Auditrapport

NEN-EN-ISO/IEC 27001:2017+A11:2020 + BIO
Extra audit

Provincie Gelderland

Provincie Gelderland

Auditdagen op locatie

donderdag 4 juli 2024

Auteur: [redacted]5.1.2e[redacted]@digitrust.nl)
Datum: Donderdag 04-07-2024

Gegevens

Klant:	
Naam	Provincie Gelderland
Adres	Provincie Gelderland
Contact	5.1.2e @gelderland.nl / 5.1.2e
BBN level	BBN2

Audit:	
Scope ISMS	*Informatiebeveiliging gerelateerd aan en met betrekking tot het organisatieonderdelen Kwaliteit Openbaar Bestuur voor het uitvoeren en beheren van de activiteiten, producten en diensten van het proces BIBOB.* *Dit conform de vastgestelde verklaring van toepasselijkheid d.d. 6-april-2023 versie 1.1 waarin de eisen uit de Baseline Informatiebeveiliging Overheid (BIO) zijn opgenomen.*
Organisatorische en functionele eenheden	*Provincie Gelderland*
Vestigingen in scope	*Markt 11 6811CG Arnhem*
Vestigingen bezocht	*Markt 11 6811CG Arnhem*
Naam en versie VvT op certificaat	*DOC-B-06 Verklaring van Toepasselijkheid* *Datum: 06-04-2023* *Versie: 1.1*
Aantal FTE	*10*

Auditoren:	
Leadauditor	5.1.2e @digitrust.nl)
Auditor(en)	n.v.t.
Auditor in opleiding	n.v.t.
Technisch/ Juridisch deskundige	n.v.t.
Waarnemer	n.v.t.

Bijzonderheden:	
Audit gecombineerd met andere audit?	Ja
Speciale communicatie-middelen?	Ja
Welke ICT tool is gebruikt?	MS Teams
Was de inzet van het ICT middel effectief mbt het behalen van de auditdoelstellingen?	Ja
Klant werkt met ploegen-diensten?	Nee
Klant spreekt (deels) geen Nederlands?	Nee

Terminologie:	
Kritieke afwijking	Afwijking die van invloed is op het vermogen van het managementsysteem om de beoogde resultaten te behalen.
Niet-kritieke afwijking	Afwijking die niet van invloed is op het vermogen van het managementsysteem om de beoogde resultaten te behalen.
Kans voor verbetering	Een door de auditor geobserveerde situatie, die voor de klant een verbeter kans geeft. De kans voor verbetering is gebaseerd op algemene 'best practices', maar zal nooit een specifieke oplossing geven.

Algemene conclusie

Advies auditor	Op basis van de auditresultaten van deze Extra certificatieaudit, geeft de auditor een POSITIEF advies voor de voortzetting van de certificatie van de activiteiten zoals beschreven in het toepassingsgebied van uw managementsysteem voor informatiebeveiliging. De auditor verklaart op basis van de resultaten van deze audit dat het managementsysteem van de klant het vermogen heeft om aan de toepasselijke eisen en verwachte resultaten te voldoen.
Eindconclusie auditor	1. Realisatie auditplan De lead auditor is in staat geweest om het gehele auditplan zoals afgestemd uit te voeren. 2. Behalen auditdoelstellingen: a. Het ISMS voldoet aan de criteria/eisen van de ISO27001 en de BIO maatregelen omdat er geen kritieke, één niet-kritieke afwijkingen en ook een aantal Kansen voor verbetering zijn vastgesteld door de auditor. (c.q. nog open staan na deze extra audit ten opzichte van de C1 audit) b. Het ISMS heeft het vermogen om aan wet/regelgeving te voldoen omdat deze zijn geïnventariseerd en er een proces ingericht is waarin dit wordt bewaakt. Hiervoor zijn geen afwijkingen geconstateerd. c. Het ISMS is doeltreffend omdat het de eigen doelstellingen aantoonbaar kan behalen. d. De belangrijkste verbetergebieden van het ISMS zijn: - Dat het verbetertraject voor het proces voor Informatiebeveiliging continuïteit conform plannen wordt afgerond Voor details, overige afwijkingen en kansen voor verbetering verwijs ik naar onderstaande rapportage. 3. Doeltreffendheid interne audits en directiebeoordeling: De uitgevoerde interne audit en directiebeoordeling is doeltreffend omdat deze worden uitgevoerd op een objectieve en onafhankelijke wijze en bevindingen leiden tot een verbetering van het ISMS. 4. Significante wijzigingen: Er zijn sinds de laatste audit (C1 audit) geen significante wijzigingen geweest die impact hebben op het ISMS of op de beveiliging van informatie. Wel is het SCC opnieuw ingericht zodat het beter aansluit bij de organisatie en beheer onderhouden en beheerd kan worden. 5. Toepassingsgebied van certificatie: De scope is helder en geeft een duidelijke beschrijving van de diensten die binnen het ISMS vallen. (Ongewijzigd gebleven) 6. Waren er nog eventuele onopgeloste punten en/of meningsverschillen: Tijdens de audit waren er geen onopgeloste punten of meningsverschillen omdat er overeenstemming is bereikt over de bevindingen. 7. Certificatie uitingen en logo's: Tijdens de audit is door de lead-auditor beoordeeld dat er geen afwijkingen zijn op het gebied van logo of certificering uitingen. (Deze worden nog niet gebruikt) 8. Klachten ontvangen bij klant m.b.t. het ISMS of Informatie beveiliging: Tijdens de audit is door de lead-auditor beoordeeld dat er geen klachten zijn ontvangen met betrekking tot informatiebeveiliging of het ISMS.
Samenvatting bevindingen	Tijdens deze audit zijn er 1 niet-kritieke afwijkingen en geen kritieke afwijkingen vastgesteld. Daarnaast zijn er tijdens deze audit 3 kansen voor verbetering genoteerd. Details vindt u in het hoofdstuk 'Resultaten' in dit rapport. De audit is verricht met behulp van steekproeven, daarom kunnen afwijkingen aanwezig zijn die niet zijn geïdentificeerd.
Corrigerende maatregelen nav vorige audit	Tijdens deze audit is de doeltreffendheid van corrigerende maatregelen betreffende openstaande afwijkingen van eerdere audits geverifieerd. Details vindt u in het hoofdstuk 'Resultaten' in dit rapport.
Controle FTE's	ISMS Tijdens deze audit is het aantal opgegeven FTE's gecontroleerd dat door de organisatie is opgegeven bij de intake. Hierbij is geen afwijking gevonden die van invloed kan zijn op de berekening van de in de ISO27006 voorgeschreven audittijd.
Gecombineerde Management systeem audits	n.v.t.
Corrective Action Plan (CAP)	Wij vragen u een plan in te dienen, waarin voor elke vastgestelde afwijking de oorzaak wordt omschreven en de door u voorgestelde corrigerende actie, met daarbij de verantwoordelijkheden en een tijdsplanning. Dit plan moet uiterlijk op de eerste werkdag na donderdag 18 juli 2024 per e-mail worden verstuurd naar de DigiTrust auditor. Uw ingediende plan zal samen met dit rapport de basis vormen waarop DigiTrust haar certificatiebeslissing zal nemen.
Tot slot	Wij willen de deelnemers aan deze audit hartelijk danken voor hun ondersteuning en medewerking. Deze rapportage en aanverwante documenten zijn uitsluitend opgesteld voor de cliënt van DigiTrust. DigiTrust aanvaardt geen verantwoordelijkheid (juridisch of anderszins) of aansprakelijkheid in relatie tot elk ander doel waarvoor het rapport kan worden gebruikt of derden die zich beroepen op de inhoud van dit rapport. Indien u kopieën van dit rapport wilt distribueren, dan dienen alle pagina's van dit rapport te worden toegevoegd. Dit auditrapport blijft eigendom van DigiTrust [17021-1:2015/9.4.8.1]

Resultaten

H4	Context van de organisatie	
Norm par 4.1	**Inzicht in de organisatie en haar context**	**Oordeel**
Norm eis:	De organisatie moet externe en interne belangrijke punten (issues) vaststellen die relevant zijn voor haar doelstelling en die haar vermogen beïnvloeden om het (de) beoogde resultaat(a)t(en) van haar managementsysteem voor informatiebeveiliging te behalen.	Niet in audit scope
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
Norm par 4.2	**Inzicht in de behoeften en verwachtingen van belanghebbenden**	**Oordeel**
Norm eis:	De organisatie moet vaststellen: a)welke belanghebbenden relevant zijn voor het managementsysteem voor informatiebeveiliging, en b)welke eisen van deze belanghebbenden relevant zijn voor informatiebeveiliging. OPMERKING De eisen van belanghebbenden kunnen eisen op het gebied van wet- en regelgeving en contractuele verplichtingen inhouden.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	Inzicht in de behoefte en verwachtingen van belanghebbende zijn in kaart gebracht. Er kan explicieter de eisen en verwachtingen van de relatie beschreven worden in plaats van het geleverde door de relaties. Dit levert een KVV.	
Bewijslast:	DOC-B-05 Toepassingsgebied ISMS	
Interview met:	5.1.2e	
Toelichting auditor	Inzicht in de behoefte en verwachtingen van belanghebbende zijn in kaart gebracht. Er zijn belanghebbende toegevoegd en de eisen zijn wat explicieter benoemd. Deze KVV is effectief opgepakt en opgelost.	
Norm par 4.3	**Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen**	**Oordeel**
Norm eis:	De organisatie moet de grenzen en toepasselijkheid van het managementsysteem voor informatiebeveiliging bepalen om het toepassingsgebied ervan vast te stellen. Bij het vaststellen van dit toepassingsgebied moet de organisatie het volgende overwegen: a) de in 4.1 genoemde externe en interne belangrijke punten (issues); b) de in 4.2 genoemde eisen, en c) raakvlakken en afhankelijkheden tussen de activiteiten die door de organisatie en de activiteiten die door andere organisaties worden verricht. Het toepassingsgebied moet als gedocumenteerde informatie beschikbaar zijn.	Niet in audit scope
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
Norm par ISO17021-1/8.2.2-f	**Scope**	**Oordeel**
Norm eis:	Het toepassingsgebied van de certificatie moet helderheid geven over de soort activiteiten, producten en diensten zoals van toepassing is op elke vestiging, zonder misleidend of dubbelzinnig te zijn.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de beschrijving van het toepassingsgebied helderheid geeft over de soort activiteiten, producten en diensten zoals van toepassing is op elke vestiging, zonder misleidend of dubbelzinnig te zijn.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	DOC-B-05 Toepassingsgebied ISMS	
Interview met:	5.1.2e	
Toelichting auditor	Het toepassingsgebied voor het certificatie geeft helderheid over de soort activiteiten, producten en diensten zoals van toepassing, zonder misleidend of dubbelzinnig te zijn.	

