**Excel Export ICO Wizard tbv Inkoopafdeling/opdrachtgever/budgethouder**

| | |
|---|---|
| **Inkooponderdelen** | Clouddiensten |
| **Proceseis** | ja |
| **Producteis** | ja |
| **Eis voor de opdrachtgever** | nee |
| **Eis voor de opdrachtnemer** | ja |
| **Ook eisen meegeven die alleen te maken hebben met schaalgrootte** | ja |
| **Basispakket** | ja |
| **Privacy-supplement** | ja |
| **Toon BIO-O maatregelen BBN1** | ja |
| **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** | 90 |

| | |
|---|---|
| **Samengesteld door** | <naam> |
| **Organisatie** | <afdeling, affiliatie> |
| | <vrije tekst> |
| | |
| **Datum** | 2-10-2023 |

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: |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 749 | 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. | | | | | |
| 753 | 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. | | | | | |
| 754 | 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. | | | | | |
| 755 | 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. | | | | | |
| 756 | 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. | | | | | |
| 757 | 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. | | | | | |
| 758 | 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. | | | | | |
| 759 | 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. | | | | | |
| 760 | 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. | | | | | |

| Nr | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 749 | 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 |
| 753 | 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 |
| 754 | 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 |
| 755 | 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 |
| 756 | 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 |
| 757 | 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 |
| 758 | 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 |
| 759 | 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 |
| 760 | 24 | Onduidelijkheid over classificatie en bevoegdheden. | 212 | De bedrijfs- en persoonlijke data wordt onderbeveiligd. | | | | | | | | | 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: |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 761 | 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. | | | | | |
| 762 | O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging | BIO 2019 | 6.1.1.1 | Ja | De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie. | Direct op BIO 2019 gebaseerd | | Overleg bewijsstukken en/of Verklaring. | | | | | |
| BIO | O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging | BIO 2019 | 6.1.1.2 | Ja | De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten. | Direct op BIO 2019 gebaseerd | | Overleg bewijsstukken en/of Verklaring. | | | | | |
| BIO | O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging | BIO 2019 | 6.1.1.3 | Ja | De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd. | Direct op BIO 2019 gebaseerd | | Overleg bewijsstukken en/of Verklaring. | | | | | |
| BIO | O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging | BIO 2019 | 6.1.1.4 | Ja | Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel. | Direct op BIO 2019 gebaseerd | | Overleg bewijsstukken en/of Verklaring. | | | | | |
| 763 | 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. | | | | | |
| 764 | 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. | | | | | |
| 765 | 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. | | | | | |
| 766 | 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. | | | | | |
| 767 | 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. | | | | | |

| Nr | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 761 | 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 |
| 762 | 2 | Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet. | 4 | Medewerkers handelen onvoldoende naar hetgeen van hen verwacht wordt. | | | | | | | | | Clouddiensten |
| BIO | 2 | Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet. | 4 | Medewerkers handelen onvoldoende naar hetgeen van hen verwacht wordt. | | | | | | | | | Clouddiensten |
| BIO | 2 | Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet. | 4 | Medewerkers handelen onvoldoende naar hetgeen van hen verwacht wordt. | | | | | | | | | Clouddiensten |
| BIO | 2 | Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet. | 4 | Medewerkers handelen onvoldoende naar hetgeen van hen verwacht wordt. | | | | | | | | | Clouddiensten |
| 763 | 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 |
| 764 | 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 |
| 765 | 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 |
| 766 | 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 |
| 767 | 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: |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 768 | 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)<br>* DNSSEC (ondertekende domeinnaam)<br>* STARTTLS en DANE (beveiligde mailserver-verbindingen)<br>* DMARC+DKIM+SPF (anti-mailphishing/-spoofing)<br>* Digikoppeling (beveiligde gegevensuitwisseling tussen systemen) | Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl. | | | | | |
| 769 | 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. | | | | | |
| BIO | 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. | | | | | |
| 770 | 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. | | | | | |
| 771 | 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. | | | | | |
| 772 | 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. | | | | | |
| BIO | 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. | | | | | |
| BIO | O-maatregel. Beheersmaatregelen tegen malware | BIO 2019 | 12.2.1.2 | Ja | Gebruikers zijn voorgelicht 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. | | | | | |
| BIO | 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. | | | | | |
| BIO | 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. | | | | | |
| 773 | O-maatregel. Beheersmaatregelen tegen malware | BIO 2019 | 12.2.1.5 | Ja | De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie. | Direct op BIO 2019 gebaseerd | | Overleg bewijsstukken en/of Verklaring. | | | | | |
| 774 | 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. | | | | | |

