Excel Export ICO Wizard tbv Inkoopafdeling/opdrachtgever/budgethouder

Inkooponderdelen	Clouddiensten, Mobiele Applicaties, Serverplatform, Softwarepakketten, Toegangsbeveiliging
Proceseis	ja
Producteis	ja
Eis voor de opdrachtgever	nee
Eis voor de opdrachtnemer	ja
Ook eisen meegeven die alleen te maken hebben met	ja
Basispakket	ja
Privacy-supplement	nee
Toon BIO-O maatregelen BBN1	nee
Toon BIO-O maatregelen BBN2	ja
Toon ABDO-eisen TBB4	nee
Toon ABDO-eisen TBB3	nee
Toon ABDO-eisen TBB2	nee
Toon ABDO-eisen TBB1	nee
Aantal geselecteerde eisen	155

Samengesteld door	Projectteam
Organisatie	Waterschap Limburg (directie Ontwikkeling, Strategie en transitie (OST))
Datum	11-06-2025

Dit rapport geeft de veiligheidseisen weer van een of meer opgegeven inkooponderdelen.

Deze eisen zijn gericht op basisbeveiligingsniveaus (BBN) 1 en 2 van de BIO. Hogere beveiligingsniveaus zijn altijd maatwerk.
Het gebruik van de ICO-hulpmiddelen is geen substituut voor eigen risicoafweging.

Voor de gemitieerde dreigingen is aangesloten op de standaarddreigingenlijst van RAVIB, het Open Source tool voor Risicoanalyse.

Nr	Naam Eis	Referentie brondocument:	Referentie code norm:	BIO-O-maatregel:	Samenvatting eis:	Gebaseerd op: (ISO27002-paragraaf, of ander framework)	Relevante standaard PToLU-lijst Forum Standaardisatie:	Verificatie methode(n):	Eis gevraagd J/N	Als Eis/Wens	Reden niet gevraagd/geeist	Weging in RFC	Toelichting:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Inkooponderdeel
291	Veilige server side applicaties	SSD Mobile	SSDm-1		Bij de bouw van de app worden de beveiligingseisen van de applicatie op de server door de ontwikkelaar gerespecteerd.	SSD: alle eisen		Overleg bewijsstukken.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	10	Uitval van systemen door configuratiefouten.									Mobiele Applicaties
292	Veilig besturingssysteem	SSD Mobile	SSDm-2		De app controleert of het besturingssysteem aan de beveiligingsvereisten voldoet waarop de veiligheid van de app is gebaseerd en geeft een melding aan de gebruiker.	ASVS : V17.7		Overleg bewijsstukken.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	10	Uitval van systemen door configuratiefouten.									Mobiele Applicaties
293	Up-to-date apps	SSD Mobile	SSDm-3		De leverancier past lifecyclemanagement toe op de apps die hij levert, waardoor gebruikers altijd over de meest veilige appversie (kunnen) beschikken.	ASVS : V17.17		Overleg bewijsstukken en/of Verklaring.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	50	Software wordt niet meer ondersteund door de uitgever.	49	Niet beschikbaar zijn van diensten van derden.							Mobiele Applicaties
294	Third party apps	SSD Mobile	SSDm-4		Het gebruik van third party apps is gebaseerd op een risicoafweging.	ASVS : V17.17		Overleg bewijsstukken en/of Verklaring.						3	Onvoldoende aandacht voor beveiliging binnen projecten.	28	Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.											Mobiele Applicaties
295	Veilige code bij oplevering	SSD Mobile	SSDm-5		De ontwikkelaar gebruikt alleen vertrouwde broncode bibliotheken van derden	ASVS: V17.11, V17.16, V17.25		Overleg bewijsstukken en/of Verklaring.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.											Mobiele Applicaties
296	Integere werking van de app	SSD Mobile	SSDm-6		De app op het mobiele apparaat is afgeschermd tegen ongewenste of onbedoelde manipulatie en de uitkomsten van de kritische bedrijfslogica worden altijd gecontroleerd op de server.	SSD: 3		Testen.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.											Mobiele Applicaties
297	Locatie voor de opslag	SSD Mobile	SSDm-7		De keuze van de locatie waar de gegevens en informatie van de logica van de app worden opgeslagen is gebaseerd op het principe van de vertrouwelijkheid.	ASVS: V17.3, V17.4		Overleg bewijsstukken en/of Verklaring.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	36	Wetgeving over informatie in de cloud.											Mobiele Applicaties
298	Opslag op het mobiele apparaat	SSD Mobile	SSDm-8		Bij het opslaan van vertrouwelijke informatie op het mobiele apparaat zijn de vertrouwelijke gegevens afgeschermd door toepassing van cryptografische technieken.	SSD: 2 ASVS: V17.5, V17.21, V17.24, V17.27		Testen.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	18	Verlies van mobiele apparatuur en opslagmedia.	25	Informatie op systemen bij reparatie of verwijdering.								Mobiele Applicaties
299	Onnodige informatie in het cachegeheugen	SSD Mobile	SSDm-9		Vertrouwelijke informatie is in het cachegeheugen op basis van een risicoafweging per gegeven tot een minimum beperkt, dit geldt zowel binnen als buiten de eigen app.	ASVS: V17.14, V17.18, V17.20		Testen.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.											Mobiele Applicaties
300	Timeout gebruikersessie	SSD Mobile	SSDm-10		De app beëindigt een gebruikerssessie na een voor-ingestelde periode van inactiviteit van de gebruiker via automatische session termination.	27002: 11.3.2 SSD: 12B ASVS: 17.8		Testen.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.											Mobiele Applicaties
301	Logging	SSD Mobile	SSDm-11		Logging voor debugging is vóór in productiename uitgeschakeld en de logbestanden zijn verwijderd. Wanneer statistische logging over het gebruik van de app plaatsvindt, dan bevat deze géén persoonlijke gegevens.	SSD: 30 ASVS: V17.10, V17.13, V17.22		Testen.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	18	Verlies van mobiele apparatuur en opslagmedia.	25	Informatie op systemen bij reparatie of verwijdering.								Mobiele Applicaties
302	Sessie versleuteling	SSD Mobile	SSDm-12		De applicatie past encryptie toe op alle communicatie via netwerken.	27002: 10.6.1 27002: 10.8.1 27002: 10.9.1	TLS en HTTPS (beveiligde verbinding)	Testen. Daarnaast Internet.nl.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	27	Misbruiken van zwakheden in netwerkbeveiliging.								Mobiele Applicaties
303	Certificaat-pinning	SSD Mobile	SSDm-13		De app controleert tijdens het opzetten van een versleutelde verbinding of het server-certificaat vertrouwd is en neemt de nodige maatregelen.	ASVS: V17.1, V17.15	TLS en HTTPS (beveiligde verbinding)	Testen. Daarnaast Internet.nl.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	27	Misbruiken van zwakheden in netwerkbeveiliging.								Mobiele Applicaties
304	Hardening van de apps	SSD Mobile	SSDm-14		De ontwikkelaar waarborgt dat toegang tot de app alleen mogelijk is via interacties die noodzakelijk zijn voor het correct functioneren van de applicatie.	SSD-1		Testen.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.											Mobiele Applicaties
305	Least Privilege voor andere apps	SSD Mobile	SSDm-15		De toegangsrechten van de app tot functies en data zijn alleen uitgegeven waar zij het onderbouwde doel en belang van de gebruiker dienen.	SSD: 8 ASVS: V17.9, V17.23, V17.26, V17.28		Overleg bewijsstukken.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	24	Onduidelijkheid over classificatie en bevoegdheden.											Mobiele Applicaties
306	Invoernormalisatie	SSD Mobile	SSDm-16		De app voorkomt manipulatie door alle ontvangen invoer te normaliseren alvorens die te valideren.	SSD-19		Testen.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.											Mobiele Applicaties
307	Invoervalidatie	SSD Mobile	SSDm-17		De app voorkomt de mogelijkheid tot manipulatie door alle ontvangen invoer te valideren, voordat deze invoer wordt verwerkt.	SSD: 22 ASVS: V17.19		Testen.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.											Mobiele Applicaties
308	HTTP-methoden	SSD Mobile	SSDm-18		De app gebruikt alleen de HTTP-functionaliteiten die nodig zijn voor het communiceren met andere apps en services, al dan niet over het netwerk.	SSD: 26 ASVS: V17.19	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam)	Testen. Daarnaast Internet.nl.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.											Mobiele Applicaties
309	XML externe entiteit injectie	SSD Mobile	SSDm-19		De app beperkt de mogelijkheid tot manipulatie door alle externe XML invoer te beschermen tegen entiteit injectie.	SSD Mobile: SSDm-19		Testen.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	26	Misbruik van kwetsbaarheden in applicaties of hardware.											Mobiele Applicaties