H5	Leiderschap	
Norm par 5.1	**Leiderschap en betrokkenheid**	**Oordeel**
Norm eis:	De directie moet leiderschap en betrokkenheid tonen met betrekking tot het managementsysteem voor informatiebeveiliging door: a)te bewerkstelligen dat het informatiebeveiligingsbeleid en de informatiebeveiligingsdoelstellingen worden vastgesteld en compatibel zijn met de strategische richting van de organisatie; b)te bewerkstelligen dat de eisen van het managementsysteem voor informatiebeveiliging in de processen van de organisatie worden geïntegreerd; c)te bewerkstelligen dat de voor het managementsysteem voor informatiebeveiliging benodigde middelen beschikbaar zijn; d)het belang van doeltreffend informatiebeveiligingsmanagement en van het voldoen aan de eisen van het managementsysteem voor informatiebeveiliging te communiceren; e)te bewerkstelligen dat het managementsysteem voor informatiebeveiliging zijn beoogde resulta(a)t(en) behaalt; f)mensen aan te sturen en te ondersteunen om een bijdrage te leveren aan de doeltreffendheid van het managementsysteem voor informatiebeveiliging; g)continue verbetering te bevorderen; en h)andere relevante managementfuncties te ondersteunen om hun leiderschap te tonen binnen hun verantwoordelijkheidsgebieden.	Niet in audit scope
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
Norm par 5.2	**Beleid**	**Oordeel**
Norm eis:	De directie moet een informatiebeveiligingsbeleid vaststellen dat: a)passend is voor het doel van de organisatie; b)informatiebeveiligingsdoelstellingen bevat (zie 6.2) of het kader biedt voor het vaststellen van informatiebeveiligingsdoelstellingen; c)een verbintenis bevat om te voldoen aan van toepassing zijnde eisen in verband met informatiebeveiliging; en d)een verbintenis bevat tot continue verbetering van het managementsysteem voor informatiebeveiliging. Het beleid voor informatiebeveiliging moet: e)beschikbaar zijn als gedocumenteerde informatie; f)worden gecommuniceerd binnen de organisatie, en g)op een geschikte manier beschikbaar zijn voor belanghebbenden.	Niet in audit scope
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
Norm par 5.3	**Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie**	**Oordeel**
Norm eis:	De directie moet bewerkstelligen dat de verantwoordelijkheden en bevoegdheden voor rollen die relevant zijn voor informatiebeveiliging worden toegekend en gecommuniceerd. De directie moet de verantwoordelijkheid en bevoegdheid toekennen met betrekking tot: a)het bewerkstelligen dat het managementsysteem voor informatiebeveiliging voldoet aan de eisen van deze internationale norm; en b)het rapporteren over de prestaties van het managementsysteem voor informatiebeveiliging aan de directie.	Niet in audit scope
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	

H6	Planning	
Norm par 6.1	**Acties om risico's en kansen op te pakken**	
Norm par 6.1.1	**Algemeen**	**Oordeel**
Norm eis:	Bij het plannen voor het managementsysteem voor informatiebeveiliging moet de organisatie de in 4.1 genoemde belangrijke punten (issues) en de in 4.2 genoemde eisen overwegen, en de risico's en kansen vaststellen die moeten worden opgepakt om: a)te bewerkstelligen dat het managementsysteem voor informatiebeveiliging zijn beoogde resulta(a)t(en) kan behalen; b)ongewenste effecten te voorkomen of te verminderen; en c)continue verbetering te bereiken. De organisatie moet: d)acties plannen om deze risico's te beperken en kansen te benutten; e)plannen op welke manier: 1)de acties in haar managementsysteemprocessen voor informatiebeveiliging worden geïntegreerd en geïmplementeerd; en 2)de doeltreffendheid van deze acties wordt geëvalueerd.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	DOC-B-05 Toepassingsgebied ISMS DOC-BB-05 Rapportage risicoanalyse proces Bibob DOC-BB-01A - Richtlijn methode risico analyse	
Interview met:	5.1.2e	
Toelichting auditor	Het toepassingsgebied is opnieuw beoordeeld en aangepast (Er zijn wat externe stakeholders toegevoegd) De algemene risico's voor het ISMS zijn beschreven binnen het toepassingsgebied. Deze zijn weer (indirect) opgenomen in de risico analyse in SCC	
Norm par 6.1.2	**Risicobeoordeling van informatiebeveiliging**	**Oordeel**
Norm eis:	De organisatie moet een risicobeoordelingsproces voor informatiebeveiliging definiëren en toepassen dat: a)risicocriteria voor informatiebeveiliging vaststelt en onderhoudt, waaronder: 1)de risicoacceptatiecriteria; en 2)criteria voor het verrichten van risicobeoordelingen van informatiebeveiliging; b)waarborgt dat herhaalde risicobeoordelingen van informatiebeveiliging consistente, valide en vergelijkbare resultaten opleveren; c)de informatiebeveiligingsrisico's identificeert: 1)het risicobeoordelingsproces voor informatiebeveiliging toepassen om de risico's in verband met het verlies van vertrouwelijkheid, integriteit en beschikbaarheid van informatie binnen het toepassingsgebied van het managementsysteem voor informatiebeveiliging te identificeren; en 2)de risico-eigenaren identificeren; d)de informatiebeveiligingsrisico's analyseert: 1)de potentiële gevolgen beoordelen indien de risico's die in 6.1.2 c) 1) zijn vastgesteld, zich zouden voordoen; 2)de realistische waarschijnlijkheid beoordelen van het voorkomen van de risico's die zijn vastgesteld in 6.1.2 c) 1); en 3)de risiconiveaus vaststellen; e)de informatiebeveiligingsrisico's evalueert: 1)de resultaten vergelijken van risicoanalyses met de risicocriteria die zijn vastgesteld in6.1.2a); en 2)de geanalyseerde risico's prioriteren voor risicobehandeling. De organisatie moet gedocumenteerde informatie bewaren over het risicobeoordelingsproces voor informatiebeveiliging.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	DOC-B-05 Toepassingsgebied ISMS DOC-BB-05 Rapportage risicoanalyse proces Bibob (2023) DOC-BB-01A - Richtlijn methode risico analyse SCC	
Interview met:	5.1.2e	
Toelichting auditor	Middels de Methode SRAM zijn alle risico's in kaart gebracht en opgenomen in het SCC. In het SCC systeem is de methodiek voor de risico beoordeling en criteria geborgd Eigenaren zijn gekoppeld aan de proceseigenaren. Middels een proces inventarisatie verbeteracties wordt er geborgd dat de risico's/maatregelen jaarlijks worden beoordeeld.	
Norm par 6.1.3	**Behandeling van informatiebeveiliging risico's**	**Oordeel**

