

BIJLAGE 14 EXPORT ICO WIZARD

Nr	Naam Eis	Referentie brondoc ument:	Referentie code norm:	BIO-O- maatreg el:	Samenvatting eis:	Gebaseerd op: (ISO27002- paragraaf, of ander framework)	Verificatie methode(n):
37	Inrichting van verantwoordelijkheden bij informatiebeveiliging	BIO 2019	Ketenpartnereis 7	Ja	Op de inrichting van verantwoordelijkheden bij informatiebeveiliging is paragraaf 6.1. van de BIO 2019 van toepassing	Direct op BIO 2019 gebaseerd	Overleg bewijsstukken en/of verklaring
43	O-maatregel. Contact met overheidsinstanties	BIO 2019	6.1.3.1	Ja	Er is door de organisatie 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.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
44	O-maatregel. Contact met overheidsinstanties	BIO 2019	6.1.3.2	Ja	Het contactoverzicht wordt jaarlijks geactualiseerd.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
45	Sturen op veilig personeel	BIO 2019	Ketenpartnereis 8	Ja	Bij het sturen op veilig personeel is hoofdstuk 7 van de BIO 2019 van toepassing.	Direct op BIO 2019 gebaseerd	Overleg bewijsstukken en/of verklaring
53	O-maatregel. Speciale systeemhulpmiddelen gebruiken	BIO 2019	9.4.4.2	Ja	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoekhulpmiddelen.	Direct op BIO 2019 gebaseerd	Overleg bewijsstukken en/of Verklaring.
54	Goed opdrachtgeverschap	BIO 2019	Ketenpartnereis 9	Ja	Op het leveranciersmanagement zijn de Informatiebeveiligingsaspecten van hoofdstuk 15 van de BIO 2019 van toepassing.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
56	O-maatregel. Informatiebeveiligingsbeleid voor leveranciersrelaties	BIO 2019	15.1.1.2	Ja	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekking tot leverancierstoegang tot bedrijfsinformatie vastgesteld.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
57	O-maatregel. Informatiebeveiligingsbeleid voor leveranciersrelaties	BIO 2019	15.1.1.3	Ja	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
62	O-maatregel. Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	BIO 2019	15.1.2.5	Ja	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.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
63	O-maatregel. Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	BIO 2019	15.1.2.6	Ja	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.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.

64	O-maatregel. Toeleveringsketen van informatie- en communicatietechnologie	BIO 2019	15.1.3.1	Ja	Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
65	O-maatregel. Monitoring en beoordeling van dienstverlening van leveranciers	BIO 2019	15.2.1.1	Ja	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatieindicatoren, zoals in het contract opgenomen is.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
168	Privacybeleid	Privacy-supplement Algemeen	ALG P.01		De organisatie heeft privacybeleid en procedures ontwikkeld en vastgesteld, waarin de verantwoordelijkheid is vastgelegd op welke wijze persoonsgegevens worden verwerkt, invulling wordt gegeven aan de wettelijke beginselen en hoe in een cyclisch proces wordt vastgelegd op welke wijze transparant aan de wet- en regelgeving wordt voldaan en afwijkingen worden opgelost.	AVG: art. 5, 24, 40 en UAVG: art. 2, 4, 78 en 157, CIP De Privacy Baseline2020 : B.01	Overleg bewijsstukken en/of verklaring
169	Privacy-organisatie	Privacy-supplement Algemeen	ALG P.02		De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen, zijn door de organisatie vastgelegd en vastgesteld , inclusief die bij uitwisseling van persoonsgegevens tussen organisaties, zodat ook bij doorgifte van persoonsgegevens de privacybelangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, zijn gewaarborgd.	ISO 27701 2019: 6.3.1.1 CIP De Privacy Baseline 2020: B.02	Overleg bewijsstukken en/of verklaring
170	Privacy-bewustzijn	Privacy-supplement Algemeen	ALG P.03		De organisatie waarborgt dat eenieder die persoonsgegevens verwerkt of een verwerking voorbereidt zich bewust is van de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwt dit conform de verwachtingen als hoogste prioriteit om deze overtuiging toe te passen; deze betrokkenen hebben daarvoor de benodigde kennis en zijn op de hoogte van grote veranderingen in de verwachtingen.	AVG: art. 32, ISO 27701 2019: 6.12.1.2, Wpg: art 31	Overleg bewijsstukken en/of verklaring
172	Privacy in de levenscyclus	Privacy-supplement Algemeen	ALG P.05		Vooraf aan het ontwerp van een gegevensverwerking en bij een verandering wordt een inschatting gemaakt van de privacyrisico's en wordt bepaald welke passende maatregelen nodig zijn; hiervoor zijn de verantwoordelijkheden duidelijk en is een proces ingeregeld voor het kunnen aantonen van het passend zijn van deze maatregelen.	ISO 27002 2017: 7.2.3	Overleg bewijsstukken en/of verklaring