Nr	Naam Eis	Referentie brondocument:	Referentie code norm:	BIO-O-maatregel:	Samenvatting eis:	Gebaseerd op: (ISO27002-paragraaf, of ander framework)	Relevante standaard PToLU-lijst Forum Standaardisatie:	Verificatie methode(n):	Eis gevraagd J/N	Als Eis/Wens	Reden niet gevraagd/geeist	Weging in RFC	Toelichting:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Inkooponderdeel
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.						3	Onvoldoende aandacht voor beveiliging binnen projecten.	28	Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	183	Onvoldoende mogelijkheid om sturing te geven aan leveranciersrelaties specifiek voor informatiebeveiliging.								Softwarepakketten
344	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		Overleg bewijsstukken en/of Verklaring.						3	Onvoldoende aandacht voor beveiliging binnen projecten.	28	Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	183	Onvoldoende mogelijkheid om sturing te geven aan leveranciersrelaties specifiek voor informatiebeveiliging.								Softwarepakketten
345	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		Overleg bewijsstukken en/of Verklaring.						3	Onvoldoende aandacht voor beveiliging binnen projecten.	28	Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	183	Onvoldoende mogelijkheid om sturing te geven aan leveranciersrelaties specifiek voor informatiebeveiliging.								Softwarepakketten
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.						184	Het niet beschikken over een overeengekomen leidraad/globale manier van aanpak bij beëindiging van leverancierscontracten.												Softwarepakketten
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.						28	Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	185	Datalekken en de continuïteit niet kunnen waarborgen.										Softwarepakketten
348	Cryptografie	Thema Softwarepakketten	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.		Overleg bewijsstukken en/of Verklaring.						35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	186	Onvoldoende mogelijkheid om sturing te geven aan de effectieve en betrouwbare inrichting van cryptografische beheersmaatregelen binnen softwarepakketten.										Softwarepakketten
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.						35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	31	Onveilig versturen van gevoelige informatie.										Softwarepakketten
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.						35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	31	Onveilig versturen van gevoelige informatie.										Softwarepakketten
352	Levenscyclusmanagement softwarepakket	Thema Softwarepakketten	U.01		De leverancier behoort de klant te adviseren met marktontwikkelingen en kennis van (de leeftijd van) applicaties en technische softwarestack over strategische ontwikkeling en innovatieve keuzes voor het ontwikkelen en onderhouden van informatiesystemen in het applicatielandschap.	CIP-netwerk		Overleg bewijsstukken.						50	Software wordt niet meer ondersteund door de uitgever.	188	De continuïteit van de bedrijfsprocessen kan niet gewaarborgd worden.										Softwarepakketten
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.						10	Uitval van systemen door configuratiefouten.	11	Uitval van systemen door softwarefouten.	189	Aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van de data.								Softwarepakketten
355	Bedrijfscontinuïteit	Thema Softwarepakketten	U.03		De leverancier behoort processen, procedures en beheersmaatregelen te documenteren, te implementeren en te handhaven.	BIO 2019: 17.1.2.		Testen.						190	Onnodig lange uitval van bedrijfsactiviteiten na calamiteiten waardoor bedrijfsdoelstellingen niet worden gehaald.												Softwarepakketten
356	Input-/output-validatie	Thema Softwarepakketten	U.04		Het softwarepakket behoort mechanismen te bevatten voor normalisatie en validatie van invoer en voor schoning van de uitvoer.	SSD 2020: SSD-19; SSD 2020: SSD-20		Testen.						26	Misbruik van kwetsbaarheden in applicaties of hardware.	191	Misbruiken van softwarepakketten en ongemerkt toegang krijgen tot gegevens en de beschikbaarheid, integriteit en vertrouwelijkheid van de data schaden.										Softwarepakketten
357	Sessiebeheer	Thema Softwarepakketten	U.05		Sessies behoren authentiek te zijn voor elke gebruiker en behoren ongeldig gemaakt te worden na een time-out of perioden van inactiviteit.	SSD 2020: SSD-12; SSD 2020: SSD-14	SAML (authenticatie)	Testen.						26	Misbruik van kwetsbaarheden in applicaties of hardware.	192	Onbevoegden maken via kwetsbaarheden gebruik van openstaande sessies en krijgen toegang krijgen tot gevoelige data. Het ontstaan van zwakheden als Cross-Site Request Forgery (CSRF) en Clickjacking.										Softwarepakketten
358	Gegevensopslag	Thema Softwarepakketten	U.06		Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als noodzakelijk.	SSD 2020: SSD-2 met O-maatregel BIO 2019: 10.1.1.2.		Testen.						26	Misbruik van kwetsbaarheden in applicaties of hardware.	193	Opgeslagen gegevens worden ongeautoriseerd ingezien, aangepast of verwijderd door ontoereikende versleuteling.										Softwarepakketten
359	Communicatie	Thema Softwarepakketten	U.07		Het softwarepakket past versleuteling toe op de communicatie van gegevens die passend bij het classificatieniveau is van de gegevens en controleert hierop.	SSD 2020: SSD-4	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam)	Testen.						26	Misbruik van kwetsbaarheden in applicaties of hardware.	35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	194	Onbevoegden krijgen toegang tot getransporteerde gegevens.								Softwarepakketten
360	Authenticatie	Thema Softwarepakketten	U.08		Softwarepakketten behoren de identiteiten van gebruikers vast te stellen met een mechanisme voor identificatie en authenticatie.	SSD 2020: SSD-5 SIG 2019: 3.2.3		Testen.						26	Misbruik van kwetsbaarheden in applicaties of hardware.	19	Misbruik van andermans identiteit.	21	Onterecht hebben van rechten.	195	Onbevoegde personen krijgen toegang tot de data in het softwarepakket.					Softwarepakketten
361	Toegangsautorisatie	Thema Softwarepakketten	U.09		Het softwarepakket behoort een autorisatiemechanisme te bieden.	SSD 2020: SSD-8		Testen.						26	Misbruik van kwetsbaarheden in applicaties of hardware.	196	Het toegang krijgen tot gegevens die niet noodzakelijk zijn voor het uitvoeren van de rol/functie.										Softwarepakketten
362	Autorisatiebeheer	Thema Softwarepakketten	U.10		De rechten die gebruikers hebben binnen een softwarepakket (inclusief beheerders) zijn zo ingericht dat autorisaties kunnen worden toegewezen aan organisatorische functies en scheiding van niet verenigbare autorisaties mogelijk is.	SSD 2020: SSD-7		Testen.						26	Misbruik van kwetsbaarheden in applicaties of hardware.	19	Misbruik van andermans identiteit.	21	Onterecht hebben van rechten.	197	Misbruik van gegevens in een softwarepakket.					Softwarepakketten
363	Logging	Thema Softwarepakketten	U.11		Het softwarepakket biedt signaleringsfuncties voor registratie en detectie die beveiligd zijn ingericht.	SSD 2020: SSD-30		Testen.						39	Incidenten worden niet tijdig opgepakt.	40	Informatie voor het aanpakken van incidenten ontbreekt.	52	Ketenafhankelijke data (-bestanden) input/output uit systemen	198	Afwijkingen van normaal gedrag binnen het softwarepakket zijn niet zichtbaar.					Softwarepakketten

Nr	Naam Eis	Referentie brondocument:	Referentie code norm:	BIO-O-maatregel:	Samenvatting eis:	Gebaseerd op: (ISO27002-paragraaf, of ander framework)	Relevante standaard PToLU-lijst Forum Standaardisatie:	Verificatie methode(n):	Eis gevraagd J/N	Als Eis/Wens	Reden niet gevraagd/geeist	Weging in RFC	Toelichting:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Inkooponderdeel
364	Application Programming Interface (API)	Thema Softwarepakketten	U.12		Softwarepakketten behoren veilige API's te gebruiken voor import en export van gegevens.	OWASP ASVS 2020: V13		Testen.						8	Aanvallen via systemen die niet in eigen beheer zijn.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	52	Ketenafhankelijke data (-bestanden) input/output uit systemen	199	Gegevens kunnen niet uitgewisseld worden.						Softwarepakketten
365	Gegevensimport	Thema Softwarepakketten	U.13		Softwarepakketten behoren mechanismen te bieden om niet-vertrouwde bestandsgegevens uit niet-vertrouwde omgevingen veilig te importeren en veilig op te slaan.	OWASP ASVS 2020: V12		Testen.						8	Aanvallen via systemen die niet in eigen beheer zijn.	52	Ketenafhankelijke data (-bestanden) input/output uit systemen	200	De beschikbaarheid, integriteit en vertrouwelijkheid van de data wordt geschaad.						Softwarepakketten