Norm eis:	De organisatie moet een behandelprocedure voor informatiebeveiligingsrisico's definiëren en toepassen om: a)passende opties voor het behandelen van informatiebeveiligingsrisico's te kiezen, rekening houdend met de resultaten van de risicobeoordeling; b)alle beheersmaatregelen vast te stellen die nodig zijn om de gekozen optie(s) voor het behandelen van informatiebeveiligingsrisico's te implementeren; OPMERKING Organisaties kunnen beheersmaatregelen naar behoefte ontwerpen of ze uit een bepaalde bron halen. c)de beheersmaatregelen die hiervoor in 6.1.3 b) zijn vastgesteld te vergelijken met die in bijlage A, en om te verifiëren dat geen noodzakelijke beheersmaatregelen zijn weggelaten; OPMERKING 1 Bijlage A bevat een uitgebreide lijst van beheersdoelstellingen en beheersmaatregelen. Gebruikers van deze internationale norm worden verwezen naar bijlage A om te bewerkstelligen dat geen noodzakelijke beheersmaatregelen over het hoofd worden gezien. OPMERKING 2 Bij de gekozen beheersmaatregelen zijn beheersdoelstellingen impliciet begrepen. De in bijlage A opgesomde beheersdoelstellingen en beheersmaatregelen zijn niet uitputtend, en mogelijk zijn aanvullende beheersdoelstellingen en beheersmaatregelen nodig. d)een verklaring van toepasselijkheid op te stellen die bevat: —de benodigde beheersmaatregelen (zie 6.1.3 b) en c)); —een rechtvaardiging voor het opnemen ervan; —de informatie of de benodigde beheersmaatregelen zijn geïmplementeerd of niet, en —de rechtvaardiging voor het uitsluiten van in bijlage A genoemde beheersmaatregelen. e)een behandelplan voor informatiebeveiligingsrisico te formuleren; en f)van de risico-eigenaren goedkeuring te verkrijgen voor het behandelplan voor informatiebeveiligingsrisico en acceptatie van de overblijvende informatiebeveiligingsrisico's. De organisatie moet gedocumenteerde informatie bewaren over de behandelprocedure van informatiebeveiligingsrisico's.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	DOC-B-05 Toepassingsgebied ISMS DOC-BB-05 Rapportage risicoanalyse proces Bibob DOC-BB-01A - Richtlijn methode risico analyse Geaccepteerde risico's VM-02 Beleggen maatregelen informatiebeveiliging TM-01 inventariseren verbeteracties DOC-B-06 Verklaring van Toepasselijkheid	
Interview met:	5.1.2e	
Toelichting auditor	In SCC zijn voor alle risico's de bijbehorende maatregelen gekoppeld waarmee de behandeling wordt geborgd. VVT is opgezet vanuit het SCC en alle maatregelen zijn van toepassing verklaart. Vanuit de risicoanalyse is bepaald welke maatregelen van toepassing zijn. Alle restrisico's zijn besproken binnen het IB-Forum waarin de restrisico's zijn geaccepteerd. Deze zijn samen met andere stukken ook weer voorgelegd aan de directie welke deze heeft tevens vastgesteld. Hiermee is de voorgaande KVV opgelost.	
Norm par 6.2	**Informatiebeveiliging doelstellingen en de planning om ze te bereiken**	**Oordeel**
Norm eis:	De organisatie moet voor relevante functies en niveaus informatiebeveiligingsdoelstellingen vaststellen. De informatiebeveiligingsdoelstellingen moeten: a) consistent zijn met het informatiebeveiligingsbeleid; b) meetbaar zijn (indien praktisch uitvoerbaar); c) rekening houden met van toepassing zijnde informatiebeveiligingseisen en resultaten van risicobeoordeling en -behandeling; d) worden gecommuniceerd; en e) passend bij de situatie worden geactualiseerd. De organisatie moet gedocumenteerde informatie over de informatiebeveiligingsdoelstellingen bijhouden. Bij het opstellen van planningen voor het bereiken van de informatiebeveiligingsdoelstellingen moet de organisatie vaststellen: f) wat er zal worden gedaan; g) welke middelen er nodig zijn; h) wie er verantwoordelijk is; i) wanneer het zal zijn voltooid; en j) hoe de resultaten zullen worden geëvalueerd.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	DOC-B-02 Jaarplan Informatiebeveiliging 2023 DOC-B-02 Jaarplan Informatiebeveiliging 2024 DOC-B-01 Beleid Informatiebeveiliging 6-3-2024	
Interview met:	5.1.2e	
Toelichting auditor	In het jaarplan zijn de doelstellingen van het lopende/komende jaar vastgesteld.	

H7	Ondersteuning	
Norm par 7.1	**Middelen**	**Oordeel**
Norm eis:	De organisatie moet de middelen vaststellen en beschikbaar stellen die nodig zijn voor het inrichten, implementeren, onderhouden en continu verbeteren van het managementsysteem voor informatiebeveiliging.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	DOC-B-02 Jaarplan Informatiebeveiliging 2023 DOC-B-02 Jaarplan Informatiebeveiliging 2024 DOC-B-01 Beleid Informatiebeveiliging 6-3-2024	
Interview met:	5.1.2e	
Toelichting auditor	De provincie heeft Strict in de arm genomen om het ISMS op te zetten, te ondersteunen en te onderhouden Daarnaast is er nu ondersteuning vanuit Securesult 5.1.2e Verder is er een Jaarplan opgezet waarin de geraamde kosten en inzet is opgenomen.	
Norm par 7.2	**Competentie**	**Oordeel**
Norm eis:	De organisatie moet: a) de benodigde competentie vaststellen van de perso(o)n(en) die onder haar gezag werkzaamheden verricht(en) die haar prestaties op het gebied van informatiebeveiliging beïnvloeden; b) bewerkstelligen dat deze personen competent zijn op basis van de juiste opleiding, training of ervaring; c) indien van toepassing, acties ondernemen om de benodigde competentie te verwerven, en de doeltreffendheid van de ondernomen acties evalueren; en d) geschikte gedocumenteerde informatie als bewijs van competentie bijhouden. OPMERKING Toepasbare acties kunnen bijvoorbeeld zijn: het voorzien in training van, het begeleiden van, of het in een andere functie benoemen van mensen die al in dienst zijn; of het inhuren of contracteren van competente personen.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	Competenties zijn opgenomen in de functieprofielen. De huidige interne auditoren hebben een auditor training gevolgd bij DNV en daarvoor een certificaat behaald. Tijdens de audit is vastgesteld dat met het wegvallen van de oorspronkelijke "SO / ondersteuning SCC" er niet meer de juiste kennis aanwezig is van het Strict Control Cockpit (SCC) waardoor het systeem niet meer goed kan worden onderhouden en de juiste registraties en vastlegging geschieden. Dit levert een KA	
Bewijslast:	SCC - Beheer rollen en autorisaties Functieprofiel CISO PG DNV certificaat ISO27001 auditor 5.1.2e SCC - Functieprofiel FG SCC - Functieprofiel IA Extra: SCC - Functies en opleidingen informatiebeveiliging	
Interview met:	5.1.2e	
Toelichting auditor	Competenties zijn opgenomen in de functieprofielen. De huidige interne auditoren hebben een auditor training gevolgd bij DNV en daarvoor een certificaat behaald. Door de provincie Gelderland is een nieuwe externe deskundige (Chris Hazewinkel) aangetrokken welke een training heeft gevolgd bij Strict voor het inrichten, gebruik en beheer van het SCC systeem. Deze kennis wordt nu periodiek en ad-hoc overgedragen aan de CISO en SO. De SO is nieuw aangesteld om het ISMS verder mee te ondersteunen en te onderhouden. Daarnaast houdt Chris na contact met Strict over het gebruik en inirchting van Strict. Daarnaast is door het huidige Team Informatiebeveiliging het SCC opnieuw ingericht en beter passend gemaakt voor de organisatie. De voorgaande KA is hiermee effectief opgelost.	
Norm par 7.3	**Bewustzijn**	**Oordeel**
Norm eis:	Personen die werkzaamheden verrichten onder het gezag van de organisatie, moeten zich bewust zijn van: a) het informatiebeveiligingsbeleid; b) hun bijdrage aan de doeltreffendheid van het managementsysteem voor informatiebeveiliging, met inbegrip van de voordelen van verbeterde informatiebeveiligingsprestaties; c) de gevolgen van het niet voldoen aan de eisen van het managementsysteem voor informatiebeveiliging.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	DOC-B-01 Beleid Informatiebeveiliging 6-3-2024 Digitale weerbaarheid 2.0 Gelderlandleert.StudyTube.nl e-mail Oproep aanmeling training "Digitale weerbaarheid 2.0" d.d. 6-2-2024	
Interview met:	5.1.2e	

Toelichting auditor	De CISO geeft alle medewerkers een Introductie/training ISO. Deze training wordt een aantal keren per week gegeven. Hierin worden verschillende regels, procedures en bewustwording toegelicht. Ongeveer 70% heeft de training gevolgd. De Ciso houdt bij wie de training heeft gevolgd en wie nog niet. De directie heeft voor deze training een e-mail naar alle medewerkers gestuurd dat deze training verplicht is om te volgen.	
Norm par 7.4	**Communicatie**	**Oordeel**
Norm eis:	De organisatie moet de behoefte vaststellen aan interne en externe communicatie die relevant is voor het managementsysteem voor informatiebeveiliging, inclusief: a) waarover te communiceren; b) wanneer te communiceren; c) met wie te communiceren; d) wie moet communiceren; en e) volgens welke processen de communicatie moet plaatsvinden.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	SCC - overlegstructuren DOC-B-02 jaarplan informatiebeveiliging 2024	
Interview met:	5.1.2e	
Toelichting auditor	Alle verschillende overleggen/communicatie voor zowel intern als extern zijn opgenomen in het SCC onder de overlegstructuren	
Norm par 7.5	**Gedocumenteerde informatie**	
Norm par 7.5.1	**Algemeen**	**Oordeel**
Norm eis:	Het managementsysteem voor informatiebeveiliging van de organisatie moet onder andere bevatten: a) de gedocumenteerde informatie die deze internationale norm vereist; en b) de gedocumenteerde informatie die de organisatie nodig acht voor de doeltreffendheid van het managementsysteem voor informatiebeveiliging. OPMERKING De uitgebreidheid van gedocumenteerde informatie voor een managementsysteem voor informatiebeveiliging kan van organisatie tot organisatie verschillen vanwege: 1) de omvang van de organisatie en het type van haar activiteiten, processen, producten en diensten; 2) de complexiteit van de processen en hun interacties; en 3) de competentie van de mensen.	Niet in steekproef van deze audit
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
Norm par 7.5.2	**Creëren en actualiseren**	**Oordeel**
Norm eis:	Bij het creëren en actualiseren van gedocumenteerde informatie moet de organisatie zorgen voor een passend(e): a) identificatie en beschrijving (bijv. een titel, datum, auteur of referentienummer); b) format (bijv. taal, softwareversie, afbeeldingen) en media (bijv. papier, elektronisch); en c) beoordeling en goedkeuring van geschiktheid en toereikendheid.	Niet in steekproef van deze audit
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
Norm par 7.5.3	**Beheersing van gedocumenteerde informatie**	**Oordeel**
Norm eis:	7.5.3.1 Gedocumenteerde informatie zoals het managementsysteem voor informatiebeveiliging en deze internationale norm vereisen, moet worden beheerst om te bewerkstelligen dat: a) de informatie beschikbaar is en geschikt is voor gebruik, waar en wanneer het nodig is; b) de informatie afdoend is beveiligd (bijv. tegen verlies van vertrouwelijkheid, oneigenlijk gebruik en aantasting). 7.5.3.2 Voor het beheersen van gedocumenteerde informatie moet de organisatie, voor zover van toepassing, invulling geven aan de volgende activiteiten: c) distributie, toegang, het terugvinden alsmede het gebruik; d) opslag en behoud, waaronder behoud van leesbaarheid; e) beheersing van wijzigingen (bijv. versiebeheer); en f) het bewaren en vernietigen. Gedocumenteerde informatie van externe oorsprong die de organisatie nodig acht voor de planning en uitvoering van het managementsysteem voor informatiebeveiliging, moet bij de situatie passend worden geïdentificeerd, en worden beheerst. OPMERKING Toegang impliceert een besluit tot toestemming om de gedocumenteerde informatie alleen in te zien, of tot toestemming en bevoegdheid om de gedocumenteerde informatie in te zien en te wijzigen, enz.	Niet in steekproef van deze audit
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	

