en -procedures te worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.	Bewerkstelligen dat een gebruiker of een entiteit veilig wordt geauthenticeerd wanneer toegang tot systemen, toepassingen en diensten wordt verleend.	09.4.2	09.4.2.2	8.05.2	2	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Identiteits-_en_toegangsbeheer	#Bescherming
8.6	Technologisch	1	Capaciteitsbeheer	Het gebruik van middelen behoort te worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	De vereiste capaciteit van informatieverwerkende faciliteiten, personeel, kantoren en andere faciliteiten waarborgen.	12.1.3	/	/	/	/	Dienstenleverancier	#Preventief #Detectief	#Integriteit #Beschikbaarheid	#Identificeren #Beschermen #Detecteren	#Continuïteit	#Governance_en_Ecosysteem #Bescherming
8.7	Technologisch	1	Bescherming tegen malware	Bescherming tegen malware behoort te worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen beschermd zijn tegen malware.	12.2.1	12.2.1.1	8.07.1	1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	Secretaris/Algemeen directeur Dienstenleverancier	#Preventief #Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Systeem-_en_netwerkbeveiliging #Informatiebescherming	#Bescherming #Verdediging
8.7	Technologisch	1	Bescherming tegen malware	Bescherming tegen malware behoort te worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen beschermd zijn tegen malware.	12.2.1	12.2.1.2	8.07.2	1	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.	Secretaris/Algemeen directeur Dienstenleverancier	#Preventief #Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Systeem-_en_netwerkbeveiliging #Informatiebescherming	#Bescherming #Verdediging
8.7	Technologisch	1	Bescherming tegen malware	Bescherming tegen malware behoort te worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen beschermd zijn tegen malware.	12.2.1	12.2.1.3	8.07.3	1	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	Secretaris/Algemeen directeur Dienstenleverancier	#Preventief #Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Systeem-_en_netwerkbeveiliging #Informatiebescherming	#Bescherming #Verdediging
8.7	Technologisch	1	Bescherming tegen malware	Bescherming tegen malware behoort te worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen beschermd zijn tegen malware.	12.2.1	12.2.1.4 12.2.1.5	8.07.4	1	De malwarescan wordt uitgevoerd op: (a) alle omgevingen, bijvoorbeeld op mailservers, (desktop)computers en bij de toegangsverlening tot het netwerk van de organisatie; (b) alle gedownloade content voorafgaand aan executie of opslag; (c) alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik of opslag in de eigen omgeving.	Secretaris/Algemeen directeur Dienstenleverancier	#Preventief #Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Systeem-_en_netwerkbeveiliging #Informatiebescherming	#Bescherming #Verdediging
8.8	Technologisch	1	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.	Misbruik van technische kwetsbaarheden voorkomen.	12.6.1	12.6.1.1	8.08.1	1	Als de kans op misbruik en de verwachte schade beide hoog zijn (bijvoorbeeld met de NCSC-Inschalingsmatrix beveiligingsadviezen of leveranciersbeveiligingsadviezen), worden passende mitigerende maatregelen zo snel mogelijk, maar uiterlijk binnen een week getroffen.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Beheer_van_bedreigingen_en_kwetsbaarheden	#Governance_en_Ecosysteem #Bescherming #Verdediging
8.8	Technologisch	1	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.	Misbruik van technische kwetsbaarheden voorkomen.	12.6.1	/	8.08.2	1	Op basis van een expliciete risicoafweging wordt bepaald op welke wijze mitigerende maatregelen getroffen worden.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Beheer_van_bedreigingen_en_kwetsbaarheden	#Governance_en_Ecosysteem #Bescherming #Verdediging
8.8	Technologisch	1	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.	Misbruik van technische kwetsbaarheden voorkomen.	12.6.1	/	8.08.3	1	In de tussentijd of als installatie binnen een week niet mogelijk is, worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Beheer_van_bedreigingen_en_kwetsbaarheden	#Governance_en_Ecosysteem #Bescherming #Verdediging
8.8	Technologisch	1	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.	Misbruik van technische kwetsbaarheden voorkomen.	18.2.3	18.2.3.1	8.08.4	1	Informatiesystemen worden bij voorkeur jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses, penetratietesten of red-teamingstesten.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Beheer_van_bedreigingen_en_kwetsbaarheden	#Governance_en_Ecosysteem #Bescherming #Verdediging