368	Versiebeheer	Thema Softwarepakketten	C.02	Ja	Wijzigingen aan het softwarepakket binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	BIO 2019: 12.1.2, 14.2.2.		Overleg bewijsstukken en/of Verklaring.						12	Fouten als gevolg van wijzigingen in andere systemen.	202	Werken met verouderde versies van een softwarepakket.									Softwarepakketten
371	Patchmanagement	Thema Softwarepakketten	C.03	Ja	Patchmanagement behoort procesmatig en procedureel uitgevoerd te worden, dat tijdig vanuit externe bibliotheken informatie wordt ingewonnen over technische kwetsbaarheden van de gebruikte code, zodat zo snel mogelijk de laatste (beveiligings-)patches kunnen worden geïnstalleerd.	BIO 2019: 12.6.1, NCSC 2015: C.09.		Interne controle.						26	Misbruik van kwetsbaarheden in applicaties of hardware.	203	Kwetsbaarheden brengen de stabiliteit en betrouwbaarheid van systemen in gevaar.									Softwarepakketten
395	Beleid voor beveiligde inrichting en onderhoud	Thema Serverplatform	B.01	Ja	Voor het beveiligd inrichten en onderhouden van het serverplatform behoren regels te worden vastgesteld en binnen de organisatie te worden toegepast.	BIO 2019: 14.2.1.		Interne controle, Overleg bewijsstukken of Verklaring.						5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	159	Onvoldoende mogelijkheden om sturing te geven aan de effectieve en betrouwbare inrichting van een serverplatform en hierover een verantwoordingsrapportage te laten afgeven.									Serverplatform
397	Inrichtingsprincipes voor serverplatform	Thema Serverplatform	B.02	Ja	Principes voor het inrichten van beveiligde servers behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het inrichten van servers.	BIO 2019: 14.2.1, 14.2.5.		Overleg bewijsstukken en/of Verklaring.						10	Uitval van systemen door configuratiefouten.	27	Misbruiken van zwakheden in netwerkbeveiliging.	51	Kwijtraken van belangrijke kennis bij niet beschikbaar zijn van medewerkers.	9	Uitval van systemen door hardwarefouten.	160	Bij de inrichting van servers zijn niet alle vereiste beveiligingsprincipes meegenomen.				Serverplatform
407	Serverplatform-architectuur	Thema Serverplatform	B.03		De functionele eisen, beveiligingseisen en architectuurvoorschriften van het serverplatform zijn in samenhang in een architectuurdocument vastgelegd.	NIST SP 800-53 Rev. 5 2020: PL-8		Interne controle, Overleg bewijsstukken of Verklaring.						10	Uitval van systemen door configuratiefouten.	27	Misbruiken van zwakheden in netwerkbeveiliging.	51	Kwijtraken van belangrijke kennis bij niet beschikbaar zijn van medewerkers.	161	Onvoldoende sturing hebben op de inrichting van het serverplatform. Bedreigingen worden over het hoofd gezien.						Serverplatform
408	Bedieningsprocedure	Thema Serverplatform	U.01		Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	BIO 2019: 12.1.1.		Overleg bewijsstukken.						13	Gebruikersfouten.	162	Het optreden van beveiligingsincidenten en/of datalekken en verlies van kennis voor het bedienen van serverplatforms.									Serverplatform
409	Standaarden voor serverconfiguratie	Thema Serverplatform	U.02		Het serverplatform is geconfigureerd volgens gedocumenteerde standaarden.	SoGP 2018: SY1.2		Overleg bewijsstukken en/of Verklaring.						10	Uitval van systemen door configuratiefouten.	163	De server is niet of onvoldoende geconfigureerd voor de functionaliteit binnen de IT-omgeving.									Serverplatform
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.						6	Toegang tot informatie wordt geblokkeerd.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	39	Incidenten worden niet tijdig opgepakt.	53	Verificatie op corrupte data(-bestanden) uit de keten.	164	Malware wordt niet of te laat opgespoord en aangetroffen malware wordt niet of voldoende hersteld.				Serverplatform
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.	STIX en TAXII (uitwisseling van cyberdreigingsinformatie)	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.						11	Uitval van systemen door softwarefouten.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	51	Kwijtraken van belangrijke kennis bij niet beschikbaar zijn van medewerkers.	165	Kwetsbaarheden in servers worden niet opgemerkt, waardoor er misbruik van gemaakt kan worden.						Serverplatform
427	Patchmanagement	Thema Serverplatform	U.05		Patchmanagement is procesmatig en procedureel opgezet en wordt ondersteund door richtlijnen zodat het zodanig kan worden uitgevoerd dat op de servers de laatste (beveiligings)patches tijdig zijn geïnstalleerd.	NCSC 2015: C.09		Overleg bewijsstukken en/of Verklaring.						11	Uitval van systemen door softwarefouten.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	40	Informatie voor het aanpakken van incidenten ontbreekt.	49	Niet beschikbaar zijn van diensten van derden.	50	Software wordt niet meer ondersteund door de uitgever.	166	De stabiliteit en betrouwbaarheid van servers komt in gevaar.		Serverplatform
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.						26	Misbruik van kwetsbaarheden in applicaties of hardware.	49	Niet beschikbaar zijn van diensten van derden.	167	De server is onbetrouwbaar en functioneert niet naar behoren.							Serverplatform
431	Server-onderhoud	Thema Serverplatform	U.07		Servers behoren correct te worden onderhouden om de continue beschikbaarheid en integriteit te waarborgen.	BIO 2019: 11.2.4.		Overleg bewijsstukken en/of Verklaring.						11	Uitval van systemen door softwarefouten.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	50	Software wordt niet meer ondersteund door de uitgever.	40	Informatie voor het aanpakken van incidenten ontbreekt.	43	Brand.	168	Aantasting van de beschikbaarheid en integriteit van servers.		Serverplatform
432	Verwijderen of hergebruiken serverapparatuur	Thema Serverplatform	U.08		Alle onderdelen van servers die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	BIO 2019: 11.2.7.		Overleg bewijsstukken en/of Verklaring.						25	Informatie op systemen bij reparatie of verwijdering.	169	Informatie met een vertrouwelijk karakter komt in handen van onbevoegden.									Serverplatform
433	Hardenen server	Thema Serverplatform	U.09		Voor het beveiligen van een server worden overbodige functies en ongeoorloofde toegang uitgeschakeld.	SoGP 2018: SY1.2.5 SoGP 2018: SY1.2.8		Overleg bewijsstukken en/of Verklaring.						10	Uitval van systemen door configuratiefouten.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	9	Uitval van systemen door hardwarefouten.	170	Misbruik van overbodige en/of niet gebruikte functies, services en accounts.						Serverplatform
434	Serverconfiguratie	Thema Serverplatform	U.10		Serverplatforms behoren zo geconfigureerd te zijn, dat zij functioneren zoals het vereist is en zijn beschermd tegen ongeautoriseerd en incorrecte updates.	SoGP 2018: SY1.2		Overleg bewijsstukken en/of Verklaring.						10	Uitval van systemen door configuratiefouten.	171	Serverplatforms functioneren niet zoals vereist en zijn niet/onvoldoende beschermd tegen ongeautoriseerd en incorrecte updates.									Serverplatform
435	Virtualisatie serverplatform	Thema Serverplatform	U.11		Virtuele servers behoren goedgekeurd te zijn en toegepast te worden op robuuste en veilige fysieke servers (bestaande uit hypervisors en virtuele servers) en behoren zodanig te zijn geconfigureerd dat gevoelige informatie in voldoende mate is beveiligd.	SoGP 2018: SY1.3		Overleg bewijsstukken en/of Verklaring.						10	Uitval van systemen door configuratiefouten.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	172	Dat onbevoegden inzicht krijgen in gevoelige informatie.							Serverplatform
436	Beperking van software- installatie	Thema Serverplatform	U.12	Ja	Voor het door gebruikers (beheerders) installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	BIO 2019: 12.6.2.		Overleg bewijsstukken en/of Verklaring.						14	Systemen worden niet gebruikt waarvoor ze bedoeld zijn.	21	Onterecht hebben van rechten.	173	Het introduceren van kwetsbaarheden.						Serverplatform
437	O-maatregel. Beperkingen voor het installeren van software	BIO 2019	12.6.2.1	Ja	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan wat via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.						14	Systemen worden niet gebruikt waarvoor ze bedoeld zijn.	136	Het introduceren van kwetsbaarheden in de software.									Serverplatform
