

Inkooponderdelen	Clouddiensten
Procesels	nee
Producteis	ja
Eis voor de opdrachtgever	nee
Eis voor de opdrachtnemer	ja
Ook eisen meegeven die alleen te maken hebben met schaalgrootte	nee
Basispakket	ja
Privacy-supplement	nee
Toon B10-O maatregelen BBN1	ja
Toon B10-O maatregelen BBN2	nee
Toon ABDO-eisen TB4	nee
Toon ABDO-eisen TB3	nee
Toon ABDO-eisen TB2	nee
Toon ABDO-eisen TB1	nee
Aantal geselecteerde eisen	27

Samengesteld door	<naam>
Organisatie	<afdeling, afligingsie>
	<vrije tekst>
Datum	28-03-2025

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 substitoot voor eigen risicoafweging.

Nr	Naam Eis	Referentie bronndocument	Referentie code norm	BIO-O-maatregel	Samenvatting eis:	Gebaseerd op: (ISO 27002-paragraaf, of ander framework)	Relevante standaard PTOLU-Bijst Norm Standaardisatie:	Verificatie methode(n):	Eis gevraagd /N	Als Eis/Wens	Reden niet gevraagd /geest	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
865	Transparantie	Thema Clouddiensten	8.05		De CSP voorziet de CSC in een systembeschrijving waarin de clouddiensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geïmpliceerd.	BSI CS 2020: BC-01 BSI CS 2020: BC-05 BSI CS 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 beveiligingsniveau.	28	Onvoldoende aandacht voor beveiliging bij uitbesteding van werkzaamheden.	208	De CSP kan leverancier niet of onvoldoende afstemmen op de behoeften van de CSP.	Clouddiensten		
871	IT-functionaliteit	Thema Clouddiensten	8.07		IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systemen 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 beveiligingsniveau.	210	IT-functionaliteiten zijn een zwakte schakel in de beveiliging.	Clouddiensten		
873	Privacy en bescherming persoonsgegevens	Thema Clouddiensten	8.09		De CSP behoort, ter bescherming van bedrijfs- en persoonlijke data, beveiligingsmaatregelen te hebben getroffen vanuit verschillende dimensies: beveiligingsaspecten en data, toegang en privacy, classificatie, beheer, opvoer, verspreiding en lokale.	ITU-T FG Cloud TR Part 5 2012: 8.5		Overleg bewijsstukken en/of Verklaring.						24	Onduidelijkheid over classificatie en beveiligingsniveau.	212	De bedrijfs- en persoonlijke data wordt onbeveiligd.									Clouddiensten		
874	Cloudstendarchitectuur	Thema Clouddiensten	8.11		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 beveiligingsniveau.	214	Geen of onvoldoende sturing hebben op de clouddiensten. De werking van de clouddiensten is onbetrouwbare.	Clouddiensten		
882	Bedrijfscontinuïteitsservices	Thema Clouddiensten	U.03		Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan continuïteitsdoelen 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 aangaan van incidenten ontbreekt.	43	Brand.	Clouddiensten		
883	Herstefunctie voor data en clouddiensten	Thema Clouddiensten	U.04		De herstefunctie 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	Het beschikbaar zijn van diensten van derden.	40	Informatie voor het aangaan 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	Overstrijken van het maximale datalevensduur en/of uitvalduur.	Clouddiensten		
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 worden aan Nederlandse wetgeving.	ISO 27040 2016: 6.3.2.1		Interne controle, Overleg bewijsstukken of Verklaring.						38	Wetgeving over het gebruik van cryptografie.	219	Data met de classificatie BBN2 of hoger is onvoldoende beveiligd.									Clouddiensten		
885	Dataresistentie en gegevensvermogen	Thema Clouddiensten	U.06	Ja	Gearchiverde data behoort gedurende de overeengekomen bewaartijd, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integre te worden opgeslagen en op aanvraag van de CSC/data-gebruiker 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		
887	Dataislanding	Thema Clouddiensten	U.07		CSC-gegevens behoren tijdens transport, bewaking 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 naar onjuiste persoon.	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 die 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			
890	O-maatregel, Beheersmaatregelen tegen malware	BIO 2019	12.2.1.1	Ja	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.						7	Netwerkdiensten raken overbelast.	14	Medewerkers handelen onbewust en/of onbekwaam fout. Dit zorgt voor schade.	31	Onveilig versturen van gevoelige informatie.							Clouddiensten		
891	O-maatregel, Beheersmaatregelen tegen malware	BIO 2019	12.2.1.2	Ja	Gebruikers zijn voorgedicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.						4	Medewerkers handelen onbewust en/of onbekwaam fout. Dit zorgt voor schade.	32	Misbruik van kwetsbaarheden in applicaties of hardware.									Clouddiensten		
892	O-maatregel, Beheersmaatregelen tegen malware	BIO 2019	12.2.1.3	Ja	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.						6	Toegang tot informatie wordt geblokkeerd.	26	Misbruik van kwetsbaarheden in applicaties of hardware.									Clouddiensten		
893	O-maatregel, Beheersmaatregelen tegen malware	BIO 2019	12.2.1.4	Ja	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: (a) Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen. (b) Bijlagen en downloads vóór gebruik.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.						6	Toegang tot informatie wordt geblokkeerd.	26	Misbruik van kwetsbaarheden in applicaties of hardware.									Clouddiensten		
894	O-maatregel, Beheersmaatregelen tegen malware	BIO 2019	12.2.1.5	Ja	De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op malwares, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	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		
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		
896	O-maatregel, Toegang tot netwerken en netwerkdiensten	BIO 2019	9.1.2.1	Ja	Alle fysieke/hetnetwerkd apparatuur kan toegang krijgen tot een vertrouwde zone.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.						21	Onterecht hebben van rechten.												Clouddiensten	