173	Register van verwerkingsactiviteiten	Privacy-supplement Algemeen	ALG P.06		De verwerkingsverantwoordelijke(n) en de verwerker(s) hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens en dat voldoet aan de vereisten van de AVG.	AVG: art. 30, Wpg: art 31d lid 1 en 2	Overleg bewijsstukken en/of verklaring
312	Informatieverstrekking aan betrokkene met mobile apps	Privacy-supplement SSD Mobile	SSDm P.03		Om de gegevens te mogen verwerken wordt de betrokkene, waarvan de persoonsgegevens worden verwerkt, geïnformeerd betreffende welke verwerking (van de persoonsgegevens) plaatsvindt en krijgt deze betrokkene een waarschuwing bij het verkrijgen van toegang tot bijzondere persoonsgegevens.	CIP De Privacy Baseline 2020: U.05, AVG: art. 14, AVG: overweging 60, Wpg: Art 24a lid 1 t/m 4, art 24b	Overleg bewijsstukken en/of verklaring en testen
315	Dataminimalisatie binnen mobile apps	Privacy-supplement SSD Mobile	SSDm P.06		De organisatie behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn.	AVG: art. 6 lid 1, Wpg art 3 lid 2 en 5, Art 4 lid 2, Art 8 lid 1, 2, 6, Art 9 lid 4, Art 14	Overleg bewijsstukken en/of verklaring
340	Verwervingsbeleid softwarepakketten	Thema Softwarepakketten	B.01	Ja	Voor het verwerven van software behoren regels te worden vastgesteld en op verwervingsactiviteiten binnen de organisatie te worden toegepast.	BIO 2019: 14.2.1.	Overleg bewijsstukken en/of Verklaring.
342	Informatiebeveiligingsbeleid voor leveranciersrelaties	Thema Softwarepakketten	B.02	Ja	Met de leverancier behoren de informatiebeveiligingseisen en een periodieke actualisering daarvan te worden overeengekomen.	BIO 2019: 15.1.1.	Overleg bewijsstukken en/of Verklaring.
346	Exit-strategie	Thema Softwarepakketten	B.03		In de overeenkomst tussen de klant en leverancier behoort een exit-strategie te zijn opgenomen, waarbij zowel een aantal bepalingen over exit zijn opgenomen, als een aantal condities die aanleiding kunnen geven tot een exit.	CIP-netwerk	Overleg bewijsstukken en/of Verklaring.
347	Bedrijfs- en beveiligingsfuncties	Thema Softwarepakketten	B.04		De noodzakelijke bedrijfs- en beveiligingsfuncties binnen het veranderingsgebied behoren te worden vastgesteld met organisatorische en technisch uitgangspunten.	CIP-netwerk	Overleg bewijsstukken en/of Verklaring.
348	Cryptografie	Thema Softwarepakketten Thema Communicatievoorzieningen Thema Toegangsbeveiliging	B.03 B.04 B.05	Ja	Ter bescherming van de communicatie en opslag van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	BIO 2019: 10.1.1. BIO2.0-opmaat: 8.24	Overleg bewijsstukken en/of Verklaring.