438	Kloksynchronisatie	Thema Serverplatform	U.13		De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gedocumenteerd en gesynchroniseerd met één referentietijdbron.	BIO 2019: 12.4.4.		Overleg bewijsstukken en/of Verklaring.						20	Misbruik van speciale bevoegdheden.	40	Informatie voor het aanpakken van incidenten ontbreekt.	174	Onnauwkeurige auditlogbestanden niet kunnen onderzoeken of als bewijs in juridische of disciplinaire zaken belemmeren en de geloofwaardigheid van dat bewijsmateriaal schaden.							Serverplatform
440	Ontwerpdocument	Thema Serverplatform	U.14		Het ontwerp van een serverplatform behoort te zijn gedocumenteerd.	SoGP 2018: SY1.1.1		Overleg bewijsstukken en/of Verklaring.						49	Niet beschikbaar zijn van diensten van derden.	50	Software wordt niet meer ondersteund door de uitgever.	51	Kwijtraken van belangrijke kennis bij niet beschikbaar zijn van medewerkers.	175	De inrichting van de server en het serverplatform wijkt af van wat vooraf nodig is geacht.					Serverplatform

Nr	Naam Eis	Referentie brondocument:	Referentie code norm:	BIO-O-maatregel:	Samenvatting eis:	Gebaseerd op: (ISO27002-paragraaf, of ander framework)	Relevante standaard PToLU-lijst Forum Standaardisatie:	Verificatie methode(n):	Eis gevraagd J/N	Als Eis/Wens	Reden niet gevraagd/geeist	Weging in RFC	Toelichting:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Inkooponderdeel
441	Evaluatierichtlijn servers en serverplatforms	Thema Serverplatform	C.01		Richtlijnen behoren te worden vastgesteld om de implementatie en beveiliging van servers en besturingssystemen te controleren waarbij de bevindingen tijdig aan het management worden gerapporteerd.	ISO 27002 2017: 10.10.2		Interne controle, Overleg bewijsstukken of Verklaring.						10	Uitval van systemen door configuratiefouten.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	176	De resultaten van de controle-activiteiten voldoen niet aan de verwachte eisen. Het management stuurt niet op afwijkingen.								Serverplatform
442	Beoordeling technische serveromgeving	Thema Serverplatform	C.02	Ja	Technische serveromgevingen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor servers en besturingssystemen.	BIO 2019: 18.2.3.		Overleg bewijsstukken en/of Verklaring.						10	Uitval van systemen door configuratiefouten.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	177	Kwetsbaarheden in technische serveromgevingen voor servers en besturingssystemen worden niet opgemerkt.								Serverplatform
443	O-maatregel. Beoordeling van technische naleving	BIO 2019	18.2.3.1	Ja	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.						6	Toegang tot informatie wordt geblokkeerd.	26	Misbruik van kwetsbaarheden in applicaties of hardware.											Serverplatform
444	Logbestanden beheerders	Thema Serverplatform	C.03		Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	BIO 2019: 12.4.3.		Overleg bewijsstukken en/of Verklaring.						20	Misbruik van speciale bevoegdheden.	21	Onterecht hebben van rechten.	178	Schade door het niet opmerkingen van fouten en/of onrechtmatigheden in het gebruik van waaronder ongeautoriseerde toegangspogingen tot technische componenten.								Serverplatform
446	Logging	Thema Serverplatform	C.04	Ja	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	BIO 2019: 12.4.1.		Overleg bewijsstukken en/of Verklaring.						14	Systemen worden niet gebruikt waarvoor ze bedoeld zijn.	40	Informatie voor het aanpakken van incidenten ontbreekt.	34	Foutieve informatie.	179	Ongeoorloofde acties op servers en besturingssystemen worden niet opgemerkt. Bij wel opmerken, is er geen bewijs voorhanden.						Serverplatform
449	O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.3	Ja	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, 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		Overleg bewijsstukken en/of Verklaring.						39	Incidenten worden niet tijdig opgepakt.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Herhaling van incidenten.								Serverplatform
450	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		Overleg bewijsstukken en/of Verklaring.						39	Incidenten worden niet tijdig opgepakt.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Herhaling van incidenten.								Serverplatform
451	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		Overleg bewijsstukken en/of Verklaring.						39	Incidenten worden niet tijdig opgepakt.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Herhaling van incidenten.								Serverplatform
461	Monitoring	Thema Serverplatform	C.05		De organisatie reviewt/analyseert regelmatig de logbestanden om onjuist gebruik en verdachte activiteiten op servers en besturingssystemen vast te stellen en bevindingen aan het management te rapporteren.	NCSC 2015: C.07		Overleg bewijsstukken en/of Verklaring.						14	Systemen worden niet gebruikt waarvoor ze bedoeld zijn.	20	Misbruik van speciale bevoegdheden.	180	Onvoldoende mogelijkheden om tijdig bij te sturen om organisatorisch en technisch te (blijven) voldoen aan de doelstellingen.								Serverplatform
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.						39	Incidenten worden niet tijdig opgepakt.	181	De beheersorganisatie is niet effectief ingericht waardoor servers en serverplatforms onvoldoende zijn beveiligd.										Serverplatform
713	Toegangbeveiligingsbeleid	Thema Toegangsbeveiliging	B.01		Een toegangsbeveiligingsbeleid behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en informatiebeveiligingseisen.	BIO 2019: 9.1.1, BIO2.0-opmaat: 5.15		Interne controle, Overleg bewijsstukken of Verklaring.						19	Misbruik van andermans identiteit.	20	Misbruik van speciale bevoegdheden.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	27	Misbruiken van zwakheden in netwerkbeveiliging.	54	Onvoldoende mogelijkheden om sturing te geven aan de effectieve en betrouwbare inrichting van toegangsbeveiligingsmaatregelen en het inrichten van de beheerorganisatie van de autorisatievoorzieningen en hierover verantwoordingrapportage te laten afgeven.				Toegangsbeveiliging
727	Eigenaarschap	Thema Toegangsbeveiliging	B.02		Het eigenaarschap en de verantwoordelijkheden voor logische toegangsbeveiligingssystemen en de verantwoordelijkheden voor fysieke toegangsbeveiligingssystemen behoren te zijn vastgelegd.	ISO 27002 2017: 8.1.1 ISO 27002 2017: 8.1.2 SoGP 2018: PM1.2		Interne controle, Overleg bewijsstukken of Verklaring.						2	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	12	Fouten als gevolg van wijzigingen in andere systemen.	14	Systemen worden niet gebruikt waarvoor ze bedoeld zijn.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	27	Misbruiken van zwakheden in netwerkbeveiliging.	55	Noodzakelijke beveiligingsacties blijven achterwege.		Toegangsbeveiliging
729	Beveiligingsfunctie	Thema Toegangsbeveiliging	B.03		Een gespecialiseerde beveiligingsfunctie dient te zijn vastgesteld die verantwoordelijk is voor het bevorderen van toegangsbeveiliging binnen de gehele organisatie.	SoGP 2018: SM2.1		Interne controle, Overleg bewijsstukken of Verklaring.						19	Misbruik van andermans identiteit.	20	Misbruik van speciale bevoegdheden.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	27	Misbruiken van zwakheden in netwerkbeveiliging.	56	Activiteiten over toegangsbeveiliging zijn ongecoördineerd, onjuist of niet tijdig uitgevoerd. Afwijkingen leiden niet tot corrigerende acties.				Toegangsbeveiliging
732	Cryptografie	Thema Toegangsbeveiliging	B.04	Ja	Ter bescherming van authenticatie-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		Interne controle, Overleg bewijsstukken of Verklaring.						35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	57	De vertrouwelijkheid en integriteit van data is niet garandeert.										Toegangsbeveiliging
733	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		Interne controle, Overleg bewijsstukken of Verklaring.						35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	31	Onveilig versturen van gevoelige informatie.										Toegangsbeveiliging
734	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		Interne controle, Overleg bewijsstukken of Verklaring.						35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	31	Onveilig versturen van gevoelige informatie.										Toegangsbeveiliging