8.8	Technologisch	1	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.	Misbruik van technische kwetsbaarheden voorkomen.	18.2.3	/	8.08.5	2	Internetfacing-systemen hebben een verplichte (bij voorkeur geautomatiseerde) penetratietest bij iedere nieuwe release of major update. Als daar bevindingen met een hoog risico uitkomen, mag het systeem niet in productie.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen	#Beheer_van_bedreigingen_en_kwetsbaarheden	#Governance_en_Ecosysteem #Bescherming #Verdediging
8.9	Technologisch	1	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken behoren te worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Garanderen dat hardware, software, diensten en netwerken correct met de vereiste beveiligingsinstellingen functioneren en de configuratie niet door ongeautoriseerde of onjuiste wijzigingen wordt gewijzigd.	/	/	/	/	Dit is een nieuwe control. Er zijn geen overheidsmaatregelen nodig. De richtlijnen uit de NEN-EN-ISO/IEC 27002:2022 geven voldoende houvast.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie	#Bescherming
8.10	Technologisch	1	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie behoort te worden gewist als deze niet langer vereist is.	Onnodige openbaarmaking van gevoelige informatie voorkomen en aan de eisen van wet- en regelgeving, statutaire en contractuele eisen voor het wissen van informatie voldoen.	/	/	/	/	Dit is een nieuwe control. Er zijn geen overheidsmaatregelen nodig. De richtlijnen uit de NEN-EN-ISO/IEC 27002:2022 geven voldoende houvast.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid	#Beschermen	#Informatiebescherming #Juridisch_en_compliance	#Bescherming
8.11	Technologisch	2	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.	De openbaarmaking van gevoelige informatie met inbegrip van persoonsgegevens beperken en aan de eisen van wet- en regelgeving, statutaire en contractuele eisen voldoen.	/	/	/	/	Dit is een nieuwe control. Er zijn geen overheidsmaatregelen nodig. De richtlijnen uit de NEN-EN-ISO/IEC 27002:2022 geven voldoende houvast.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid	#Beschermen	#Informatiebescherming	#Bescherming
8.12	Technologisch	2	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 verzonden.	Om de ongeoorloofde openbaarmaking en extractie van informatie door personen of systemen te detecteren en te voorkomen.	/	/	/	/	Dit is een nieuwe control. Er zijn geen overheidsmaatregelen nodig. De richtlijnen uit de NEN-EN-ISO/IEC 27002:2022 geven voldoende houvast.	Proceseigenaar Dienstenleverancier	#Preventief #Detectief	#Vertrouwelijkheid	#Beschermen #Detecteren	#Informatiebescherming	#Bescherming #Verdediging
8.13	Technologisch	1	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.	Herstel mogelijk maken na verlies van gegevens of systemen.	12.3.1	12.3.1.1	8.13.1	1	Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld. Er moet speciale aandacht zijn voor het beschermen van de back-up tegen ransomware-aanvallen.	Proceseigenaar Dienstenleverancier	#Corrigerend	#Integriteit #Beschikbaarheid	#Herstellen	#Continuïteit	#Bescherming
8.13	Technologisch	1	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.	Herstel mogelijk maken na verlies van gegevens of systemen.	12.3.1	12.3.1.2	8.13.2	1	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	Proceseigenaar Dienstenleverancier	#Corrigerend	#Integriteit #Beschikbaarheid	#Herstellen	#Continuïteit	#Bescherming
8.13	Technologisch	1	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.	Herstel mogelijk maken na verlies van gegevens of systemen.	12.3.1	12.3.1.3	8.13.3	1	In het back-upbeleid staan minimaal de volgende eisen: (a) Dataverlies bedraagt maximaal 28 uur. (b) Hersteltijd in geval van incidenten is maximaal 16 werkuren (2 dagen van 8 uur) in 85% van de gevallen.	Proceseigenaar Dienstenleverancier	#Corrigerend	#Integriteit #Beschikbaarheid	#Herstellen	#Continuïteit	#Bescherming
8.13	Technologisch	1	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.	Herstel mogelijk maken na verlies van gegevens of systemen.	12.3.1	12.3.1.4	8.13.4	2	Het back-upproces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	Proceseigenaar Dienstenleverancier	#Corrigerend	#Integriteit #Beschikbaarheid	#Herstellen	#Continuïteit	#Bescherming