Bewijslast:	0
Interview met:	0
Toelichting auditor	0

H8	Uitvoering	
Norm par 8.1	**Operationele planning en beheersing**	**Oordeel**
Norm eis:	Om te voldoen aan de informatiebeveiligingseisen en om de in 6.1 vastgestelde acties te implementeren moet de organisatie de benodigde processen plannen, implementeren en beheersen. De organisatie moet ook plannen implementeren om de in 6.2 vastgestelde informatiebeveiligingsdoelstellingen te bereiken. De organisatie moet gedocumenteerde informatie bijhouden in de omvang die nodig is om het vertrouwen te hebben dat de processen volgens planning zijn uitgevoerd. De organisatie moet geplande wijzigingen beheersen en de consequenties van onbedoelde wijzigingen beoordelen, en zo nodig maatregelen treffen om nadelige effecten tegen te gaan. De organisatie moet bewerkstelligen dat uitbestede processen worden vastgesteld en beheerst.	
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	Geen afwijkingen
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	DOC-B-02 jaarplan informatiebeveiliging 2024 SCC- Activiteiten jaarplan 2024 Topdesk - Operationele acitiviteiten. DOC-B-05 Toepassingsgebied ISMS	
Interview met:	5.1.2e	
Toelichting auditor	Alle activiteiten welke benodigde zijn voor het ISMS zijn opgenomen in het SCC systeem waarmee ze ook worden opgenomen in het jaarplan en goedgekeurd moeten worden door de directie. Daarnaast zijn er praktische taken zoals rechten controle e.d. opgenomen in de operationele activiteiten in Topdesk.	
Norm par 8.2	**Risicobeoordeling van informatiebeveiliging**	**Oordeel**
Norm eis:	De organisatie moet risicobeoordelingen van informatiebeveiliging met geplande tussenpozen uitvoeren, of als significante veranderingen worden voorgesteld of zich voordoen, rekening houdend met de criteria die zijn vastgesteld in 6.1.2 a). De organisatie moet gedocumenteerde informatie bewaren van de resultaten van de risicobeoordelingen van informatiebeveiliging.	
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	In de afgelopen periode zijn de risico's niet aantoonbaar opnieuw beoordeeld. Dit levert een KA.	
Bewijslast:	DOC-B-05 Toepassingsgebied ISMS DOC-BB- -05 Rapportage risicoanalyse proces Bibob DOC-BB-01A - Richtlijn methode risico analyse Extra: SCC_638556964028074805 - Risicoanalyse BIBOB d.d. 20-6-2024 SCC - Module Risicomanagement	Geen afwijkingen
Interview met:	5.1.2e	
Toelichting auditor	De risico analyse cq. het proces BIBOB is opnieuw beoordeeld en vastgesteld. De voorgaande KA is hiermee effectief opgelost.	
Norm par 8.3	**Informatiebeveiligingsrisico's behandelen**	**Oordeel**
Norm eis:	De organisatie moet het behandelplan van informatiebeveiligingsrisico's implementeren. De organisatie moet gedocumenteerde informatie bewaren van de resultaten van het behandelen van informatiebeveiligingsrisico's.	
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	De behandelingen van de risico's zijn niet aantoonbaar uitgevoerd. Dit levert een KA.	
Bewijslast:	DOC-B-05 Toepassingsgebied ISMS DOC-BB- -05 Rapportage risicoanalyse proces Bibob DOC-BB-01A - Richtlijn methode risico analyse SCC Extra: SCC - Module Risicomanagement	Geen afwijkingen
Interview met:	5.1.2e	

Toelichting auditor	In SCC zijn voor alle risico's de bijbehorende maatregelen gekoppeld waarmee de behandeling wordt geborgd. In het SCC zijn de activiteiten opgenomen welke uitgevoerd moeten worden om de maatregelen doorgevoerd te krijgen. Aan de hand van het opnieuw beoordeeld proces BIBOB is bepaald welke maatregelen (nog) niet voldoende zijn doorgevoerd en verder behandeld moeten worden. Dit alles is weer geborgd in SCC. De voorgaande KA is hiermee effectief opgelost.	

H9	Evaluatie van prestaties	
Norm par 9.1	**Monitoren, meten, analyseren en evalueren**	**Oordeel**
Norm eis:	De organisatie moet de informatiebeveiligingsprestaties en de doeltreffendheid van het managementsysteem voor informatiebeveiliging evalueren. De organisatie moet vaststellen: a) wat moet worden gemonitord en gemeten, met inbegrip van informatiebeveiligingsprocessen en -beheersmaatregelen; b) welke methoden worden gebruikt voor het, voor zover van toepassing, monitoren, meten, analyseren en evalueren, om valide resultaten te bewerkstelligen; OPMERKING De gekozen methoden behoren vergelijkbare en reproduceerbare resultaten op te leveren om als valide te worden beschouwd. c) wanneer moet worden gemonitord en gemeten; d) wie moet monitoren en meten; e) wanneer de resultaten van het monitoren en meten moeten worden geanalyseerd en geëvalueerd; en f) wie deze resultaten moet analyseren en evalueren. De organisatie moet geschikte gedocumenteerde informatie bijhouden als bewijs van de resultaten van het monitoren en meten.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	ISMS Informatiebeveiliging DOC-BB-00 rapportage bepalen behoefte informatiebeveiliging (DOC-BB-00) DOC-BB-03A KPI SCC Statussen 2	
Interview met:	5.1.2e	
Toelichting auditor	Voor alle hoofdprocessen zijn verschillende Monitoren en Meten activiteiten ingericht welke middels rapportages beoordeeld worden. KPI's worden beoordeeld	
Norm par 9.2	**Interne audit**	**Oordeel**
Norm eis:	De organisatie moet met geplande tussenpozen interne audits uitvoeren om informatie te verkrijgen of het managementsysteem voor informatiebeveiliging: a)voldoet aan: 1)de eigen eisen van de organisatie voor haar managementsysteem voor informatiebeveiliging; en 2)de eisen van deze internationale norm; b) doeltreffend is geïmplementeerd en onderhouden. De organisatie moet: c) (een) auditprogramma('s) plannen, vaststellen, implementeren en onderhouden, met inbegrip van de frequentie, methoden, verantwoordelijkheden, planningseisen en rapportage. Het auditprogramma moet rekening houden met het belang van de betrokken processen en met de resultaten van voorgaande audits; d) de auditcriteria voor en de reikwijdte van elke audit definiëren; e) auditoren selecteren en audits uitvoeren zodanig dat de objectiviteit en de onpartijdigheid van het auditproces worden bewerkstelligd; f) bewerkstelligen dat de resultaten van de audits worden gerapporteerd aan het relevante management; en g) gedocumenteerde informatie bijhouden als bewijs van het auditprogramma en de auditresultaten.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	Intern Auditplan 2023-2026 Auditrapport IB Proces bibob januari 2024 DOC-B-07 jaarverslag IB 2023 (24-1-2024) Actielijst audit januari 2024 PB-B-04 Directiebeoordeling ISMS DNV certificaat ISO27001 auditor 5.1.2e	
Interview met:	5.1.2e	
Toelichting auditor	Er is een interne audit uitgevoerd over de volledige norm maar dan wel steekproefsgewijs. Deze is uitgevoerd door de onafhankelijke en objectieve auditoren welke binnen Prov. Gelderland aanwezig zijn en de juiste opleiding hebben genoten en mandaat hebben. De punten uit de interne audit zijn als actie punten opgenomen in een overzicht (xls-sheet) Voor het meer jaren plan is auditprogramma opgesteld (Intern Auditplan 2023-2026). In het plan is opgenomen dat alle jaren de gehele norm (steekproefsgewijs) geaudit gaan worden.	
Norm par 9.3	**Directiebeoordeling**	**Oordeel**

Norm eis:	De directie moet met geplande tussenpozen het managementsysteem voor informatiebeveiliging van de organisatie beoordelen, om de continue geschiktheid, toereikendheid en doeltreffendheid te bewerkstelligen. Bij de directiebeoordeling moet onder andere in overweging worden genomen: a) de status van acties die zijn voortgekomen uit voorgaande directiebeoordelingen; b) wijzigingen in externe en interne belangrijke punten (issues) die relevant zijn voor het managementsysteem voor informatiebeveiliging; c) feedback over de informatiebeveiligingsprestaties, met inbegrip van trends in: 1) afwijkingen en corrigerende maatregelen; 2) resultaten van monitoren en meten; 3) auditresultaten; en 4) voldoen aan informatiebeveiligingsdoelstellingen; d) feedback van belanghebbenden; e) resultaten van risicobeoordeling en de status van het risicobehandelplan; en f) kansen voor continue verbetering. De resultaten van de directiebeoordeling moeten beslissingen omvatten met betrekking tot kansen voor continue verbetering en de noodzaak voor wijzigingen in het managementsysteem voor informatiebeveiliging. De organisatie moet gedocumenteerde informatie bijhouden als bewijs van de resultaten van de directiebeoordeling.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	De directie beoordeling is niet als een geheel gedaan maar versnipperd uitgevoerd waardoor niet aantoonbaar is dat alle verplichte onderdelen vanuit de norm zijn beoordeeld. Dit levert een KA.	
Bewijslast:	PB-B-04 Directiebeoordeling ISMS Extra: E-mail: Directieoverleg Informatiebeveiliging 20062024 DOC-B-04AA Directiebeoordeling 2023 (tussentijds) 2024 final. DOC-B-04A Tussenrapportage Directiebeoordeling ISMS (juni 2024)	
Interview met:	5.1.2e	
Toelichting auditor	De directiebeoordeling is opnieuw gedaan en in SCC geborgd dat deze 2 keer per jaar uitgevoerd zullen worden. Bij de directiebeoordeling worden alle normellementen welek vermeld zijn in H9.3 doorlopen en opgenomen in de presentatie van de directiebeoordeling. De voorgaande KA is hiermee effectief opgelost.	