742	Beveiligingsorganisatie	Thema Toegangsbeveiliging	B.05		De organisatie moet een beveiligingsorganisatie gedefinieerd hebben waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden (TVB) van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.	ISO 27001 2017: 5.3		Interne controle, Overleg bewijsstukken of Verklaring.						2	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	58	Het informatiebeveiliging sbeleid komt niet effectief tot uitvoering.										Toegangsbeveiliging

Nr	Naam Eis	Referentie brondocument:	Referentie code norm:	BIO-O-maatregel:	Samenvatting eis:	Gebaseerd op: (ISO27002-paragraaf, of ander framework)	Relevante standaard PToLU-lijst Forum Standaardisatie:	Verificatie methode(n):	Eis gevraagd J/N	Als Eis/Wens	Reden niet gevraagd/geeist	Weging in RFC	Toelichting:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Inkooponderdeel
746	Toegangsbeveiligingsarchitectuur	Thema Toegangsbeveiliging	B.06		De organisatie behoort met organisatorische eisen en wensen de technische inrichting beschreven te hebben en behoort in een toegangsbeveiligingsarchitectuur te zijn vastgelegd.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.						10	Uitval van systemen door configuratiefouten.	59	Er is onvoldoende beheersing in het autorisatie 'inrichtings- en beheerdomein'.									Toegangsbeveiliging
749	Registratieprocedure	Thema Toegangsbeveiliging	U.01	Ja	Een formele registratie- en afmeldprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	BIO 2019: 9.2.1 BIO2.0-opmaat: 5.16		Overleg bewijsstukken en/of Testen.						21	Onterecht hebben van rechten.	60	Er ontstaat een onbetrouwbaar registratiesysteem. Bewerkingen kunnen door onbevoegden plaatsvinden.									Toegangsbeveiliging
754	Toegangsverleningsprocedure	Thema Toegangsbeveiliging	U.02	Ja	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle type gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	BIO 2019: 9.2.2 BIO2.0-opmaat: 5.18		Overleg bewijsstukken en/of Testen.						21	Onterecht hebben van rechten.	61	Er is geen duidelijkheid over wie welke handelingen mag verrichten.									Toegangsbeveiliging
757	O-maatregel. Gebruikers toegang verlenen	BIO 2019	9.2.2.3	Ja	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Testen.						21	Onterecht hebben van rechten.										Toegangsbeveiliging
758	Inlogprocedure	Thema Toegangsbeveiliging	U.03	Ja	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	BIO 2019: 9.4.2 BIO2.0-opmaat: 8.5		Overleg bewijsstukken en/of Testen.						19	Misbruik van andermans identiteit.	20	Misbruik van speciale bevoegdheden.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	27	Misbruiken van zwakheden in netwerkbeveiliging.	62	Er is misbruik en verlies van gevoelige gegevens en beïnvloeding van beschikbaarheid van informatiesystemen.			Toegangsbeveiliging
760	O-maatregel. Beveiligde inlogprocedures	BIO 2019	9.4.2.2	Ja	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.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Testen.						21	Onterecht hebben van rechten.	27	Misbruiken van zwakheden in netwerkbeveiliging.									Toegangsbeveiliging
772	Autorisatieproces	Thema Toegangsbeveiliging	U.04		Een formeel autorisatieproces dient geïmplementeerd te zijn voor het beheersen van de toegangsrechten van alle medewerkers en externe gebruikers tot informatie en informatieverwerkende faciliteiten.	SoGP 2018: SA1.2.1		Overleg bewijsstukken en/of Testen.						19	Misbruik van andermans identiteit.	20	Misbruik van speciale bevoegdheden.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	27	Misbruiken van zwakheden in netwerkbeveiliging.	63	Onbevoegden hebben toegang tot informatie van de organisatie.			Toegangsbeveiliging
778	Wachtwoordenbeheer	Thema Toegangsbeveiliging	U.05	Ja	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.	BIO2.0-opmaat: 5.17 BIO 2019: 9.3.1, 9.4.3		Overleg bewijsstukken en/of Testen.						22	Slecht wachtwoordgebruik.	64	Bedrijfsbelangen lopen schade op.									Toegangsbeveiliging
779	O-maatregel. Geheime authenticatie-informatie gebruiken	BIO 2019	9.3.1.1	Ja	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Testen.						22	Slecht wachtwoordgebruik.										Toegangsbeveiliging
781	O-maatregel. Systeem voor wachtwoordbeheer	BIO 2019	9.4.3.2	Ja	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.).	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Testen.						19	Misbruik van andermans identiteit.	22	Slecht wachtwoordgebruik.									Toegangsbeveiliging
782	O-maatregel. Systeem voor wachtwoordbeheer	BIO 2019	9.4.3.3	Ja	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Testen.						19	Misbruik van andermans identiteit.	22	Slecht wachtwoordgebruik.									Toegangsbeveiliging
783	O-maatregel. Systeem voor wachtwoordbeheer	BIO 2019	9.4.3.4	Ja	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Testen.						19	Misbruik van andermans identiteit.	22	Slecht wachtwoordgebruik.									Toegangsbeveiliging
784	O-maatregel. Systeem voor wachtwoordbeheer	BIO 2019	9.4.3.5	Ja	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Testen.						19	Misbruik van andermans identiteit.	22	Slecht wachtwoordgebruik.									Toegangsbeveiliging
794	Speciale toegangsrechtenbeheer	Thema Toegangsbeveiliging	U.06	Ja	Het toewijzen en het gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	BIO 2019: 9.2.3, 9.4.1 BIO2.0-opmaat: 8.2		Interne controle, Overleg bewijsstukken of Verklaring.						20	Misbruik van speciale bevoegdheden.	65	Bedrijfsbelangen lopen schade op.									Toegangsbeveiliging
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.						19	Misbruik van andermans identiteit.	20	Misbruik van speciale bevoegdheden.	21	Onterecht hebben van rechten.						Toegangsbeveiliging
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.						21	Onterecht hebben van rechten.										Toegangsbeveiliging
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.						21	Onterecht hebben van rechten.										Toegangsbeveiliging
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.						20	Misbruik van speciale bevoegdheden.	21	Onterecht hebben van rechten.	66	Er treedt fraude of misbruik van bedrijfsmiddelen bij kritische of fraudegevoelige taken op. Informatie wordt opzettelijk of onopzettelijk gebruikt, gewijzigd of vernietigd.						Toegangsbeveiliging
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.						21	Onterecht hebben van rechten.	67	Onbevoegden misbruiken gegevens.									Toegangsbeveiliging
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.						21	Onterecht hebben van rechten.	68	Ongewenste wijzigingen worden in een informatiesysteem aangebracht.									Toegangsbeveiliging
813	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.						21	Onterecht hebben van rechten.										Toegangsbeveiliging
814	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		Overleg bewijsstukken en/of Testen.						21	Onterecht hebben van rechten.										Toegangsbeveiliging
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.						21	Onterecht hebben van rechten.	69	Er treedt vervuiling op bij het autorisatiebeheer, die mogelijk in onvoldoende mate of niet tijdig wordt gesignaleerd. Hierdoor krijgen onbevoegden toegang tot gegevens.									Toegangsbeveiliging
827	Fysieke toegangsbeveiliging	Thema Toegangsbeveiliging	U.11	Ja	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging.	BIO 2019: 11.1.2 BIO2.0-opmaat: 7.2		Overleg bewijsstukken en/of Testen.						19	Misbruik van andermans identiteit.	20	Misbruik van speciale bevoegdheden.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	27	Misbruiken van zwakheden in netwerkbeveiliging.	70	Onbevoegden brengen schade toe aan en verstoringen in de computerruimte en aan informatie in de Huisvesting-IV-			Toegangsbeveiliging
828	Fysieke toegangsbeveiliging	BIO 2019	11.1.2.1	Ja	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.						19	Misbruik van andermans identiteit.	20	Misbruik van speciale bevoegdheden.	70	Onbevoegden brengen schade toe aan en verstoringen in de computerruimte en aan informatie in de Huisvesting-IV-						Toegangsbeveiliging
833	Beoordelingsprocedure	Thema Toegangsbeveiliging	C.01		Om het gebruik van toegangsbeveiligingsvoorzieningen te (kunnen) controleren, behoren er procedures te zijn vastgesteld.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.						19	Misbruik van andermans identiteit.	20	Misbruik van speciale bevoegdheden.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	27	Misbruiken van zwakheden in netwerkbeveiliging.	71	Er zijn onvoldoende mogelijkheden om vast te stellen of de controle-activiteiten gestructureerd plaatsvinden.			Toegangsbeveiliging