| Nr | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 768 | 38 | Wetgeving over het gebruik van cryptografie. | 219 | Data met de classificatie BBN2 of hoger is onvoldoende beveiligd | | | | | | | | | Clouddiensten |
| 769 | 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 |
| BIO | 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 |
| 770 | 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 |
| 771 | 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 |
| 772 | 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 |
| BIO | 7 | Netwerkdiensten raken overbelast. | 14 | Systemen worden niet gebruikt waarvoor ze bedoeld zijn. | 31 | Onveilig versturen van gevoelige informatie. | | | | | | | Clouddiensten |
| BIO | 4 | Medewerkers handelen onvoldoende naar hetgeen van hen verwacht wordt. | 82 | Schade door onbewust en/of onbekwaam fout handelen van medewerkers. | | | | | | | | | Clouddiensten |
| BIO | 6 | Toegang tot informatie wordt geblokkeerd. | 26 | Misbruik van kwetsbaarheden in applicaties of hardware. | | | | | | | | | Clouddiensten |
| BIO | 6 | Toegang tot informatie wordt geblokkeerd. | 26 | Misbruik van kwetsbaarheden in applicaties of hardware. | | | | | | | | | Clouddiensten |
| 773 | 6 | Toegang tot informatie wordt geblokkeerd. | 26 | Misbruik van kwetsbaarheden in applicaties of hardware. | | | | | | | | | Clouddiensten |
| 774 | 21 | Onterecht hebben van rechten. | 224 | Misbruik en verlies van (gevoelige) gegevens | | | | | | | | | 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: |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 775 | O-maatregel. Toegang tot netwerken en netwerkdiensten | BIO 2019 | 9.1.2.1 | Ja | Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone. | Direct op BIO 2019 gebaseerd | | Interne controle, Overleg bewijsstukken of Verklaring. | | | | | |
| BIO | O-maatregel. Toegang tot netwerken en netwerkdiensten | BIO 2019 | 9.1.2.2 | Ja | Gebruikers 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. | | | | | |
| 776 | 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. | | | | | |
| 777 | 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. | | | | | |
| BIO | 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. | | | | | |
| 778 | 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. | | | | | |
| BIO | 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. | | | | | |
| 779 | 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. | | | | | |
| 780 | 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. | | | | | |
| 781 | 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. | | | | | |
| 782 | 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. | | | | | |
| 783 | 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. | | | | | |

| Nr | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 775 | 21 | Onterecht hebben van rechten. | | | | | | | | | | | Clouddiensten |
| BIO | 21 | Onterecht hebben van rechten. | | | | | | | | | | | Clouddiensten |
| 776 | 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 |
| 777 | 35 | Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen. | 31 | Onveilig versturen van gevoelige informatie. | | | | | | | | | Clouddiensten |
| BIO | 35 | Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen. | 31 | Onveilig versturen van gevoelige informatie. | | | | | | | | | Clouddiensten |
| 778 | 35 | Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen. | | | | | | | | | | | Clouddiensten |
| BIO | 35 | Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen. | | | | | | | | | | | Clouddiensten |
| 779 | 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 |
| 780 | 8 | Aanvallen via systemen die niet in eigen beheer zijn. | | | | | | | | | | | Clouddiensten |
| 781 | 39 | Incidenten worden niet tijdig opgepakt. | 39 | Incidenten worden niet tijdig opgepakt. | | | | | | | | | Clouddiensten |
| 782 | 31 | Onveilig versturen van gevoelige informatie. | 32 | Versturen van gevoelige informatie naar onjuiste persoon. | | | | | | | | | Clouddiensten |
| 783 | 7 | Netwerkdiensten raken overbelast. | 8 | Aanvallen via systemen die niet in eigen beheer zijn. | | | | | | | | | 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: |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 784 | 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. | | | | | |
| 785 | 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. | | | | | |
| 786 | 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. | | | | | |
| 731 | O-maatregel. Gebeurtenissen registreren | BIO 2019 | 12.4.1.1 | Ja | Een logregel bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis. | Direct op BIO 2019 gebaseerd | | Interne controle, Overleg bewijsstukken of Verklaring. | | | | | |
| 732 | O-maatregel. Gebeurtenissen registreren | BIO 2019 | 12.4.1.2 | Ja | Een logregel 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. | | | | | |
| BIO | 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. | | | | | |
| BIO | 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. | | | | | |
| BIO | 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. | | | | | |
| 788 | 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. | | | | | |
| 789 | 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. | | | | | |
| 790 | 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. | | | | | |