H10	Verbetering	
Norm par 10.1	**Afwijkingen en corrigerende maatregelen**	**Oordeel**
Norm eis:	Wanneer zich een afwijking voordoet, moet de organisatie: a) op de afwijking reageren, en indien van toepassing: 1) maatregelen treffen om de afwijking te beheersen en te corrigeren, en 2) de consequenties aanpakken; b) de noodzaak evalueren om maatregelen te treffen om de oorzaken van de afwijking weg te nemen, zodat de afwijking zich niet herhaalt of zich elders voordoet, door: 1) de afwijking te beoordelen; 2) de oorzaken van de afwijking vast te stellen, en 3) vast te stellen of zich gelijksoortige afwijkingen voordoen of zouden kunnen voordoen; c)de benodigde maatregelen implementeren; d) de doeltreffendheid van getroffen corrigerende maatregelen beoordelen; e) zo nodig, wijzigingen aanbrengen in het managementsysteem voor informatiebeveiliging. Corrigerende maatregelen moeten passend zijn voor de effecten van de opgetreden afwijkingen. De organisatie moet gedocumenteerde informatie bijhouden als bewijs van: f) de aard van de afwijkingen en de vervolgens genomen maatregelen, en g) de resultaten van corrigerende maatregelen.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	De afwijkingen welke vanuit de interne audit zijn geconstateerd zijn opgenomen in een overzicht ,maar hierbij zijn (o.a.) geen oorzaak en omvanganalyse gedaan. Wel zijn er acties ondernomen of gepland om deze te verhelpen. Dat er geen aantoonbare oorzaak en omvanganalyse wordt gedaan bij afwijkingen (waar de afwijking vandaan komt) levert een NKA.	
Bewijslast:	Actielijst audit januari 2024 Extra: SCC - Activiteiten jaarplan 2024 - Audits informatiebeveiliging - Verbeteringen vanuit externe audits SCC - Activiteiten jaarplan 2024 - Audits informatiebeveiliging - Verbeteringen vanuit interne audits	
Interview met:	5.1.2e	
Toelichting auditor	Alle afwijkingen en verbeteringen zijn allemaal expliciet opgenomen in het SCC waarin de volledige registratie en status hiervan ook plaatsvindt. De voorgaande NKA is hiermee effectief opgelost.	
Norm par 10.2	**Continue verbetering**	**Oordeel**
Norm eis:	De organisatie moet continu de geschiktheid, toereikendheid en doeltreffendheid van het managementsysteem voor informatiebeveiliging verbeteren.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht of de organisatie de norm eisen mbt opzet, bestaan en werking aantoonbaar en doelmatig heeft geïmplementeerd en effectief heeft onderhouden.	
Relevante bevinding uit vorige audit(s):	Verbeteringen c.q. taken welke worden opgemerkt en opgepakt voor het ISMS worden vastgelegd in het SCC systeem. Uit de verbeteracties in SCC voor 2023 en 2024 vastgesteld dat de rapportage c.q. status niet is bijgewerkt. Dat niet kan worden aangetoond dat er continu wordt gewerkt aan de verbetering van de geschiktheid, toereikendheid en doeltreffendheid van het managementsysteem levert een NKA.	
Bewijslast:	PB-IM-01 Incident management IB PB-TM-01 Inventarisatie verbeteractie SCC - Activiteiten regulier 2023 SCC - Activiteiten regulier 2024 Extra: SCC - Activiteiten jaarplan 2024 - Audits informatiebeveiliging - Verbeteringen vanuit externe audits SCC - Activiteiten jaarplan 2024 - Audits informatiebeveiliging - Verbeteringen vanuit interne audits	
Interview met:	5.1.2e	
Toelichting auditor	Alle afwijkingen en verbeteringen zijn allemaal expliciet opgenomen in het SCC waarin de volledige registratie en status hiervan ook plaatsvindt. De voorgaande NKA is hiermee effectief opgelost.	

Bijlage A: Beheersmaatregelen

	A.5.1.1	Beleidsregels voor informatie-beveiliging	Oordeel
	Beheersmaatregel:	Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht of alle beleidsstukken aantoonbaar zijn goedgekeurd door de directie (De andere eisen van dit normelement zijn reeds beoordeeld bij H5.2).	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SharePoint - I&A Beleidsportaal SharePoint - ISMS Provincie Gelderland - 2023 - ISMS richtlijnen	
	Interview met:	5.1.2e	
	Toelichting auditor	Alle beleidsregels (en richtlijnen) zijn opgenomen in "SharePoint - I&A Beleidsportaal" en voor alle medewerkers beschikbaar	
Control BBN1	**A.5.1.1.1**	**Beleidsregels voor informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat ten minste de volgende punten: a.De strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. b.De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. c.De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers. d.De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn. e.De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. f.De bevordering van het beveiligingsbewustzijn.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) of het beleid aantoonbaar is goedgekeurd door de directie. 2) of de organisatie bepaald heeft aan wie het beleid moet worden opgelegd 3) of het beleid aantoonbaar is gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SharePoint - I&A Beleidsportaal DOC-B-01 Beleid Informatiebeveiliging 6-3-2024 PB-B-01 Beheren Beleid informatiebeveiliging E-mail: Verzoek tot vaststelling door AD van stukken Forum IB 27-9 d.d 17-10-2023 E-mail: Vaststeling documenten ISO27001 d.d.17-10-2023 lincl. beleid)	
	Interview met:	5.1.2e	
	Toelichting auditor	Alle onderdelen zijn opgenomen in DOC-B-01 Beleid Informatiebeveiliging. Het beleid wordt iedere jaar beoordeeld of als er eerder noodzaak toe is. Iedere 3 jaar moet het beleid altijd herzien worden. Het beleid is voor het laatst vastgesteld door de directie op 6-3-2024	
	A.5.1.2	**Beoordeling van het Informatie-beveiligings-beleid**	**Oordeel**
	Beheersmaatregel:	Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) of de organisatie een planning heeft gemaakt voor het periodiek opnieuw beoordelen van het beleid (en de daarvan afgeleide beleidsregels). 2) of de organisatie in staat is om zich aan haar eigen planning te houden. 3) of de organisatie, indien zich een significante verandering heeft voorgedaan, het beleid opnieuw heeft beoordeeld.	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SharePoint - I&A Beleidsportaal DOC-B-01 Beleid Informatiebeveiliging 6-3-2024 PB-B-01 Beheren Beleid informatiebeveiliging E-mail: Verzoek tot vaststelling door AD van stukken Forum IB 27-9 d.d 17-10-2023 E-mail: Vaststeling documenten ISO27001 d.d.17-10-2023 incl. beleid)	
	Interview met:	5.1.2e	
	Toelichting auditor	Alle onderdelen zijn opgenomen in DOC-B-01 Beleid Informatiebeveiliging. Het beleid wordt iedere jaar beoordeeld of als er eerder noodzaak toe is. Iedere 3 jaar moet het beleid altijd herzien worden. Het beleid is voor het laatst vastgesteld door de directie op 6-3-2024	
Control BBN1	**A.5.1.2.1**	**Beoordeling van het Informatiebeveiligingsbeleid**	**Oordeel**
	Beheersmaatregel:	Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) of de organisatie een planning heeft gemaakt voor het periodiek opnieuw beoordelen van het beleid (en de daarvan afgeleide beleidsregels). 2) of de organisatie in staat is om zich aan haar eigen planning te houden. 3) of de organisatie, indien zich een significante verandering heeft voorgedaan, het beleid opnieuw heeft beoordeeld.	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SharePoint - I&A Beleidsportaal DOC-B-01 Beleid Informatiebeveiliging 6-3-2024 PB-B-01 Beheren Beleid informatiebeveiliging E-mail: Verzoek tot vaststelling door AD van stukken Forum IB 27-9 d.d 17-10-2023 E-mail: Vaststeling documenten ISO27001 d.d.17-10-2023 lincl. beleid)	
	Interview met:	5.1.2e	