349	O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen	BIO 2019	10.1.1.1	Ja	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 worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	Direct op BIO 2019 gebaseerd	Overleg bewijsstukken en/of Verklaring.
350	O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen	BIO 2019	10.1.1.2	Ja	Cryptografische toepassingen voldoen aan passende standaarden.	Direct op BIO 2019 gebaseerd	Overleg bewijsstukken.
351	Beveiligingsarchitectuur	Thema Softwarepakketten	B.06		De klant behoort het architectuurlandschap in kaart te hebben gebracht waarin het softwarepakket geïntegreerd moet worden en beveiligingsprincipes te hebben ontwikkeld.	CIP-netwerk	Overleg bewijsstukken en/of Verklaring.
353	Beperkingen wijziging softwarepakket	Thema Softwarepakketten	U.02	Ja	Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd.	ISO 27002 2017: 14.2.4, BIO 2019: 14.1.1.	Overleg bewijsstukken.
366	Evaluatie leveranciersdienstverlening	Thema Softwarepakketten	C.01	Ja	De klant behoort regelmatig de dienstverlening van softwarepakketleveranciers te monitoren, te beoordelen en te auditen.	BIO 2019: 15.2.1.	Interne controle, Overleg bewijsstukken of Verklaring.
388	Informatieverstrekking aan betrokkene met applicaties	Privacy-supplement SSD	SSD P.03		Om de gegevens te mogen verwerken wordt de betrokkene, waarvan de persoonsgegevens worden verwerkt, geïnformeerd betreffende welke verwerking (van de persoonsgegevens) plaatsvindt en krijgt deze betrokkene een waarschuwing bij het verkrijgen van toegang tot bijzondere persoonsgegevens.	CIP De Privacy Baseline 2020: U.05, AVG: art. 14, AVG: overweging 60, Wpg: Art 24a lid 1	Overleg bewijsstukken en/of verklaring en testen
391	Dataminimalisatie binnen applicaties	Privacy-supplement SSD	SSD P.06		De organisatie behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn.	AVG: art. 6 lid 1, Wpg art 3 lid 2 en 5, Art 4 lid 2, Art 8 lid 1, 2, 6, Art 9 lid 4, Art 14	Overleg bewijsstukken en/of verklaring
410	Malwareprotectie	Thema Serverplatform	U.03	Ja	Ter bescherming tegen malware behoren beheersmaatregelen voor preventie, detectie en herstel te worden geïmplementeerd, in combinatie met het stimuleren van een passend bewustzijn van gebruikers.	BIO 2019: 12.2.1.	Interne controle, Overleg bewijsstukken of Verklaring.
424	Technische kwetsbaarhedenbeheer	Thema Serverplatform	U.04	Ja	Informatie over technische serverkwetsbaarheden[1] behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden dient te worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.	BIO 2019: 12.6.1.	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.

430	Beheer op afstand	Thema Serverplatform	U.06		Richtlijnen en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van beheer op afstand van servers.	BIO 2019: 6.2.2.	Interne controle, Overleg bewijsstukken of Verklaring.
462	Beheerorganisatie servers en serverplatforms	Thema Serverplatform	C.06		Binnen de beheerorganisatie is een beveiligingsfunctionaris benoemd die de organisatie ondersteunt in de vorm van het bewaken van beveiligingsbeleid en die inzicht verschaft in de inrichting van de servers en het serverplatform.	CIP-netwerk	Interne controle, Overleg bewijsstukken of Verklaring.
477	Richtlijnen voor netwerkbeveiliging	Thema Communicatievoorzieningen	U.01		Organisaties behoren hun netwerken te beveiligen op basis van richtlijnen voor ontwerp, implementatie en beheer.	CIP-netwerk	Interne controle, Overleg bewijsstukken of Verklaring.
492	Beveiliging van netwerkdiensten	Thema Communicatievoorzieningen	U.05	Ja	Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	BIO 2019: 13.1.2 BIO2.0-opmaat: 8.21	Interne controle, Overleg bewijsstukken of Verklaring.
493	O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.1	Ja	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 risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
494	O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.2	Ja	Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 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).	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
495	O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.3	Ja	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
532	Netwerk beveiligingsarchitectuur	Thema Communicatievoorzieningen	U.17		De beveiligingsarchitectuur behoort de samenhang van het netwerk te beschrijven en structuur te bieden in de beveiligingsmaatregelen, gebaseerd op het vigerende bedrijfsbeleid, de leidende principes en de geldende normen en standaarden.	CIP-netwerk	Interne controle, Overleg bewijsstukken of Verklaring.