8.13	Technologisch	1	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.	Herstel mogelijk maken na verlies van gegevens of systemen.	12.3.1	/	8.13.5	2	Zorg dat ten minste één back-up niet online benaderbaar is en beschermd wordt tegen veranderingen.	Proceseigenaar Dienstenleverancier	#Corrigerend	#Integriteit #Beschikbaarheid	#Herstellen	#Continuïteit	#Bescherming

8.13	Technologisch	1	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.	Herstel mogelijk maken na verlies van gegevens of systemen.	12.3.1	12.3.1.5	8.13.6	2	De herstelprocedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.	Proceseigenaar Dienstenleverancier	#Corrigerend	#Integriteit #Beschikbaarheid	#Herstellen	#Continuïteit	#Bescherming
8.14	Technologisch	1	Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	De ononderbroken werking van informatieverwerkende faciliteiten waarborgen.	17.2.1	/	/	/	/	Dienstenleverancier	#Preventief	#Beschikbaarheid	#Beschermen	#Continuïteit #Beheer_van_bedrijfsmiddelen	#Bescherming #Veerkracht
8.15	Technologisch	1	Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Gebeurtenissen registreren, bewijs genereren, de integriteit van informatie in logbestanden waarborgen, onbevoegde toegang voorkomen, informatiebeveiligingsgebeurtenissen identificeren die tot een informatiebeveiligingsincident kunnen	12.4.1	12.4.1.1	8.15.1	1	Een logregel bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis.	Proceseigenaar Dienstenleverancier	#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Bescherming #Verdediging
8.15	Technologisch	1	Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Gebeurtenissen registreren, bewijs genereren, de integriteit van informatie in logbestanden waarborgen, onbevoegde toegang voorkomen, informatiebeveiligingsgebeurtenissen identificeren die tot een informatiebeveiligingsincident kunnen	12.4.1	12.4.1.2	8.15.2	1	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	Proceseigenaar Dienstenleverancier	#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Bescherming #Verdediging
8.15	Technologisch	1	Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Gebeurtenissen registreren, bewijs genereren, de integriteit van informatie in logbestanden waarborgen, onbevoegde toegang voorkomen, informatiebeveiligingsgebeurtenissen identificeren die tot een informatiebeveiligingsincident kunnen	12.4.2	12.4.2.1	8.15.3	1	Er is een overzicht van logbestanden die worden gegenereerd.	Proceseigenaar Dienstenleverancier	#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Bescherming #Verdediging
8.15	Technologisch	1	Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Gebeurtenissen registreren, bewijs genereren, de integriteit van informatie in logbestanden waarborgen, onbevoegde toegang voorkomen, informatiebeveiligingsgebeurtenissen identificeren die tot een informatiebeveiligingsincident kunnen	12.4.2	12.4.2.2	8.15.4	1	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	Proceseigenaar Dienstenleverancier	#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Bescherming #Verdediging
8.15	Technologisch	1	Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Gebeurtenissen registreren, bewijs genereren, de integriteit van informatie in logbestanden waarborgen, onbevoegde toegang voorkomen, informatiebeveiligingsgebeurtenissen identificeren die tot een informatiebeveiligingsincident kunnen	12.4.2	12.4.2.4	8.15.5	2	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform control 5.24.	Proceseigenaar Dienstenleverancier	#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Bescherming #Verdediging
8.15	Technologisch	1	Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Gebeurtenissen registreren, bewijs genereren, de integriteit van informatie in logbestanden waarborgen, onbevoegde toegang voorkomen, informatiebeveiligingsgebeurtenissen identificeren die tot een informatiebeveiligingsincident kunnen	12.4.2	12.4.2.3	8.15.6	2	Minimaal halfjaarlijks wordt door een onafhankelijke functionaris (ten opzichte van de uitvoering) getoetst op het ongewijzigd bestaan van logbestanden gedurende de bewaartermijn.	Proceseigenaar Dienstenleverancier	#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Bescherming #Verdediging