| Nr | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 784 | 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 |
| 785 | 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 |
| 786 | 39 | Incidenten worden niet tijdig opgepakt. | 40 | Informatie voor het aanpakken van incidenten ontbreekt. | 41 | Herhaling van incidenten. | 73 | Zonder vastlegging en bewaking kan achteraf niet de juiste actie worden ondernomen en niet worden 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 |
| 731 | 39 | Incidenten worden niet tijdig opgepakt. | 40 | Informatie voor het aanpakken van incidenten ontbreekt. | 41 | Herhaling van incidenten. | | | | | | | Clouddiensten |
| 732 | 39 | Incidenten worden niet tijdig opgepakt. | 40 | Informatie voor het aanpakken van incidenten ontbreekt. | 41 | Herhaling van incidenten. | | | | | | | Clouddiensten |
| BIO | 39 | Incidenten worden niet tijdig opgepakt. | 40 | Informatie voor het aanpakken van incidenten ontbreekt. | 41 | Herhaling van incidenten. | | | | | | | Clouddiensten |
| BIO | 39 | Incidenten worden niet tijdig opgepakt. | 40 | Informatie voor het aanpakken van incidenten ontbreekt. | 41 | Herhaling van incidenten. | | | | | | | Clouddiensten |
| BIO | 39 | Incidenten worden niet tijdig opgepakt. | 40 | Informatie voor het aanpakken van incidenten ontbreekt. | 41 | Herhaling van incidenten. | | | | | | | Clouddiensten |
| 788 | 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 |
| 789 | 31 | Onveilig versturen van gevoelige informatie. | 35 | Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen. | 231 | Geen of onvoldoende sturing hebben | | | | | | | Clouddiensten |
| 790 | 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 |

| 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: |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 791 | 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. | | | | | |
| 792 | 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. | | | | | |
| BIO | O-maatregel. Beoordeling van het informatiebeveiligingsbeleid | BIO 2019 | 5.1.2.1 | Ja | Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P en C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld. | Direct op BIO 2019 gebaseerd | | Overleg bewijsstukken en/of Verklaring. | | | | | |
| BIO | 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. | | | | | |
| BIO | 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. | | | | | |
| BIO | O-maatregel. Naleving van beveiligingsbeleid en -normen | BIO 2019 | 18.2.2.1 | Ja | In de P en C cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording. | Direct op BIO 2019 gebaseerd | | Overleg bewijsstukken en/of Verklaring. | | | | | |
| BIO | 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. | | | | | |
| 793 | 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. | | | | | |
| 794 | O-maatregel. Beheer van technische kwetsbaarheden | BIO 2019 | 12.6.1.1 | Ja | Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen. | Direct op BIO 2019 gebaseerd | | Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl. | | | | | |