534	Compliance-toets netwerkbeveiliging	Thema Communicatievoorzieningen	C.02		De naleving van een, volgens het beveiligingsbeleid, veilige inrichting van netwerk(diensten), behoort periodiek gecontroleerd te worden en de resultaten behoren gerapporteerd te worden aan het verantwoordelijke management (compliance-toetsen).	CIP-netwerk	Interne controle, Overleg bewijsstukken of Verklaring.
554	Logging binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.03		De logging en monitoring van het netwerk behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.	AVG: art. 5 lid 2 en art. 33 lid 5, Wpg Art. 32a	Overleg bewijsstukken en/of verklaring
563	Contractmanagement	Thema Huisvesting-IV	B.05		Huisvesting IV behoort te voldoen aan kwalitatieve en kwantitatieve eisen die zijn vastgelegd in overeenkomsten met de betreffende leveranciers.	NCSC 2015: B.05 NCSC 2015: C.10	Interne controle.
639	Beheersorganisatie huisvesting IV	Thema Huisvesting-IV	C.04		De stakeholder van huisvesting IV behoort een beheersorganisatie te hebben ingericht waarin de processtructuur, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen zijn vastgesteld.	CIP-netwerk	Interne controle.
795	O-maatregel. Beheren van speciale toegangsrechten	BIO 2019	9.2.3.1	Ja	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
796	O-maatregel. Beperking toegang tot informatie	BIO 2019	9.4.1.1	Ja	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
797	O-maatregel. Beperking toegang tot informatie	BIO 2019	9.4.1.2	Ja	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
798	Functiescheiding	Thema Toegangsbeveiliging	U.07	Ja	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruiken van bedrijfsmiddelen te verminderen.	BIO 2019: 6.1.2 BIO2.0-opmaat: 5.3	Interne controle, Overleg bewijsstukken of Verklaring.
802	Geheime authenticatie-informatie	Thema Toegangsbeveiliging	U.08		Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	BIO 2019: 9.2.4 BIO2.0-opmaat: 5.17	Interne controle, Overleg bewijsstukken of Verklaring.
812	Autorisatie	Thema Toegangsbeveiliging	U.09	Ja	Toegang (autorisatie) tot informatie en systeemfuncties van toepassingen behoren te worden beperkt in overeenstemming met het toegangsbeveiligingsbeleid.	BIO 2019: 9.4.1 BIO2.0-opmaat: 8.3	Overleg bewijsstukken en/of Testen.
826	Autorisatievoorzieningen	Thema Toegangsbeveiliging	U.10		Voor autorisatiebeheer moeten binnen de daartoe in aanmerking komende applicaties technische autorisatievoorzieningen beschikbaar zijn, zoals: een personeelsregistratiesysteem, een autorisatiebeheersysteem en autorisatiefaciliteiten.	CIP-netwerk	Interne controle, Overleg bewijsstukken of Verklaring.
839	O-maatregel. Beoordeling van toegangsrechten van gebruikers (BBN2)	BIO 2019	9.2.5.3	Ja	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.

840	Logging en monitoring	Thema Toegangs beveiliging Thema Clouddiensten	C.03 U.15	Ja	Log-bestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	BIO 2019: 12.4.1 BIO2.0-opmaat: 8.15	Interne controle, Overleg bewijsstukken of Verklaring.
843	O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.3	Ja	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectievoorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
844	O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.4	Ja	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 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.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
845	O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.5	Ja	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
855	Doelbinding op rolniveau	Privacy-supplement Toegangs beveiliging	TBV P.02		De organisatie behoort verwerkers gescheiden en beperkt toegang te verlenen tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.	NEN 7510 2017: A.9.2.6, Wpg Art 6 lid 1 t/m 6 Art 6a	Overleg bewijsstukken en/of verklaring
856	Toegang op taakniveau	Privacy-supplement Toegangs beveiliging	TBV P.03		Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.	CIP-netwerk, Wpg: Art 6 lid 1 t/m 6 Art 6a	Overleg bewijsstukken en/of verklaring
859	Toegang buiten beveiligde omgevingen	Privacy-supplement Toegangs beveiliging	TBV P.06		Er is een procedure ingericht voor het transporteren van persoonsgegevens buiten een beschermde omgeving, waarbij door versleuteling de kans op een datalek is verkleind en door minimalisatie de omvang van een datalek wordt beperkt.	AVG: art.32, Wpg: Art 6 lid 1 t/m 6 Art 6a	Overleg bewijsstukken en/of verklaring