O-maatregel. Toegang tot netwerken 802 en netwerkdiensten	BIO 2019	9.1.2.2	Ja	Gebrowsers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.												21	Onterecht hebben van rechten.		Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.	35	Gegevens zijn tijdens transport via netwerken en opslag te benaderen voor onbevoegden.						Clouddiensten	
898 Cryptoservices	Thema Clouddiensten	U.11	Ja	Goedkope data van CSC's behooft 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		225						Clouddiensten		
903 Koppellinies	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 netwerkverbinding.	6	Toegang tot informatie wordt geblokkeerd.	8	Aanvallen via systemen die niet in eigen beheer zijn.	31	Onveilig versturen van gevoelige informatie naar onjuiste persoon.	32	Vernietiging van gegevens	226	Data van of in beheer van de CSP komt via de koppelvlakken in handen van de CSP.	Clouddiensten
O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.4	Ja	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en hierop te reageren.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.												7	Netwerkdiensten raken overbelast.	8	Aanvallen via systemen die niet in eigen beheer zijn.							Clouddiensten		
909 Interoperabiliteit en portabiliteit	Thema Clouddiensten	U.14		Cloud-services zijn bruikbaar (interoperabiliteit) op verschillende IT-platforms en kunnen met standaard protocollen op andere IT-systemen geïmporteerd worden. Verschillen tussen platformen moeten worden overgenomen (portabiliteit) naar andere CSP's.	ISO 19941-2017: 7.1.7 BSI CS 2020; COS-Q2	* 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 informatiebeveiligingsgebeurtenissen worden geregistreerd, behoren te worden gemaakt, bewaard en regelmatig te worden gecontroleerd.	BIO 2019: 12.4.1.	Interne controle, Overleg bewijsstukken of Verklaring.												39	Incidenten worden niet tijdig opgespoord.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Hervaling 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
O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.1	Ja	Een logreguleert bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herstellen tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handling; (e) een datum en tijdstip van de gebeurtenis.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.												39	Incidenten worden niet tijdig opgespoord.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Hervaling van incidenten.						Clouddiensten	
O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.2	Ja	Een logreguleert bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	Direct op BIO 2019 gebaseerd	Interne controle, Overleg bewijsstukken of Verklaring.												39	Incidenten worden niet tijdig opgespoord.	40	Informatie voor het aanpakken van incidenten ontbreekt.	41	Hervaling van incidenten.						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 geschieden verwerkt op geharde (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 onvolledige storing hebben						Clouddiensten	