8.15	Technologisch	1	Logging	Er behoren logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Gebeurtenissen registreren, bewijs genereren, de integriteit van informatie in logbestanden waarborgen, onbevoegde toegang voorkomen, informatiebeveiligingsgebeurtenissen identificeren die tot een informatiebeveiligingsincident kunnen	12.4.3	/	/	/	/	Proceseigenaar Dienstenleverancier	#Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Bescherming #Verdediging
8.16	Technologisch	1	Monitoren van activiteiten	Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Afwijkend gedrag en potentiële informatiebeveiligingsincidenten detecteren.	12.4.1	12.4.1.3	8.16.1	2	De informatieverwerkende omgeving wordt gemonitord met een detectie- en response-oplossing, waarmee aanvallen kunnen worden gedetecteerd en afwijkingen worden adequaat en tijdig behandeld.	Proceseigenaar Dienstenleverancier	#Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren #Reageren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
8.16	Technologisch	1	Monitoren van activiteiten	Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Afwijkend gedrag en potentiële informatiebeveiligingsincidenten detecteren.	12.4.1	/	8.16.2	2	Actieve netwerkcomponenten zijn voorzien van logging en monitoring van die logging om afwijkende gebeurtenissen te kunnen waarnemen en daarop te reageren.	Proceseigenaar Dienstenleverancier	#Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren #Reageren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
8.16	Technologisch	1	Monitoren van activiteiten	Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Afwijkend gedrag en potentiële informatiebeveiligingsincidenten detecteren.	12.4.1	/	8.16.3	2	Een risicoafweging bepaalt de bewaartermijn van de logging.	Proceseigenaar Dienstenleverancier	#Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren #Reageren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
8.16	Technologisch	1	Monitoren van activiteiten	Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Afwijkend gedrag en potentiële informatiebeveiligingsincidenten detecteren.	12.4.1	12.4.1.4	8.16.4	2	Bij ontdekte nieuwe dreigingen (aanvallen) via 8.16.1 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	Proceseigenaar Dienstenleverancier	#Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren #Reageren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
8.16	Technologisch	1	Monitoren van activiteiten	Netwerken, systemen en toepassingen behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Afwijkend gedrag en potentiële informatiebeveiligingsincidenten detecteren.	12.4.1	12.4.1.5	8.16.5	2	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Proceseigenaar Dienstenleverancier	#Detectief #Corrigerend	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Detecteren #Reageren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Verdediging
8.17	Technologisch	1	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, behoren te worden gesynchroniseerd met goedgekeurde tijdsbronnen.	De correlatie en analyse van beveiligingsgerelateerde gebeurtenissen en andere geregistreerde gegevens mogelijk maken en onderzoeken bij informatiebeveiligingsincidenten ondersteunen.	12.4.4	/	/	/	/	Dienstenleverancier	#Detectief	#Integriteit	#Beschermen #Detecteren	#Beheer_van_informatiebeveiligingsgebeurtenissen	#Bescherming #Verdediging
8.18	Technologisch	1	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.	Bewerkstelligen dat het gebruik van systeemhulpmiddelen geen schade toebrengt aan systeem- en toepassingsbeheersmaatregelen voor informatiebeveiliging.	09.4.4	09.4.4.1	8.18.1	1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem-_en_netwerkbeveiliging #Veilige_configuratie #Toepassingsbeveiliging	#Bescherming
8.18	Technologisch	1	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.	Bewerkstelligen dat het gebruik van systeemhulpmiddelen geen schade toebrengt aan systeem- en toepassingsbeheersmaatregelen voor informatiebeveiliging.	09.4.4	09.4.4.2	8.18.2	2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem-_en_netwerkbeveiliging #Veilige_configuratie #Toepassingsbeveiliging	#Bescherming
8.19	Technologisch	1	Installeren van software op operationele systemen	Er behoren procedures en maatregelen te worden geïmplementeerd om het installeren van software op operationele systemen op beveiligde wijze te beheren.	De integriteit van operationele systemen garanderen en voorkomen dat misbruik wordt gemaakt van technische kwetsbaarheden.	12.6.2	12.6.2.1	8.19.1	2	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan wat via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie #Toepassingsbeveiliging	#Bescherming