	Toelichting auditor	Alle onderdelen zijn opgenomen in DOC-B-01 Beleid Informatiebeveiliging. Het beleid wordt iedere jaar beoordeeld of als er eerder noodzaak toe is. Iedere 3 jaar moet het beleid altijd herzien worden. Het beleid is voor het laatst vastgesteld door de directie op 6-3-2024	
	A.6.1.1	**Rollen en verantwoordelijkheden bij informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) of de organisatie een planning heeft gemaakt voor het periodiek opnieuw beoordelen van het beleid (en de daarvan afgeleide beleidsregels). 2) of de organisatie in staat is om zich aan haar eigen planning te houden. 3) of de organisatie, indien zich een significante verandering heeft voorgedaan, het beleid opnieuw heeft beoordeeld.	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SCC - Beheer rollen en autorisaties Marktplaats - Functieprofiel CISO PG DNV certificaat ISO27001 auditor 5.1.2e Marktplaats - Functieprofiel FG Marktplaats - Functieprofiel Auditor	
	Interview met:	5.1.2e	
	Toelichting auditor	Verantwoordelijkheden zijn vastgelegd in functieprofielen	
Control BBN1	**A.6.1.1.1**	**Rollen en verantwoordelijkheden bij informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) of de organisatie een planning heeft gemaakt voor het periodiek opnieuw beoordelen van het beleid (en de daarvan afgeleide beleidsregels). 2) of de organisatie in staat is om zich aan haar eigen planning te houden. 3) of de organisatie, indien zich een significante verandering heeft voorgedaan, het beleid opnieuw heeft beoordeeld.	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SCC - Beheer rollen en autorisaties Marktplaats - Functieprofiel CISO PG DNV certificaat ISO27001 auditor 5.1.2e Marktplaats - Functieprofiel FG Marktplaats - Functieprofiel Auditor	
	Interview met:	5.1.2e	
	Toelichting auditor	Verantwoordelijkheden zijn vastgelegd in functieprofielen De functieprofielen zijn vastgesteld door de leidinggevende.	
Control BBN1	**A.6.1.1.2**	**Rollen en verantwoordelijkheden bij informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) of de organisatie een planning heeft gemaakt voor het periodiek opnieuw beoordelen van het beleid (en de daarvan afgeleide beleidsregels). 2) of de organisatie in staat is om zich aan haar eigen planning te houden. 3) of de organisatie, indien zich een significante verandering heeft voorgedaan, het beleid opnieuw heeft beoordeeld.	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SCC - Beheer rollen en autorisaties Marktplaats - Functieprofiel CISO PG DNV certificaat ISO27001 auditor 5.1.2e Marktplaats - Functieprofiel FG Marktplaats - Functieprofiel Auditor PB-VM-02 Beleggen maatregelen Informatiebeveiliging PB-VM-01 Vaststellen maatregelen IB	
	Interview met:	5.1.2e	
	Toelichting auditor	Bij het vaststellen van de maatregelen worden de wet en regelgeving meegenomen om deze daarna conform deze wet en regelgeving te beleggen bij de bijbehorende rollen.	
Control BBN1	**A.6.1.1.3**	**Rollen en verantwoordelijkheden bij informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) of de organisatie een planning heeft gemaakt voor het periodiek opnieuw beoordelen van het beleid (en de daarvan afgeleide beleidsregels). 2) of de organisatie in staat is om zich aan haar eigen planning te houden. 3) of de organisatie, indien zich een significante verandering heeft voorgedaan, het beleid opnieuw heeft beoordeeld.	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SCC - Beheer rollen en autorisaties Marktplaats - Functieprofiel CISO PG	
	Interview met:	5.1.2e	
	Toelichting auditor	De rol en verantwoordelijkheden van de CISO zijn vastgelegd.	
Control BBN1	**A.6.1.1.4**	**Rollen en verantwoordelijkheden bij informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) of de organisatie een planning heeft gemaakt voor het periodiek opnieuw beoordelen van het beleid (en de daarvan afgeleide beleidsregels). 2) of de organisatie in staat is om zich aan haar eigen planning te houden. 3) of de organisatie, indien zich een significante verandering heeft voorgedaan, het beleid opnieuw heeft beoordeeld.	Geen afwijkingen
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SCC - Beheer rollen en autorisaties Marktplaats - Functieprofiel CISO PG	
	Interview met:	5.1.2e	
	Toelichting auditor	Er is een CISO aangesteld welke heeft gesolliciteerd op functie CISO en voldoet aan de vacature/profiel.	
	A.6.1.2	**Scheiding van taken**	**Oordeel**
	Beheersmaatregel:	Conflicterende taken en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SCC - Beheer rollen en autorisaties	
	Interview met:	5.1.2e	
	Toelichting auditor	Binnen alle processen is opgenomen wie de proceseigenaren zijn en waar het Forum of directie zijn rol heeft.	
Control BBN1	**A.6.1.2.1**	**Scheiding van taken**	**Oordeel**
	Beheersmaatregel:	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SCC - Beheer rollen en autorisaties DocBase Portal Sharepoint (Bureau SBA/Bibob) e-mail; Toegang Sharepoint SBA (AdminOverzichtSBA.xls)	
	Interview met:	5.1.2e	
	Toelichting auditor	Binnen alle processen is opgenomen wie de proceseigenaren zijn en waar het Forum of directie zijn rol heeft. Binnen Docbase en SharePoint (waar vertrouwelijke stukken in zitten) zijn de rechten specifiek toegekend aan bepaalde rollen/functies zodat alleen gemachtigde vertrouwelijke stukken kunnen inzien. Alle systemen zijn gekoppeld middels aan de AD en werken met MFA.	
	A.6.1.3	**Contact met overheidsinstanties**	**Oordeel**
	Beheersmaatregel:	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.6.1.3.1**	**Contact met overheidsinstanties**	**Oordeel**
	Beheersmaatregel:	Er is door de organisatie uitgewerkt wie met welke (overheids) instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/ calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.6.1.3.2**	**Contact met overheidsinstanties**	**Oordeel**
	Beheersmaatregel:	Het contactoverzicht wordt jaarlijks geactualiseerd.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in steekproef van deze audit
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.6.1.4	**Contact met speciale belangengroepen**	**Oordeel**
	Beheersmaatregel:	Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in steekproef van deze audit
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.6.1.5	**Informatiebeveiliging in projectbeheer**	**Oordeel**
	Beheersmaatregel:	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in steekproef van deze audit
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.6.2.1	**Beleid voor mobiele apparatuur**	**Oordeel**
	Beheersmaatregel:	Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	Geen afwijkingen
	Bewijslast:	DOC-BB-01B Richtlijn Mobile Device Management Intune Admin Center Intune App Protection	
	Interview met:	5.1.2e	
	Toelichting auditor	Er is een uitgebreid beleid aanwezig Mobile Device management. Delen van het beleid worden ook afgedwongen middels Intune MDM.	
Control BBN2	**A.6.2.1.1**	**Beleid voor mobiele apparatuur**	**Oordeel**
	Beheersmaatregel:	Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	Geen afwijkingen
	Bewijslast:	DOC-BB-01B Richtlijn Mobile Device Management Intune Admin Center Intune App Protection Smartphone 5.1.2e	
	Interview met:	5.1.2e	
	Toelichting auditor	Middels M365 InTune is ingesteld dat policies op de mobiele apparaten worden afgedwongen en bewaakt Op de mobiele telefoons zijn zowel een privé als een bedrijfsprofiel aanwezig. (uitwisselen van gegevens hiertussen in niet mogelijk) Delen van het beleid worden ook afgedwongen middels Intune MDM.	
Control BBN2	**A.6.2.1.2**	**Beleid voor mobiele apparatuur**	**Oordeel**

	Beheersmaatregel:	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: a.In bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde. b.Het device maakt deel uit van patchmanagement en hardening. c.er wordt gebruik gemaakt van Mobile Device Management MDM of van Mobile Application Management (MAM)-oplossingen. d.Gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt. e.Periodiek wordt getoetst of de punten in lid b), c) en d) worden nageleefd.	Kans voor verbetering
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	Laptops worden gebruikt als Thinclients om toegang te verkrijgen tot de Citrix Desktop omgeving. Delen van het beleid worden ook afgedwongen middels Intune MDM. Gebruikswijzer is opgezet maar moet nog ondertekend worden door alle medewerkers. De gebruikswijzer is inhoudelijk opgezet met de richtlijnen waar gebruikers zich aan moeten houden en bewustwording over het gebruik. Deze stukken liggen ter goedkeuring bij de OR samen met en gekoppeld aan het voorstel voor de uitlevering van de nieuwe digitale werkplek. Het verbeterproces loopt nog. De KVV blijft nog staan.	
	Bewijslast:	DOC-BB-01B Richtlijn Mobile Device Management Presentatie - Digitale weerbaarheid Presentatie - Provincie en Ik	
	Interview met:	5.1.2e	
	Toelichting auditor	Laptops worden gebruikt als Thinclients om toegang te verkrijgen tot de Citrix Desktop omgeving. Delen van het beleid worden ook afgedwongen middels Intune MDM. Gebruikswijzer is opgezet maar moet nog ondertekend worden door alle medewerkers. De gebruikswijzer is inhoudelijk opgezet met de richtlijnen waar gebruikers zich aan moeten houden en bewustwording over het gebruik. Deze stukken liggen ter goedkeuring bij de OR samen met en gekoppeld aan het voorstel voor de uitlevering van de nieuwe digitale werkplek. Het verbeterproces loopt nog. De KVV blijft nog staan.	
	A.6.2.2	**Beleid voor telewerken**	**Oordeel**
	Beheersmaatregel:	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	DOC-BB-01C - Richtlijn Telewerken	
	Interview met:	5.1.2e	
	Toelichting auditor	Er is een beleid voor telewerken vastgesteld.	
	A.7.1.1	**Screening**	**Oordeel**
	Beheersmaatregel:	Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	Er is nog geen algemeen screening beleid/proces aanwezig. Vanuit de IA is dit reeds vastgesteld en is er een verbeteractie opgestart om dit screening beleid te maken. Dit levert een KVV	
	Bewijslast:	Het Plein - Beleid over verklaring omtrent Gedrag (VOG)	
	Interview met:	5.1.2e	
	Toelichting auditor	Per 1 juli 2023 is er een beleid opgesteld dat van alle medewerkers een VOG aangevraagd. De voorgaande KVV is hiermee effectief opgelost.	
Control BBN1	**A.7.1.1.1**	**Screening**	**Oordeel**
	Beheersmaatregel:	Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan een Verklaring Omtrent het Gedrag (VOG) gevraagd worden.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Het Plein - Beleid over verklaring omtrent Gedrag (VOG)	
	Interview met:	5.1.2e	
	Toelichting auditor	Per 1 juli 2023 is er een beleid opgesteld dat van alle medewerkers een VOG aangevraagd.	
	A.7.1.2	**Arbeidsvoorwaarden**	**Oordeel**