Nr	Naam Eis	Referentie brondocument:	Referentie code norm:	BIO-O-maatregel:	Samenvatting eis:	Gebaseerd op: (ISO27002-paragraaf, of ander framework)	Relevante standaard PToLU-lijst Forum Standaardisatie:	Verificatie methode(n):	Eis gevraagd J/N	Als Eis/Wens	Reden niet gevraagd/geeist	Weging in RFC	Toelichting:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Inkooponderdeel
840	Logging en monitoring	Thema Toegangsbeveiliging	C.03	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.						39	Incidenten worden niet tijdig opgepakt.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Herhaling van incidenten.	73	Achteraf wordt niet de juiste actie ondernomen. Er wordt niet vastgesteld wie welke handelingen heeft uitgevoerd.					Toegangsbeveiliging
843	O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.3	Ja	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, 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.						39	Incidenten worden niet tijdig opgepakt.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Herhaling van incidenten.							Toegangsbeveiliging
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.						39	Incidenten worden niet tijdig opgepakt.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Herhaling van incidenten.							Toegangsbeveiliging
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.						39	Incidenten worden niet tijdig opgepakt.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Herhaling van incidenten.							Toegangsbeveiliging
862	Wet en Regelgeving	Thema Clouddiensten	B.01		Alle relevante wettelijke, statutaire, regelgevende, contractuele eisen en de aanpak van de CSP om aan deze eisen te voldoen behoren voor elke clouddienst en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	BIO 2019: 18.1.1.		Overleg bewijsstukken en/of Verklaring.						49	Niet beschikbaar zijn van diensten van derden.	36	Wetgeving over informatie in de cloud.	37	Buitenlandse wetgeving bij het bezoeken van een land.	38	Wetgeving over het gebruik van cryptografie.	204	Schade door wettelijke aansprakelijkheid.			Clouddiensten
866	Cloudbeveiligingsstrategie	Thema Clouddiensten	B.02		De CSP behoort een cloud-beveiligingsstrategie te hebben ontwikkeld die samenhangt met de strategische doelstelling van de CSP en die aantoonbaar de informatieveiligheid ondersteunt.	SoGP 2018: SG2.1		Overleg bewijsstukken en/of Verklaring.						1	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	3	Onvoldoende aandacht voor beveiliging binnen projecten.	12	Fouten als gevolg van wijzigingen in andere systemen.	5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	14	Systemen worden niet gebruikt waarvoor ze bedoeld zijn.	28	Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	Clouddiensten
867	Exit-strategie	Thema Clouddiensten	B.03		In de clouddienstenovereenkomst tussen de CSP en CSC behoort een exitstrategie te zijn opgenomen waarbij zowel een aantal bepalingen6 over exit zijn opgenomen, als een aantal condities6 die aanleiding kunnen geven tot een exit.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.						49	Niet beschikbaar zijn van diensten van derden.	50	Software wordt niet meer ondersteund door de uitgever.	51	Kwijtraken van belangrijke kennis bij niet beschikbaar zijn van medewerkers.	206	Het niet beschikken over een overeengekomen leidraad/globale manier van aanpak bij beëindiging van leverancierscontracten.					Clouddiensten
868	Clouddienstenbeleid	Thema Clouddiensten	B.04		De CSP behoort haar informatiebeveiligingsbeleid uit te breiden met een cloud-beveiligingsbeleid om de voorzieningen en het gebruik van cloudservices te adresseren.	ISO 27017 2015: 5.1.1		Overleg bewijsstukken en/of Verklaring.						1	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	3	Onvoldoende aandacht voor beveiliging binnen projecten.	6	Toegang tot informatie wordt geblokkeerd.	8	Aanvallen via systemen die niet in eigen beheer zijn.	5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	207	Onvoldoende mogelijkheid om sturing te geven aan inspanningen voor clouddiensten, waardoor deze niet of onvoldoende bijdragen aan de doelstellingen van de organisatie.	Clouddiensten
869	Transparantie	Thema Clouddiensten	B.05		De CSP voorziet de CSC in een systeembeschrijving waarin de clouddiensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geadresseerd.	BSI C5 2020: BC-01 BSI C5 2020: BC-05 BSI C5 2020: BC-06		Overleg bewijsstukken en/of Verklaring.						1	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	2	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	3	Onvoldoende aandacht voor beveiliging binnen projecten.	24	Onduidelijkheid over classificatie en bevoegdheden.	28	Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	208	De CSP kan levert een dienstverlening die niet of onvolledig is afgestemd op de behoefte van de CSC.	Clouddiensten
870	Risicomanagement	Thema Clouddiensten	B.06		De CSP behoort de organisatie en verantwoordelijkheden voor het risicomanagementproces voor de beveiliging van clouddiensten te hebben opgezet en onderhouden.	ISO 27005 2018: 7.4		Interne controle, Overleg bewijsstukken of Verklaring.						1	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	209	De getroffen beveiligingsmaatregelen liggen buiten de aanvaardbare grenzen. De clouddiensten worden onder- of overbeveiligd.									Clouddiensten
871	IT-functionaliteit	Thema Clouddiensten	B.07		IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketen van de CSP naar de CSC.	SoGP 2018: BC1.3		Overleg bewijsstukken en/of Verklaring.						17	Toelaten van externen in het pand of op het netwerk.	19	Misbruik van andermans identiteit.	20	Misbruik van speciale bevoegdheden.	21	Onterecht hebben van rechten.	24	Onduidelijkheid over classificatie en bevoegdheden.	210	IT-functionaliteiten zijn een zwakke schakel in de beveiliging.	Clouddiensten
872	Bedrijfscontinuïteitsmanagement	Thema Clouddiensten	B.08		De CSP behoort haar BCM-proces adequaat te hebben georganiseerd, waarbij de volgende aspecten zijn geadresseerd: verantwoordelijkheid voor BCM, beleid en procedures, bedrijfscontinuïteitsplanning, verificatie en updaten en computercentra.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.						49	Niet beschikbaar zijn van diensten van derden.	50	Software wordt niet meer ondersteund door de uitgever.	40	Informatie voor het aanpakken van incidenten ontbreekt.	43	Brand.	211	Het niet effectief reageren op het manifest worden van omvangrijke storingen en (on)bekende risico's (ramp/noodsituaties). De bedreiging wordt niet zo snel als mogelijk gestopt en de gevolgschade wordt niet zo veel als mogelijk beperkt.			Clouddiensten
873	Privacy en bescherming persoonsgegevens	Thema Clouddiensten	B.09		De CSP behoort, ter bescherming van bedrijfs- en persoonlijke data, beveiligingsmaatregelen te hebben getroffen vanuit verschillende dimensies: beveiligingsaspecten en stadia, toegang en privacy, classificatie/labelen, eigenaarschap en locatie.	ITU-T FG Cloud TR Part 5 2012: 8.5		Overleg bewijsstukken en/of Verklaring.						24	Onduidelijkheid over classificatie en bevoegdheden.	212	De bedrijfs- en persoonlijke data wordt onderbeveiligd.									Clouddiensten
874	Beveiligingsorganisatie	Thema Clouddiensten	B.10	Ja	De CSP behoort een beveiligingsfunctie te hebben benoemd en een beveiligingsorganisatie te hebben ingericht, waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.	CIP-netwerk, BIO 2019: 6.1.1.		Overleg bewijsstukken en/of Verklaring.						2	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	4	Medewerkers handelen onvoldoende naar hetgeen van hen verwacht wordt.	213	Het niet effectief tot uiting komen van het clouddienstenbeleid.							Clouddiensten
879	Clouddienstenarchitectuur	Thema Clouddiensten	B.11		De CSP heeft een actuele architectuur vastgelegd die voorziet in een raamwerk voor de onderlinge samenhang en afhankelijkheden van de IT-functionaliteiten.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.						17	Toelaten van externen in het pand of op het netwerk.	19	Misbruik van andermans identiteit.	20	Misbruik van speciale bevoegdheden.	21	Onterecht hebben van rechten.	24	Onduidelijkheid over classificatie en bevoegdheden.	214	Geen of onvoldoende sturing hebben op de clouddiensten. De werking van de clouddiensten is onbetrouwbaar.	Clouddiensten