8.19	Technologisch	1	Installeren van software op operationele systemen	Er behoren procedures en maatregelen te worden geïmplementeerd om het installeren van software op operationele systemen op beveiligde wijze te beheren.	De integriteit van operationele systemen garanderen en voorkomen dat misbruik wordt gemaakt van technische kwetsbaarheden.	12.5.1	/	/	/	/	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie #Toepassingsbeveiliging	#Bescherming

8.20	Technologisch	1	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten behoren te worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten beschermen tegen compromittering via het netwerk.	13.1.1	/	/	/	/	Dienstenleverancier	#Preventief #Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen #Detecteren	#Systeem-_en_netwerkbeveiliging	#Bescherming
8.21	Technologisch	1	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten behoren te worden geïdentificeerd, geïmplementeerd en	De beveiliging bij het gebruik van netwerkdiensten garanderen.	13.1.2	13.1.2.4	8.21.1	1	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en hierop te reageren.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem-_en_netwerkbeveiliging	#Bescherming
8.21	Technologisch	1	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten behoren te worden geïdentificeerd, geïmplementeerd en gemonitord.	De beveiliging bij het gebruik van netwerkdiensten garanderen.	13.1.2	13.1.2.1	8.21.2	2	Het dataverkeer dat de organisatie binnenkomt of uitgaat, wordt bewaakt/geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risicoafweging, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem-_en_netwerkbeveiliging	#Bescherming
8.21	Technologisch	1	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten behoren te worden geïdentificeerd, geïmplementeerd en	De beveiliging bij het gebruik van netwerkdiensten garanderen.	13.1.2	13.1.2.2	8.21.3	2	Bij ontdekte nieuwe dreigingen vanuit 8.21.2 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem-_en_netwerkbeveiliging	#Bescherming
8.21	Technologisch	1	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten behoren te worden geïdentificeerd, geïmplementeerd en	De beveiliging bij het gebruik van netwerkdiensten garanderen.	13.1.2	13.1.2.3	8.21.4	2	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het Nationaal Bureau voor Verbindingsbeveiliging (NBV) een positief inzetadvies heeft afgegeven.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem-_en_netwerkbeveiliging	#Bescherming
8.22	Technologisch	1	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen behoren in de netwerken van de organisatie te worden gesegmenteerd.	Het netwerk opsplitsen met beveiligingsgrenzen en het verkeer ertussen op basis van de bedrijfsbehoeften beheersen.	13.1.3	13.1.3.1	8.22.1	2	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem-_en_netwerkbeveiliging	#Bescherming
8.23	Technologisch	1	Toepassen van webfilters	De toegang tot externe websites behoort te worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Systemen beschermen om te voorkomen dat ze door malware worden gecompromitteerd en om toegang tot ongeoorloofde internetbronnen te voorkomen.	/	/	/	/	Dit is een nieuwe control. Er zijn geen overheidsmaatregelen nodig. De richtlijnen uit de NEN-EN-ISO/IEC 27002:2022 geven voldoende houvast.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem-_en_netwerkbeveiliging	#Bescherming
8.24	Technologisch	2	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.	Correct en doeltreffend gebruik bewerkstelligen van cryptografie om de vertrouwelijkheid, authenticiteit of integriteit van informatie overeenkomstig de bedrijfs- en informatiebeveiligingseisen te beschermen en met inachtneming van de eisen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot cryptografie.	10.1.1	10.1.1.1	8.24.1	2	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum Standaardisatie worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie	#Bescherming
8.24	Technologisch	2	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.	Correct en doeltreffend gebruik bewerkstelligen van cryptografie om de vertrouwelijkheid, authenticiteit of integriteit van informatie overeenkomstig de bedrijfs- en informatiebeveiligingseisen te beschermen en met inachtneming van de eisen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot cryptografie.	10.1.1	10.1.1.2	8.24.2	2	Cryptografische toepassingen voldoen aan passende standaarden van het Forum Standaardisatie.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie	#Bescherming