| Nr | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 791 | 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 |
| 792 | 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 |
| BIO | 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 |
| BIO | 1 | Gebrek aan sturing op informatiebeveiliging vanuit de directie. | 2 | Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet. | | | | | | | | | Clouddiensten |
| BIO | 1 | Gebrek aan sturing op informatiebeveiliging vanuit de directie. | 2 | Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet. | | | | | | | | | Clouddiensten |
| BIO | 1 | Gebrek aan sturing op informatiebeveiliging vanuit de directie. | 2 | Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet. | | | | | | | | | Clouddiensten |
| BIO | 6 | Toegang tot informatie wordt geblokkeerd. | 26 | Misbruik van kwetsbaarheden in applicaties of hardware. | | | | | | | | | Clouddiensten |
| 793 | 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 |
| 794 | 6 | Toegang tot informatie wordt geblokkeerd. | 26 | Misbruik van kwetsbaarheden in applicaties of hardware. | | | | | | | | | 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: |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 795 | 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. | | | | | |
| 796 | 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. | | | | | |
| 797 | Testdata | Privacy-supplement Applicatieontwikkeling Algemeen | APO P.01 | | Waar mogelijk wordt als testdata gebruik gemaakt van kunstmatig gegenereerde persoonsgegevens of fictieve data, wanneer op basis van de resultaten van een risico-analyse gebruik gemaakt wordt van persoonsgegevens, worden passende maatregelen ter bescherming van de persoonsgegevens genomen. | ISO 27701 2019: 6.11.3.1, NEN 7510 2017: 14.3.1 AVG: art. 4.2, 6, 15, 25.1 en 32 | | Overleg bewijsstukken en/of verklaring | | | | | |
| 798 | Privacy by Default binnen applicaties | Privacy-supplement SSD | SSD P.01 | | De applicatie vraagt bij elke verzameling van persoonsgegevens vrijelijk en ondubbelzinnig toestemming aan betrokkene, waarvan de persoonsgegevens worden verwerkt, om de gegevens te mogen verwerken, waarbij standaard zo min mogelijk persoonsgegevens worden verwerkt | CIP De Privacy Baseline 2020: U.05, AVG: art. 25, Wpg Art 4b lid 1a en lid 1b | | Testen | | | | | |
| 799 | Correcte en gewenste verwerking met applicaties | Privacy-supplement SSD | SSD P.02 | | De applicatie biedt de mogelijkheid om op aangeven van betrokkene, waarvan de persoonsgegevens worden verwerkt, controle te houden over de gegevens en de verwerking ervan, zodat de juistheid en nauwkeurigheid van de gegevens kan worden gewaarborgd en de verwerking ervan kan worden gecorrigeerd, gestaakt of overgedragen. | AVG: art. 7, 11, 12, 16, 17, 18, 19, 20, 21, 22 en 23, Wpg: Art 27 Art 28 | | Overleg bewijsstukken en/of verklaring en testen | | | | | |
| 800 | Informatieverstrekking aan betrokkene met applicaties | Privacy-supplement SSD | SSD P.03 | | Om de gegevens te mogen verwerken wordt de betrokkene, waarvan de persoonsgegevens worden verwerkt, geïnformeerd betreffende welke verwerking (van de persoonsgegevens) plaatsvindt en krijgt deze betrokkene een waarschuwing bij het verkrijgen van toegang tot bijzondere persoonsgegevens. | CIP De Privacy Baseline 2020: U.05, AVG: art. 14, AVG: overweging 60, Wpg: Art 24a lid 1 t/m 4, art 24b | | Overleg bewijsstukken en/of verklaring en testen | | | | | |
| 801 | Toegang op taakniveau met applicaties | Privacy-supplement SSD | SSD P.04 | | Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar. | CIP-netwerk, Wpg: Art 6 lid 1 t/m 6 Art 6a | | Overleg bewijsstukken en/of verklaring | | | | | |
| 802 | Logging met applicaties | Privacy-supplement SSD | SSD P.05 | | De applicatie behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast. | AVG: art. 5 lid 2 en art. 33 lid 5, Wpg Art. 32a | | Overleg bewijsstukken en/of verklaring | | | | | |
| 803 | Dataminimalisatie binnen applicaties | Privacy-supplement SSD | SSD P.06 | | De organisatie behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn. | AVG: art. 6 lid 1, Wpg art 3 lid 2 en 5, Art 4 lid 2, Art 8 lid 1, 2, 6, Art 9 lid 4, Art 14 | | Overleg bewijsstukken en/of verklaring | | | | | |
| 804 | Generalisatie binnen applicaties | Privacy-supplement SSD | SSD P.07 | | De applicatie behoort, indien de functionele eisen aan de applicatie van de opdrachtgever dit toelaten, gegeneraliseerde gegevens te gebruiken. | ENISA strategie (January 12, 2015 ) 'generaliseren' | | Overleg bewijsstukken en/of verklaring | | | | | |
| 805 | Scheiden binnen applicaties | Privacy-supplement SSD | SSD P.08 | | Iedere applicatie kent een duidelijk verwerkingsdoel, waarbij de scheiding van de verwerking gerealiseerd is op het niveau van de applicatie, de transportpaden, de middleware, de opslagvoorzieningen en is hierop getoetst. | AVG: art. 6 lid 1, NISA strategie (January 12, 2015 ) 'scheiden' | | Overleg bewijsstukken en/of verklaring | | | | | |