880	Standaarden voor clouddiensten	Thema Clouddiensten	U.01		De CSP past aantoonbaar relevante, nationale standaarden en internationale standaarden toe voor de opzet en exploitatie van de diensten en de interactie met de CSC.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.						2	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	14	Systemen worden niet gebruikt waarvoor ze bedoeld zijn.	20	Misbruik van speciale bevoegdheden.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	20	Misbruik van speciale bevoegdheden.	215	Generieke risico's zijn niet of onvoldoende gemitigeerd.	Clouddiensten
881	Risico-assessment	Thema Clouddiensten	U.02		De CSP behoort een risico-assessment uit te voeren, bestaande uit een risico-analyse en risico-evaluatie met de criteria en de doelstelling voor clouddiensten van de CSP.	ISO 27005 2018: 8.1		Interne controle, Overleg bewijsstukken of Verklaring.						1	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	216	Geen of onvoldoende zicht hebben op de risico's die van invloed zijn op clouddiensten.									Clouddiensten
882	Bedrijfscontinuïteitsservices	Thema Clouddiensten	U.03		Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan continuïteitseisen te voldoen.	BIO 2019: 17.2.1.		Overleg bewijsstukken en/of Verklaring.						1	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	10	Uitval van systemen door configuratiefouten.	11	Uitval van systemen door softwarefouten.	12	Fouten als gevolg van wijzigingen in andere systemen.	40	Informatie voor het aanpakken van incidenten ontbreekt.	43	Brand.	Clouddiensten
883	Herstelfunctie voor data en clouddiensten	Thema Clouddiensten	U.04		De herstelfunctie van de data en clouddiensten, gericht op ondersteuning van bedrijfsprocessen, behoort te worden gefaciliteerd met infrastructuur en IT-diensten, die robuust zijn en periodiek worden getest.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.						49	Niet beschikbaar zijn van diensten van derden.	40	Informatie voor het aanpakken van incidenten ontbreekt.	10	Uitval van systemen door configuratiefouten.	11	Uitval van systemen door softwarefouten.	12	Fouten als gevolg van wijzigingen in andere systemen.	218	Overschrijden van het maximale dataverlies en/of uitvalsduur.	Clouddiensten

Nr	Naam Eis	Referentie brondocument:	Referentie code norm:	BIO-O-maatregel:	Samenvatting eis:	Gebaseerd op: (ISO27002-paragraaf, of ander framework)	Relevante standaard PToLU-lijst Forum Standaardisatie:	Verificatie methode(n):	Eis gevraagd J/N	Als Eis/Wens	Reden niet gevraagd/geeist	Weging in RFC	Toelichting:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Inkooponderdeel
884	Dataprotectie	Thema Clouddiensten	U.05		Data ('op transport', 'in verwerking' en 'in rust') met de classificatie BBN2 of hoger behoort te worden beschermd met cryptografische maatregelen en te voldoen aan Nederlandse wetgeving.	ISO 27040 2016: 6.3.2.1	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam) * STARTTLS en DANE (beveiligde mailserver-verbindingen) * DMARC+DKIM+SPF (anti-mailphishing/-spoofing) * Digikoppeling (beveiligde gegevensuitwisseling tussen systemen)	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.						38	Wetgeving over het gebruik van cryptografie.	219	Data met de classificatie BBN2 of hoger is onvoldoende beveiligd										Clouddiensten
885	Dataretentie en gegevensvernietiging	Thema Clouddiensten	U.06	Ja	Gearchiveerde data behoort gedurende de overeengekomen bewaartermijn, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integer te worden opgeslagen en op aanwijzing van de CSC/data-eigenaar te kunnen worden vernietigd.	CIP-netwerk, BIO 2019: 18.1.3.		Interne controle, Overleg bewijsstukken of Verklaring.						33	Informatieverlies door verlopen van houdbaarheid van opslagwijze.	220	De beschikbaarheid en integriteit van de data wordt aangetast gedurende archivering en langer archiveren dan noodzakelijk.										Clouddiensten
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.						33	Informatieverlies door verlopen van houdbaarheid van opslagwijze.	220	De beschikbaarheid en integriteit van de data wordt aangetast gedurende archivering en langer archiveren dan noodzakelijk.										Clouddiensten
887	Datascheiding	Thema Clouddiensten	U.07		CSC-gegevens behoren tijdens transport, bewerking en opslag duurzaam geïsoleerd te zijn van beheerfuncties en data van en andere dienstverlening aan andere CSC's, die de CSP in beheer heeft.	ISO 27040 2016: 7.7.4		Overleg bewijsstukken en/of Verklaring.						31	Onveilig versturen van gevoelige informatie.	32	Versturen van gevoelige informatie naar onjuiste persoon.	33	Informatieverlies door verlopen van houdbaarheid van opslagwijze.	34	Foutieve informatie.	35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	221	Andere CSC's en de CSP krijgen toegang tot de data of in beheer van de CSP en vice versa.	Clouddiensten
888	Scheiding dienstverlening	Thema Clouddiensten	U.08		De cloud-infrastructuur is zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten zijn gescheiden.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.						6	Toegang tot informatie wordt geblokkeerd.	8	Aanvallen via systemen die niet in eigen beheer zijn.	27	Misbruiken van zwakheden in netwerkbeveiliging.	222	Beïnvloeding of communicatie van data.					Clouddiensten
889	Malware-protectie	Thema Clouddiensten	U.09	Ja	Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers.	BIO 2019: 12.2.1.		Overleg bewijsstukken en/of Verklaring.						6	Toegang tot informatie wordt geblokkeerd.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	53	Verificatie op corrupte data(-bestanden) uit de keten.	223	Malware wordt niet opgespoord en aangetroffen malware wordt niet of voldoende hersteld.					Clouddiensten
895	Toegang IT-diensten en data	Thema Clouddiensten	U.10	Ja	Gebruikers behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn.	BIO 2019: 9.1.2.		Interne controle, Overleg bewijsstukken of Verklaring.						21	Onterecht hebben van rechten.	224	Misbruik en verlies van (gevoelige) gegevens										Clouddiensten
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.	* TLS, HTTPS en HSTS (beveiligde verbinding)	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.						31	Onveilig versturen van gevoelige informatie.	35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	225	Gegevens zijn tijdens transport via netwerken en opslag te benaderen voor onbevoegden							Clouddiensten
899	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		Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.						35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	31	Onveilig versturen van gevoelige informatie.										Clouddiensten
900	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		Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.						35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	31	Onveilig versturen van gevoelige informatie.										Clouddiensten
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.						35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.											Clouddiensten
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.						35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.											Clouddiensten
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.						27	Misbruiken van zwakheden in netwerkbeveiliging.	6	Toegang tot informatie wordt geblokkeerd.	8	Aanvallen via systemen die niet in eigen beheer zijn.	31	Onveilig versturen van gevoelige informatie.	32	Versturen van gevoelige informatie naar onjuiste persoon.	226	Data van of in beheer van de CSP komt via de koppelvlakken in handen van de CSP.	Clouddiensten
904	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.						8	Aanvallen via systemen die niet in eigen beheer zijn.											Clouddiensten
905	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.						39	Incidenten worden niet tijdig opgepakt.	39	Incidenten worden niet tijdig opgepakt.										Clouddiensten
906	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.						31	Onveilig versturen van gevoelige informatie.	32	Versturen van gevoelige informatie naar onjuiste persoon.										Clouddiensten