	Beheersmaatregel:	De contractuele overeenkomst met medewerkers en contractanten moet hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	AOK "EW" Collectieve arbeidsvoorwaarde Provincie Personeelshandboek v 1.3.5 januari 2024 AIV Provincies 2018	
	Interview met:	5.1.2e	
	Toelichting auditor	Vanuit de AOK wordt er altijd verwezen naar de CAO en het personeelshandboek. In het personeelshandboek worden de verantwoordelijkheden voor IB vermeld.	
Control BBN1	**A.7.1.2.1**	**Arbeidsvoorwaarden**	**Oordeel**
	Beheersmaatregel:	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	AOK "EW" Collectieve arbeidsvoorwaarde Provincie Personeelshandboek v 1.3.5 januari 2024 AIV Provincies 2018 SharePoint - I&A Beleidsportaal SharePoint - ISMS Provincie Gelderland - 2023 - ISMS richtlijnen	
	Interview met:	5.1.2e	
	Toelichting auditor	Vanuit de AOK wordt er altijd verwezen naar de CAO en het personeelshandboek. In het personeelshandboek worden de verantwoordelijkheden voor IB vermeld. Alle beleidsregels (en richtlijnen) zijn opgenomen in "SharePoint - I&A Beleidsportaal" en voor alle medewerkers beschikbaar	
	A.7.2.1	**Directie-verantwoordelijkheden**	**Oordeel**
	Beheersmaatregel:	De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Ambtenarenwet 2017 AIV Provincies 2018 Gebruikswijzer	
	Interview met:	5.1.2e	
	Toelichting auditor	Alle ambtenaren hebben vanuit de wet hun verantwoordelijkheden. Voor contractanten is dit opgenomen in de AIV.	
Control BBN1	**A.7.2.1.1**	**Directie-verantwoordelijkheden**	**Oordeel**
	Beheersmaatregel:	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen anoniem en veilig beveiligingsissues kan melden.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.7.2.2	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijns-opleiding en -training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Geen afwijkingen
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	DOC-B-01 Beleid Informatiebeveiliging 6-3-2024 Digitale weerbaarheid 2.0 Gelderlandleert.StudyTube.nl e-mail Oproep aanmeling training "Digitale weerbaarheid 2.0" d.d. 6-2-2024 Digitaal Gaan Quizzen 2024 Eindresultaat-werken-2023-quiz_report	
	Interview met:	5.1.2e	
	Toelichting auditor	De CISO geeft alle medewerkers een Introductie/training. Deze training wordt een aantal keren per week gegeven. Hierin worden verschillende regels, procedures en bewustwording toegelicht. Ongeveer 70% heeft de training gevolgd. De Ciso houdt bij wie de training heeft gevolgd en wie nog niet. De directie heeft voor deze training een e-mail naar iedereen gestuurd dat deze training verplicht is om te volgen. Voor 2024 zijn er quiz vragen opgesteld welke om de paar dagen naar alle gebruikers worden gestuurd middels een e-learning achtig systeem (StudyTube)	
Control BBN1	**A.7.2.2.1**	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.7.2.2.2**	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	DOC-B-01 Beleid Informatiebeveiliging 6-3-2024 Digitale weerbaarheid 2.0 Gelderlandleert.StudyTube.nl e-mail Oproep aanmeling training "Digitale weerbaarheid 2.0" d.d. 6-2-2024 Digitaal Gaan Quizzen 2024 Eindresultaat-werken-2023-quiz_report	
	Interview met:	5.1.2e	
	Toelichting auditor	De CISO geeft alle medewerkers een Introductie/training. Deze training wordt een aantal keren per week gegeven. Hierin worden verschillende regels, procedures en bewustwording toegelicht. Ongeveer 70% heeft de training gevolgd. De Ciso houdt bij wie de training heeft gevolgd en wie nog niet. De directie heeft voor deze training een e-mail naar iedereen gestuurd dat deze training verplicht is om te volgen. Voor 2024 zijn er quiz vragen opgesteld welke om de paar dagen naar alle gebruikers worden gestuurd middels een e-learning achtig systeem (StudyTube)	
Control BBN1	**A.7.2.2.3**	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	

Interview met:	0	
Toelichting auditor	0	
A.7.2.3	**Disciplinaire procedure**	**Oordeel**
Beheersmaatregel:	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	=AUDIT!J155	
Relevante bevinding uit vorige audit(s):	=AUDIT!K155	
Bewijslast:	=AUDIT!L155	
Interview met:	=AUDIT!M155	
Toelichting auditor	=AUDIT!N155	
A.7.3.1	**Beëindiging of wijziging van verantwoordelijkheden van het dienstverband**	**Oordeel**
Beheersmaatregel:	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht.	Niet in steekproef van deze audit
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
A.8.1.1	**Inventariseren van bedrijfsmiddelen**	**Oordeel**
Beheersmaatregel:	Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	Topdesk - Configuratiebeheer Topdesk - asset overzicht - Middelen	
Interview met:	5.1.2e	
Toelichting auditor	Er is een inventaris aanwezig van alle bedrijfsmiddelen (Hardware, software, etc.) Alle software wordt 3 keer per jaar gecontroleerd. Voor hardware wordt dit ook steekproefsgewijs gecontroleerd.	
A.8.1.2	**Eigendom van bedrijfsmiddelen**	**Oordeel**
Beheersmaatregel:	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	Topdesk - Configuratiebeheer Topdesk - asset overzicht - Middelen	
Interview met:	5.1.2e	
Toelichting auditor	Hoofd I&A is altijd eigenaar van alle hardware. In de inventarisatie software zijn de Eerste aanspreekpunt, functioneel behandelgroep en technische behandelgroep opgenomen.	
A.8.1.3	**Aanvaardbaar gebruik van bedrijfsmiddelen**	**Oordeel**
Beheersmaatregel:	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	Gebruikswijzer voor apparaten	
Interview met:	5.1.2e	
Toelichting auditor	Het aanvaardbaar gebruik bedrijfsmiddelen is opgenomen in de gebruiksvoorwaarde. (wat een samenvatting is van een aantal richtlijnen)	
Control BBN1 **A.8.1.3.1**	**Aanvaardbaar gebruik van bedrijfsmiddelen**	**Oordeel**
Beheersmaatregel:	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
Relevante bevinding uit vorige audit(s):	0	

	Bewijslast:	Gebruikswijzer voor apparaten	
	Interview met:	5.1.2e	
	Toelichting auditor	Het aanvaardbaar gebruik bedrijfsmiddelen is opgenomen in de gebruiksvoorwaarde. (wat een samenvatting is van een aantal richtlijnen) Deze zijn bij alle medewerkers en externe bekend en later zullen ze deze ook voor akkoord moeten tekenen. Gekoppeld aan de nieuwe werkplek	
Control BBN1	**A.8.1.3.2**	**Aanvaardbaar gebruik van bedrijfsmiddelen**	**Oordeel**
	Beheersmaatregel:	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Gebruikswijzer voor apparaten	
	Interview met:	5.1.2e	
	Toelichting auditor	Het aanvaardbaar gebruik bedrijfsmiddelen is opgenomen in de gebruiksvoorwaarde. (wat een samenvatting is van een aantal richtlijnen) Deze zijn bij alle medewerkers en externe bekend en later zullen ze deze ook voor akkoord moeten tekenen. Gekoppeld aan de nieuwe werkplek	
	A.8.1.4	**Teruggeven van bedrijfsmiddelen**	**Oordeel**
	Beheersmaatregel:	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Topdesk formulier - Inname en uitgifte ICT middelen PRV-2403 1784 In/uitgifte VG	
	Interview met:	5.1.2e	
	Toelichting auditor	In- en uitgifte materiaal wordt gedaan met een geautomatiseerd proces via Topdesk waarbij de gebruiker akkoord moet geven wat ook automatisch wordt vastgelegd in Topdesk in het bijhorende ticket.	
	A.8.2.1	**Classificatie van Informatie**	**Oordeel**
	Beheersmaatregel:	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	DOC-BB-01D Richtlijn Data Classificatie	
	Interview met:	5.1.2e	
	Toelichting auditor	Er zijn classificaties opgesteld voor BIV. Voor Vertrouwelijkheid labels wordt er gewerkt met : Openbaar, intern gebruik, vertrouwelijk en geheim	
Control BBN1	**A.8.2.1.1**	**Classificatie van Informatie**	**Oordeel**
	Beheersmaatregel:	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	DOC-BB-01D Richtlijn Data Classificatie	
	Interview met:	5.1.2e	
	Toelichting auditor	Er zijn classificaties opgesteld voor BIV. Hierin de risicoafwegingen meegenomen. Voor Vertrouwelijkheid labels wordt er gewerkt met: Openbaar, intern gebruik, vertrouwelijk en geheim	
	A.8.2.2	**Informatie labelen**	**Oordeel**
	Beheersmaatregel:	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	DocBase	
	Interview met:	0	
	Toelichting auditor	In Docbase wordt afgedwongen dat ieder document gelabeld moet zijn. Standaard is dat vertrouwelijk en indien een medewerker van SBA een dossier aanmaakt wordt deze standaard/automatisch op geheim gezet.	