| Nr | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 795 | 39 | Incidenten worden niet tijdig opgepakt. | 41 | Herhaling van incidenten. | 236 | Misbruik van de performance van informatiebeveiliging van de cloud-omgeving | | | | | | | Clouddiensten |
| 796 | 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 |
| 797 | | | | | | | | | | | | | Clouddiensten |
| 798 | | | | | | | | | | | | | Clouddiensten |
| 799 | | | | | | | | | | | | | Clouddiensten |
| 800 | | | | | | | | | | | | | Clouddiensten |
| 801 | | | | | | | | | | | | | Clouddiensten |
| 802 | | | | | | | | | | | | | Clouddiensten |
| 803 | | | | | | | | | | | | | Clouddiensten |
| 804 | | | | | | | | | | | | | Clouddiensten |
| 805 | | | | | | | | | | | | | 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: |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 806 | Verbergen binnen applicaties | Privacy-supplement SSD | SSD P.09 | | Een applicatie, en iedere Functie binnen deze applicatie, heeft een duidelijk omschreven verwerkingsdoel, zodat bij iedere doorgifte, verwerking door de applicatie en verwerking binnen een taak alleen de daarvoor noodzakelijke persoonsgegevens worden doorgegeven of zijn in te zien, waarbij de andere persoonsgegevens verborgen blijven door het toepassen van versleuteling van de opslagvoorzieningen, de transportpaden en de middleware. Het implementatiemodel is getoetst. | NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015 ) 'verbergen' | | Overleg bewijsstukken en/of verklaring | | | | | |
| 807 | DataminimalisatieDataminimalisatie door serverplatformen | Privacy-supplement Serverplatform | SVP P.01 | | De organisatie behoort een proces te hebben ingericht en afspraken te hanteren, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruiken, waarbij enkel de minimaal benodigde hoeveelheid persoonsgegevens wordt verwerkt en verwijdering van persoonsgegevens mogelijk is. | AVG: art. 6 lid 1, Wpg art 3 lid 2 | | Overleg bewijsstukken en/of verklaring | | | | | |
| 808 | Scheiden door serverplatformen | Privacy-supplement Serverplatform | SVP P.02 | | De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is. | NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015 ) 'scheiden' | | Overleg bewijsstukken en/of verklaring | | | | | |
| 809 | Verbergen door serverplatformen | Privacy-supplement Serverplatform | SVP P.03 | | De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is. | NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015 ) 'verbergen' | | Overleg bewijsstukken en/of verklaring | | | | | |
| 810 | Scheiden binnen communicatievoorzieningen | Privacy-supplement Communicatievoorzieningen | CVZ P.01 | | De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruiken, waarbij de scheiding van verwerkingen het uitgangspunt is. | NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015 ) 'scheiden' | | Overleg bewijsstukken en/of verklaring | | | | | |
| 811 | Verbergen binnen communicatievoorzieningen | Privacy-supplement Communicatievoorzieningen | CVZ P.02 | | De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruiken, waarbij het verbergen van verwerkingen het uitgangspunt is. | NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015 ) 'verbergen' | | Overleg bewijsstukken en/of verklaring | | | | | |
| 812 | Logging binnen communicatievoorzieningen | Privacy-supplement Communicatievoorzieningen | CVZ P.03 | | De logging en monitoring van het netwerk behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast. | AVG: art. 5 lid 2 en art. 33 lid 5, Wpg Art. 32a | | Overleg bewijsstukken en/of verklaring | | | | | |
| 813 | Uitvallen van een dienst | Privacy-supplement Huisvesting-IV | HVI P.01 | | De organisatie heeft maatregelen getroffen die voorkomen dat de uitval van een dienst, of dit nu een eigen dienst is of van een derde is, leidt tot een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een procedure om de werking van de maatregel te evalueren. | AVG: art. 24, 32, 35, 36 | | Overleg bewijsstukken en/of verklaring | | | | | |
| 814 | Het stelsel van toegangsbeheer | Privacy-supplement Toegangsbeveiliging | TBV P.01 | | Het doel van de verwerking van persoonsgegevens en van de toegang zijn welbepaald, gerechtvaardigd en uitdrukkelijk omschreven, waarbij de toegang naar keuze rol gebaseerd en waar nodig taak gebaseerd wordt verstrekt. Aanvullend vindt logging en monitoringplaats. | AVG: art. 5, Wpg Art 6 lid 1 t/m 6 Art 6a | | Overleg bewijsstukken en/of verklaring | | | | | |
| 815 | Doelbinding op rolniveau | Privacy-supplement Toegangsbeveiliging | TBV P.02 | | De organisatie behoort verwerkers gescheiden en beperkt toegang te verlenen tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar. | NEN 7510 2017: A.9.2.6, Wpg Art 6 lid 1 t/m 6 Art 6a | | Overleg bewijsstukken en/of verklaring | | | | | |
| 816 | Toegang op taakniveau | Privacy-supplement Toegangsbeveiliging | TBV P.03 | | Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar. | CIP-netwerk, Wpg: Art 6 lid 1 t/m 6 Art 6a | | Overleg bewijsstukken en/of verklaring | | | | | |
| 817 | Logging en monitoring uitgeven toegangsrechten | Privacy-supplement Toegangsbeveiliging | TBV P.04 | | De verwerking behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast. | AVG: art. 33 lid 5 en 5 lid 2, Wpg Art. 32a | | Overleg bewijsstukken en/of verklaring | | | | | |