908	Service-orkestratie	Thema Clouddiensten	U.13		Service-orkestratie biedt coördinatie, aggregatie en samenstelling van de servicecomponenten van de cloud-service die aan de CSC wordt geleverd.	ISO 17789 2014: 9.2.3.4		Overleg bewijsstukken en/of Verklaring.						31	Onveilig versturen van gevoelige informatie.	32	Versturen van gevoelige informatie naar onjuiste persoon.	33	Informatieverlies door verlopen van houdbaarheid van opslagwijze.	34	Foutieve informatie.	35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	227	Niet of onvoldoende coördinatie, aggregatie en samenstelling van de servicecomponenten van de cloudservice.	Clouddiensten
909	Interoperabiliteit en portabiliteit	Thema Clouddiensten	U.14		Cloud-services zijn bruikbaar (interoperabiliteit) op verschillende ITplatforms en kunnen met standaarden verschillende IT-platforms met elkaar verbinden en data overdragen (portabiliteit) naar andere CSP's.	ISO 19941 2017: 7.1.7 BSI C5 2020: COS-02	* TLS, HTTPS en HSTS (beveiligde verbinding)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.						29	Informatie buiten de beschermde omgeving.	32	Versturen van gevoelige informatie naar onjuiste persoon.	49	Niet beschikbaar zijn van diensten van derden.	228	Cloudservices zijn niet toe te passen op andere IT-platforms en data kan niet naar een andere CSP worden overgedragen.					Clouddiensten
910	Logging en monitoring	Thema Clouddiensten	U.15	Ja	Logbestanden waarin gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiliging gebeurtenissen worden geregistreerd, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	BIO 2019: 12.4.1.		Interne controle, Overleg bewijsstukken of Verklaring.						39	Incidenten worden niet tijdig opgepakt.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Herhaling van incidenten.	73	Achteraf wordt niet de juiste actie ondernomen. Er wordt niet vastgesteld wie welke handelingen heeft uitgevoerd.	229	Afwijkingen van normaal gedrag zijn niet zichtbaar en niet te onderzoeken en herstelacties kunnen niet tijdig worden genomen.			Clouddiensten
913	O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.3	Ja	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, 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.						39	Incidenten worden niet tijdig opgepakt.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Herhaling van incidenten.									Clouddiensten

Nr	Naam Eis	Referentie brondocument:	Referentie code norm:	BIO-O-maatregel:	Samenvatting eis:	Gebaseerd op: (ISO27002-paragraaf, of ander framework)	Relevante standaard PToLU-lijst Forum Standaardisatie:	Verificatie methode(n):	Eis gevraagd J/N	Als Eis/Wens	Reden niet gevraagd/geeist	Weging in RFC	Toelichting:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Mitigeert risico nummer:	Mitigeert risico omschrijving:	Inkooponderdeel
914	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.						39	Incidenten worden niet tijdig opgepakt.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Herhaling van incidenten.							Clouddiensten
915	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.						39	Incidenten worden niet tijdig opgepakt.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Herhaling van incidenten.							Clouddiensten
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.						10	Uitval van systemen door configuratiefouten.	19	Misbruik van andermans identiteit.	20	Misbruik van speciale bevoegdheden.	22	Slecht wachtwoordgebruik.	31	Onveilig versturen van gevoelige informatie.	32	Versturen van gevoelige informatie naar onjuiste persoon.	Clouddiensten
917	Multi-tenantarchitectuur	Thema Clouddiensten	U.17		Bij multi-tenancy wordt de CSC-data binnen clouddiensten, die door meerdere CSC's worden afgenomen, in rust versleuteld en gescheiden verwerkt op gehardende (virtuele) machines	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.						31	Onveilig versturen van gevoelige informatie.	35	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	231	Geen of onvoldoende sturing hebben							Clouddiensten
918	Servicemanagementbeleid en evaluatierichtlijn	Thema Clouddiensten	C.01		De CSP heeft voor clouddiensten een servicemanagementbeleid geformuleerd met daarin richtlijnen voor de beheersingsprocessen, controleactiviteiten en rapportages.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.						1	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	3	Onvoldoende aandacht voor beveiliging binnen projecten.	5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	8	Aanvallen via systemen die niet in eigen beheer zijn.	5	Onvoldoende aandacht voor beveiliging bij softwareontwikkeling.	232	De resultaten van controle-activiteiten uitgevoerd op clouddiensten voldoet niet aan de gestelde eisen.	Clouddiensten
919	Risico-control	Thema Clouddiensten	C.02		Risicomanagement en het risico-assessmentproces behoren continu te worden gemonitord en gereviewd en zo nodig te worden verbeterd.	ISO 27005 2018: 12.1 ISO 27005 2018: 12.2		Overleg bewijsstukken en/of Verklaring.						1	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	40	Informatie voor het aanpakken van incidenten ontbreekt.	233	Het niet of te laat anticiperen op risicofactoren die van invloed zijn op de uitkomst van de risicoassessment.							Clouddiensten
920	Compliance en assurance	Thema Clouddiensten	C.03	Ja	De CSP behoort regelmatig de naleving van de cloudbeveiligingsovereenkomsten op compliancy te beoordelen, jaarlijks een assurance-verklaring aan de CSC uit te brengen en te zorgen voor onderlinge aansluiting van de resultaten uit deze twee exercities.	BIO 2019: 5.1.2, 18.2.1, 18.2.2, 18.2.3.		Overleg bewijsstukken en/of Verklaring.						1	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	234	Het ongecontroleerd afwijken van hetgeen gesteld is in wet- en regelgeving, het beveiligingsbeleid, de richtlijnen en de procedures en geen zekerheid hebben over het ingevoerde beveiligingsniveau.									Clouddiensten
922	O-maatregel. Onafhankelijke beoordeling van informatiebeveiliging	BIO 2019	18.2.1.1	Ja	Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.						1	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	2	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.								Clouddiensten
923	O-maatregel. Onafhankelijke beoordeling van informatiebeveiliging	BIO 2019	18.2.1.2	Ja	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.						1	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	2	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.								Clouddiensten
925	O-maatregel. Beoordeling van technische naleving	BIO 2019	18.2.3.1	Ja	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.						6	Toegang tot informatie wordt geblokkeerd.	26	Misbruik van kwetsbaarheden in applicaties of hardware.								Clouddiensten
926	Technische kwetsbaarhedenbeheer	Thema Clouddiensten	C.04	Ja	Informatie over technische kwetsbaarheden van gebruikte informatiesystemen behoort tijdig te worden verkregen; de blootstelling aan dergelijke kwetsbaarheden dienen te worden geëvalueerd en passende maatregelen dienen te worden genomen om het risico dat ermee samenhangt aan te pakken.	BIO 2019: 12.6.1.	STIX en TAXII (Uitwisseling van cyberdreigingsinformatie)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.						6	Toegang tot informatie wordt geblokkeerd.	26	Misbruik van kwetsbaarheden in applicaties of hardware.	235	Een technische kwetsbaarheid wordt niet of niet tijdig ontdekt							Clouddiensten
928	Security-monitoringsrapportage	Thema Clouddiensten	C.05		De performance van de informatiebeveiliging van de cloud-omgeving behoort regelmatig te worden gemonitord en hierover behoort tijdig te worden gerapporteerd aan verschillende stakeholders.	ISO 27002 2017:12.4 SoGP 2018: SI2.1		Overleg bewijsstukken en/of Verklaring.						39	Incidenten worden niet tijdig opgepakt.	41	Herhaling van incidenten.	236	Misbruik van de performance van informatiebeveiliging van de cloud-omgeving							Clouddiensten
929	Beheersorganisatie clouddiensten	Thema Clouddiensten	C.06		De CSP heeft een beheersorganisatie ingericht waarin de processtructuur en de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen zijn vastgesteld.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.						1	Gebrek aan sturing op informatiebeveiliging vanuit de directie.	2	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.	21	Onterecht hebben van rechten.	237	De cloudiensten verlopen niet zoals noodzakelijk is.					Clouddiensten