8.24	Technologisch	2	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.	Correct en doeltreffend gebruik bewerkstelligen van cryptografie om de vertrouwelijkheid, authenticiteit of integriteit van informatie overeenkomstig de bedrijfs- en informatiebeveiligingseisen te beschermen en met inachtneming van de eisen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot cryptografie.	/	/	8.24.3	2	De sterkte van de cryptografie wordt waar mogelijk gebaseerd op de actuele adviezen van het NCSC.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie	#Bescherming
8.24	Technologisch	2	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.	Correct en doeltreffend gebruik bewerkstelligen van cryptografie om de vertrouwelijkheid, authenticiteit of integriteit van informatie overeenkomstig de bedrijfs- en informatiebeveiligingseisen te beschermen en met inachtneming van de eisen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot cryptografie.	10.1.2	10.1.2.1	8.24.4	2	In geval van PKIoverheid-certificaten hanteer de PKIoverheid-eisen ten aanzien van het sleutelbeheer. In overige situaties hanteer de norm ISO 11770-1 voor het beheer van cryptografische sleutels.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie	#Bescherming
8.24	Technologisch	2	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, behoren te worden gedefinieerd en geïmplementeerd.	Correct en doeltreffend gebruik bewerkstelligen van cryptografie om de vertrouwelijkheid, authenticiteit of integriteit van informatie overeenkomstig de bedrijfs- en informatiebeveiligingseisen te beschermen en met inachtneming van de eisen van wet- en regelgeving, statutaire en contractuele eisen met betrekking tot cryptografie.	10.1.2	10.1.2.2	8.24.5	2	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Veilige_configuratie	#Bescherming
8.25	Technologisch	1	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen behoren regels te worden vastgesteld en toegepast.	Bewerkstelligen dat informatiebeveiliging binnen de veilige ontwikkelcyclus van software en systemen wordt ontworpen en geïmplementeerd.	14.2.1	14.2.1.1	8.25.1	1	De gangbare principes rondom 'security by design' zijn uitgangspunt voor de ontwikkeling van software en systemen.	Secretaris/Algemeen directeur Proceseigenaar	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
8.26	Technologisch	1	Toepassingsbeveiligingseisen	Er behoren eisen aan de informatiebeveiliging te worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Garanderen dat alle informatiebeveiligingseisen zijn geïdentificeerd en meegenomen bij het ontwikkelen of aanschaffen van toepassingen.	14.1.2 14.1.3	/	8.26.1	2	Zie overheidsmaatregel 5.14.3.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming #Verdediging
8.27	Technologisch	1	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.	Waarborgen dat informatiesystemen veilig worden ontworpen, geïmplementeerd en beheerd binnen de ontwikkelingslevenscyclus.	14.2.5	14.2.5.1	8.27.1	1	Zie overheidsmaatregel 8.25.1.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
8.28	Technologisch	1	Veilig coderen	Er behoren principes voor veilig coderen te worden toegepast op softwareontwikkeling.	Waarborgen dat veilige software wordt geschreven waardoor het aantal potentiële informatiebeveiligingskwetsbaarheden in de software wordt beperkt.	/	/	/	/	Dit is een nieuwe control. Er zijn geen overheidsmaatregelen nodig. De richtlijnen uit de NEN-EN-ISO/IEC 27002:2022 geven voldoende houvast.	Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
8.29	Technologisch	1	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging behoren te worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Valideren of aan de informatiebeveiligingseisen wordt voldaan wanneer toepassingen of code in de productieomgeving worden uitgerold.	14.2.9	14.2.9.1	8.29.1	1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Toepassingsbeveiliging #Borging_van_informatiebeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
8.29	Technologisch	1	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging behoren te worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Valideren of aan de informatiebeveiligingseisen wordt voldaan wanneer toepassingen of code in de productieomgeving worden uitgerold.	14.2.9	14.2.9.2	8.29.2	1	Van de resultaten van de testen wordt verslag gemaakt.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Toepassingsbeveiliging #Borging_van_informatiebeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