860	Toegang in het buitenland	Privacy-supplement Toegangsbeveiliging	TBV P.07		De organisatie hanteert regels voor medewerkers en andere verwerkers, die buiten Nederland persoonsgegevens of authenticatiemiddelen (voor de toegang tot persoonsgegevens vanuit het buitenland) met zich meedragen of in hun bezit hebben, ongeacht of deze informatie versleuteld is.	AVG: art. 32, Wpg: Art 6 lid 1 t/m 6 Art 6a	Overleg bewijsstukken en/of verklaring
861	Beëindiging (verwerkers)overeenkomst	Privacy-supplement Toegangsbeveiliging	TBV P.08		De verwerkingsverantwoordelijke legt in de (verwerkers) overeenkomst afspraken vast, met de persoon of partij die persoonsgegevens verwerkt, over het verwijderen of overdragen van persoonsgegevens bij beëindiging van de relatie; eventuele derden worden over de beëindiging geïnformeerd.	AVG: art.32, AP Werkende verwerkersovereenkomsten september 2019 : 4.3.6	Overleg bewijsstukken en/of verklaring
886	O-maatregel. Beschermen van registraties	BIO 2019	18.1.3.1	Ja	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
898	Cryptoservices	Thema Clouddiensten	U.11	Ja	Gevoelige data van CSC's behoort conform het overeengekomen beleid inzake cryptografische maatregelen tijdens transport via netwerken en bij opslag bij CSP te zijn versleuteld	CIP-netwerk, BIO 2019: 10.1.1, 10.1.2.	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.
901	O-maatregel. Sleutelbeheer	BIO 2019	10.1.2.1	Ja	Ingeval van PKIoverheid-certificaten: hanteer de PKIoverheid-eisen ten aanzien van het sleutelbeheer. In overige situaties: hanteer de standaard ISO 11770 voor het beheer van cryptografische sleutels.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.
902	O-maatregel. Sleutelbeheer	BIO 2019	10.1.2.2	Ja	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.
903	Koppelvlakken	Thema Clouddiensten	U.12	Ja	De onderlinge netwerkconnecties (koppelvlakken) in de keten van de CSC naar de CSP behoren te worden bewaakt en beheerst om de risico's van datalekken te beperken.	CIP-netwerk, BIO 2019: 13.1.2.	Interne controle, Overleg bewijsstukken of Verklaring.
916	Clouddienstenarchitectuur	Thema Clouddiensten	U.16		De clouddienstenarchitectuur specificeert de samenhang en beveiliging van de services en de interconnectie tussen de CSC en de CSP en biedt transparantie en overzicht van randvoorwaardelijke omgevingsparameters, voor zowel de opzet, de levering en de portabiliteit van CSC-data.	CIP-netwerk	Interne controle, Overleg bewijsstukken of Verklaring.
1064	O-maatregel. Beleid voor mobiele apparatuur	BIO 2019	6.2.1.1	Ja	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.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.

1065	O-maatregel. Beleid voor mobiele apparatuur	BIO 2019	6.2.1.2	Ja	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 device 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)	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
1103	O-maatregel. Back-up van informatie	BIO 2019	12.3.1.3	Ja	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 (twee dagen van 8 uur) in 85% van de gevallen.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
1104	O-maatregel. Back-up van informatie	BIO 2019	12.3.1.4	Ja	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.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
1105	O-maatregel. Back-up van informatie	BIO 2019	12.3.1.5	Ja	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
1108	O-maatregel. Verwijderen van media	BIO 2019	8.3.2.1	Ja	Media die vertrouwelijke informatie bevatten, zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden.	8.3.1 is in de vorige versie toegevoegd. De tekst komt nergens terug. Dit is alleen de tekst van 8.3.1	Interne controle, Overleg bewijsstukken of Verklaring.

1109	O-maatregel. Verwijderen van media	BIO 2019	8.3.2.2	Ja	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 (ISO 27002 – implementatierichtlijn 8.3.2.a).	gedaan om in ICO de complete set van O-maatregelen te kunnen verwijzen. 8.3.1 en 2 komen beide terug in de O-maatregelen. Overigens hebben beide wel te maken met de titel van het object, dus het misstaat ook weer niet. In Opmaat zijn beide controls ook onder 1 dak gebracht. (7.10)	Interne controle, Overleg bewijsstukken of Verklaring.
1110	O-maatregel. Verwijderen van media	BIO 2019	8.3.2.3	Ja	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.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.
1116	Capaciteitsbeheer	Thema Middlewar e	U.13		Het gebruik van middelen behoort te worden gemonitord en beoordeeld, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	BIO 2019: 12.1.3 BIO2.0-opmaat: 8.6	Interne controle, Overleg bewijsstukken of Verklaring.
1125	Monitoren gebruikers- en beheerdersactiviteiten	Thema Middlewar e	C.05		De organisatie reviewt en analyseert regelmatig de logbestanden om onjuist gebruik en verdachte activiteiten aan middlewarefunctionaliteiten vast te stellen en bevindingen aan het management te rapporteren.	ISO 27002 2017: 12.4.1	Interne controle, Overleg bewijsstukken of Verklaring.