| Nr | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 806 | | | | | | | | | | | | | Clouddiensten |
| 807 | | | | | | | | | | | | | Clouddiensten |
| 808 | | | | | | | | | | | | | Clouddiensten |
| 809 | | | | | | | | | | | | | Clouddiensten |
| 810 | | | | | | | | | | | | | Clouddiensten |
| 811 | | | | | | | | | | | | | Clouddiensten |
| 812 | | | | | | | | | | | | | Clouddiensten |
| 813 | | | | | | | | | | | | | Clouddiensten |
| 814 | | | | | | | | | | | | | Clouddiensten |
| 815 | | | | | | | | | | | | | Clouddiensten |
| 816 | | | | | | | | | | | | | Clouddiensten |
| 817 | | | | | | | | | | | | | 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: |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 818 | Toegang tot fysieke omgevingen | Privacy-supplement Toegangsbeveiliging | TBV P.05 | | De organisatie behoort fysieke beveiliging van omgevingen waar persoonsgegevens worden verwerkt, op passende wijze ingericht te hebben, zodat enkel medewerkers met noodzakelijk belang toegang hebben tot en zich bevinden in deze omgevingen; de toegang wordt geregistreerd. | ISO 27002 2017: 11.1, ABDO 2019 v1.1: 3.1.2, Wpg: Art 6 lid 1 t/m 6 Art 6a | | Overleg bewijsstukken en/of verklaring | | | | | |
| 819 | Toegang buiten beveiligde omgevingen | Privacy-supplement Toegangsbeveiliging | TBV P.06 | | Er is een procedure ingericht voor het transporteren van persoonsgegevens buiten een beschermde omgeving, waarbij door versleuteling de kans op een datalek is verkleind en door minimalisatie de omvang van een datalek wordt beperkt. | AVG: art.32, Wpg: Art 6 lid 1 t/m 6 Art 6a | | Overleg bewijsstukken en/of verklaring | | | | | |
| 820 | Toegang in het buitenland | Privacy-supplement Toegangsbeveiliging | TBV P.07 | | De organisatie hanteert regels voor medewerkers en andere verwerkers, die buiten Nederland persoonsgegevens of authenticatiemiddelen (voor de toegang tot persoonsgegevens vanuit het buitenland) met zich meedragen of in hun bezit hebben, ongeacht of deze informatie versleuteld is. | AVG: art. 32, Wpg: Art 6 lid 1 t/m 6 Art 6a | | Overleg bewijsstukken en/of verklaring | | | | | |
| 821 | Beëindiging (verwerkers)overeenkomst | Privacy-supplement Toegangsbeveiliging | TBV P.08 | | De verwerkingsverantwoordelijke legt in de (verwerkers) overeenkomst afspraken vast, met de persoon of partij die persoonsgegevens verwerkt, over het verwijderen of overdragen van persoonsgegevens bij beëindiging van de relatie; eventuele derden worden over de beëindiging geïnformeerd. | AVG: art.32, AP Werkende verwerkersovereenkomsten september 2019 : 4.3.6 | | Overleg bewijsstukken en/of verklaring | | | | | |

| Nr | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 818 | | | | | | | | | | | | | Clouddiensten |
| 819 | | | | | | | | | | | | | Clouddiensten |
| 820 | | | | | | | | | | | | | Clouddiensten |
| 821 | | | | | | | | | | | | | Clouddiensten |