8.29	Technologisch	1	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging behoren te worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Valideren of aan de informatiebeveiligingseisen wordt voldaan wanneer toepassingen of code in de productieomgeving worden uitgerold.	14.2.8	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren	#Toepassingsbeveiliging #Borging_van_informatiebeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming

8.30	Technologisch	1	Uitbestede systeemontwikkeling	De organisatie behoort de activiteiten in verband met uitbestede systeemontwikkeling te sturen, bewaken en beoordelen.	Garanderen dat de door de organisatie vereiste informatiebeveiligingsmaatregelen bij uitbestede systeemontwikkeling worden geïmplementeerd.	14.2.7	14.2.7.1	8.30.1	1	Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen, worden aan de leverancier opgelegd.	Proceseigenaar	#Preventief #Detectief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Identificeren #Beschermen #Detecteren	#Systeem-_en_netwerkbeveiliging #Toepassingsbeveiliging #Beveiliging_in_leveranciersrelaties	#Governance_en_Ecosysteem #Bescherming
8.31	Technologisch	1	Scheiden van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden en beveiligd.	De productieomgeving en de gegevens beschermen tegen compromittering door ontwikkel- en testactiviteiten	14.2.6	14.2.6.1	8.31.1	1	Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
8.31	Technologisch	1	Scheiden van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden en beveiligd.	De productieomgeving en de gegevens beschermen tegen compromittering door ontwikkel- en testactiviteiten.	12.1.4	12.1.4.1	8.31.2	2	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
8.31	Technologisch	1	Scheiden van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden en beveiligd.	De productieomgeving en de gegevens beschermen tegen compromittering door ontwikkel- en testactiviteiten.	12.1.4	12.1.4.2	8.31.3	2	Wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
8.32	Technologisch	2	Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer.	De informatiebeveiliging behouden tijdens het uitvoeren van wijzigingen.	12.1.2	12.1.2.1	8.32.1	1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: (a) het administreren van wijzigingen; (b) risicoafweging van mogelijke gevolgen van de wijzigingen; (c) goedkeuringsprocedure voor wijzigingen	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
8.32	Technologisch	2	Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer.	De informatiebeveiliging behouden tijdens het uitvoeren van wijzigingen.	14.2.2	14.2.2.1	8.32.2	1	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerraamwerk.	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
8.32	Technologisch	2	Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer.	De informatiebeveiliging behouden tijdens het uitvoeren van wijzigingen.	14.2.3	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
8.32	Technologisch	-	Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen behoren onderworpen te zijn aan procedures voor wijzigingsbeheer.	De informatiebeveiliging behouden tijdens het uitvoeren van wijzigingen.	14.2.4	/	/	/	/	-	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Toepassingsbeveiliging #Systeem-_en_netwerkbeveiliging	#Bescherming
8.33	Technologisch	2	Testgegevens	Testgegevens behoren op passende wijze te worden geselecteerd, beschermd en beheerd.	De relevantie van het testen en de bescherming van operationele gegevens die voor het testen worden gebruikt, waarborgen	14.3.1	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit	#Beschermen	#Informatiebescherming	#Bescherming
8.34	Technologisch	1	Bescherming van informatiesystemen tijdens audits	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, behoren te worden gepland en overeengekomen tussen de tester en het verantwoordelijke management	De impact van audittests en andere auditactiviteiten op operationele systemen en bedrijfsprocessen tot een minimum beperken.	12.7.1	/	/	/	/	Proceseigenaar Dienstenleverancier	#Preventief	#Vertrouwelijkheid #Integriteit #Beschikbaarheid	#Beschermen	#Systeem-_en_netwerkbeveiliging #Informatiebescherming	#Governance_en_Ecosysteem #Bescherming