	A.8.2.3	Behandelen van bedrijfsmiddelen	Oordeel
	Beheersmaatregel:	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.8.3.1	**Beheer van verwijderbare media**	**Oordeel**
	Beheersmaatregel:	Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Ticket W3201 629 uitfaseren en verwijderen ESX30, ... Certificaat - Data Erasure Report - Blancco d.d. 23-6-2023	
	Interview met:	5.1.2e	
	Toelichting auditor	Alle digitale systemen met informatie bevinden zich in het datacenter (of SaaS) en als de media het datacenter verlaat worden deze leeg gemaakt alvorens deze worden afgevoerd. Voor het leegmaken en verwijderen van de media wordt een gecertificeerd bedrijf ingeschakeld. Als steekproef gezien het verwijderen van de media bij het uitfaseren van ESX30	
Control BBN1	**A.8.3.1.1**	**Beheer van verwijderbare media**	**Oordeel**
	Beheersmaatregel:	Er is een verwijderinstructie waarin is opgenomen dat van verwijderbare media die herbruikbaar zijn en die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd is (ISO 27002 – implementatierichtlijn 8.3.1.a).	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Ticket W3201 629 uitfaseren en verwijderen ESX30, ... Certificaat - Data Erasure Report - Blancco d.d. 23-6-2023	
	Interview met:	5.1.2e	
	Toelichting auditor	Alle digitale systemen met informatie bevinden zich in het datacenter (of SaaS) en als de media het datacenter verlaat worden deze leeg gemaakt alvorens deze worden afgevoerd. Voor het leegmaken en verwijderen van de media wordt een gecertificeerd bedrijf ingeschakeld. Als steekproef gezien het verwijderen van de media bij het uitfaseren van ESX30	
	A.8.3.2	**Verwijderen van media**	**Oordeel**
	Beheersmaatregel:	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Ticket W3201 629 uitfaseren en verwijderen ESX30, ... Certificaat - Data Erasure Report - Blancco d.d. 23-6-2023	
	Interview met:	5.1.2e	
	Toelichting auditor	Alle digitale systemen met informatie bevinden zich in het datacenter (of SaaS) en als de media het datacenter verlaat worden deze leeg gemaakt alvorens deze worden afgevoerd. Voor het leegmaken en verwijderen van de media wordt een gecertificeerd bedrijf ingeschakeld. Als steekproef gezien het verwijderen van de media bij het uitfaseren van ESX30	
Control BBN2	**A.8.3.2.1**	**Verwijderen van media**	**Oordeel**
	Beheersmaatregel:	Media die vertrouwelijke informatie bevatten, zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	

	Relevante bevinding uit vorige audit(s):	0	Geen afwijkingen
	Bewijslast:	Ticket W3201 629 uitfaseren en verwijderen ESX30, ... Certificaat - Data Erasure Report - Blancco d.d. 23-6-2023	
	Interview met:	5.1.2e	
	Toelichting auditor	Alle digitale systemen met informatie bevinden zich in het datacenter (of SaaS) en als de media het datacenter verlaat worden deze leeg gemaakt alvorens deze worden afgevoerd. Voor het leegmaken en verwijderen van de media wordt een gecertificeerd bedrijf ingeschakeld. Als steekproef gezien het verwijderen van de media bij het uitfaseren van ESX30	
Control BBN2	**A.8.3.2.2**	**Verwijderen van media**	**Oordeel**
	Beheersmaatregel:	Verwijdering vindt plaats op een veilige manier, bijvoorbeeld door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie (ISO 27002 – implementatierichtlijn 8.3.2.a).	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Ticket W3201 629 uitfaseren en verwijderen ESX30, ... Certificaat - Data Erasure Report - Blancco d.d. 23-6-2023	
	Interview met:	5.1.2e	
	Toelichting auditor	Alle digitale systemen met informatie bevinden zich in het datacenter (of SaaS) en als de media het datacenter verlaat worden deze leeg gemaakt alvorens deze worden afgevoerd. Voor het leegmaken en verwijderen van de media wordt een gecertificeerd bedrijf ingeschakeld. Als steekproef gezien het verwijderen van de media bij het uitfaseren van ESX30	
Control BBN2	**A.8.3.2.3**	**Verwijderen van media**	**Oordeel**
	Beheersmaatregel:	Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.8.3.3	**Media fysiek overdragen**	**Oordeel**
	Beheersmaatregel:	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.8.3.3.1**	**Media fysiek overdragen**	**Oordeel**
	Beheersmaatregel:	Er is een vastgestelde procedure voor het fysiek transport van media.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.8.3.3.2**	**Media fysiek overdragen**	**Oordeel**
	Beheersmaatregel:	Het gebruik van koeriers of transporteurs voor transport van op BBN2 of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	

	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.9.1.1	**Beleid voor toegangs-beveiliging**	**Oordeel**
	Beheersmaatregel:	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	DOC-BB-01F Richtlijn Logische toegangsbeveiliging Sharepoint Afdeling SBA	
	Interview met:	5.1.2e	
	Toelichting auditor	Er is een beleid voor logische toegangsbeveiliging wat gebaseerd is op RBAC, ABAC en Need-to-Know	
	A.9.1.2	**Toegang tot netwerken en netwerkdiensten**	**Oordeel**
	Beheersmaatregel:	Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Topdesk - W2403 195 van tijdelijk naar vast - W2401 673 MS Visio 5.1.2e PG - Autorisaties - Autorisatieprocedure Contactpersonen rechten op netwerkmappen (d.d. 16-2-2024)	
	Interview met:	5.1.2e	
	Toelichting auditor	Toegang wordt aangevraagd via Topdesk. Waarbij managers vooraf goedkeuring moeten geven bij systemen met gevoelige gegevens. Rechten worden aangevraagd via een MMF (medewerker mutatie formulier) waarvan dan in Topdesk een ticket wordt aangemaakt en alle acties en goedkeuringen worden vastgelegd. Voor OGD is er een overzicht wie welke rechten mogen aanvragen. Deze lijst is 16-2-2024 nog bijgewerkt	
Control BBN1	**A.9.1.2.1**	**Toegang tot netwerken en netwerkdiensten**	**Oordeel**
	Beheersmaatregel:	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	PG- Netwerk overzichtstekening v4.5 Intune Admin Center Intune App Protection	
	Interview met:	5.1.2e	
	Toelichting auditor	Er kan alleen toegang gekregen via Citrix Desktop	
Control BBN1	**A.9.1.2.2**	**Toegang tot netwerken en netwerkdiensten**	**Oordeel**
	Beheersmaatregel:	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	PG- Netwerk overzichtstekening v4.5 Intune Admin Center Intune App Protection	
	Interview met:	5.1.2e	
	Toelichting auditor	Er kan alleen toegang gekregen via Citrix Desktop. Indien via een niet vertrouwd netwerk toegang wordt verkregen tot de Citrix Desktop dan wordt MFA afgedwongen.	
	A.9.2.1	**Registratie en uitschrijving van gebruikers**	**Oordeel**
	Beheersmaatregel:	Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Geen afwijkingen
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Topdesk - W2403 195 van tijdelijk naar vast - W2401 673 MS Visio 5.1.2e - W2212 182 22-12-30 Uit dienst Rutten N PG - Autorisaties - Autorisatieprocedure Contactpersonen rechten op netwerkmappen (d.d. 16-2-2024)	
	Interview met:	5.1.2e	
	Toelichting auditor	Middels formele procedure worden gebruikers aangemaakt en verwijderd.	
Control BBN1	**A.9.2.1.1**	**Registratie en uitschrijving van gebruikers**	**Oordeel**
	Beheersmaatregel:	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Topdesk - W2403 195 van tijdelijk naar vast - W2401 673 MS Visio 5.1.2e - W2212 182 22-12-30 Uit dienst 5.1.2e PG - Autorisaties - Autorisatieprocedure Contactpersonen rechten op netwerkmappen (d.d. 16-2-2024) Accountbeleid rapport 2024-02-19	
	Interview met:	5.1.2e	
	Toelichting auditor	Middels formele procedure worden gebruikers aangemaakt en verwijderd. Het gehele proces wordt geborgd binnen Topdesk. Daarnaast worden na 90 dagen inactiviteit van accounts gedeactiveerd (middels een scripts) als deze dan nogmaals 90 dagen niet worden gebruikt verwijderd. (beoordeling gaat in overleg tussen Ciso en PO)	
Control BBN1	**A.9.2.1.2**	**Registratie en uitschrijving van gebruikers**	**Oordeel**
	Beheersmaatregel:	Het gebruiken van groepsaccounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Accountbeleid (24-1-2024)	
	Interview met:	5.1.2e	
	Toelichting auditor	Er worden geen groepsaccounts gebruikt deze zijn ook niet toegestaan	
	A.9.2.2	**Gebruikers toegang verlenen**	**Oordeel**
	Beheersmaatregel:	Een formele gebruikerstoegangs-verleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Topdesk - W2403 195 van tijdelijk naar vast - W2401 673 MS Visio 5.1.2e PG - Autorisaties - Autorisatieprocedure Contactpersonen rechten op netwerkmappen (d.d. 16-2-2024)	
	Interview met:	5.1.2e	
	Toelichting auditor	Toegang/wijzigingen worden aangevraagd via MMF (medewerker mutatie formulier)/Topdesk. Waarbij managers vooraf goedkeuring moeten geven bij systemen met gevoelige gegevens. Rechten worden aangevraagd via een MMF (medewerker mutatie formulier) waarvan dan in Topdesk een ticket wordt aangemaakt en alle acties en goedkeuringen worden vastgelegd. Voor OGD is er een overzicht wie welke rechten mogen aanvragen. Deze lijst is 16-2-2024 nog bijgewerkt	
Control BBN1	**A.9.2.2.1**	**Gebruikers toegang verlenen**	**Oordeel**
	Beheersmaatregel:	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Geen afwijkingen
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Topdesk - W2403 195 van tijdelijk naar vast - W2401 673 MS Visio 5.1.2e PG - Autorisaties - Autorisatieprocedure Contactpersonen rechten op netwerkmappen (d.d. 16-2-2024)	
	Interview met:	5.1.2e	
	Toelichting auditor	Toegang/wijzigingen worden aangevraagd via MMF (medewerker mutatie formulier)/Topdesk. Waarbij managers vooraf goedkeuring moeten geven bij systemen met gevoelige gegevens. Rechten worden aangevraagd via een MMF (medewerker mutatie formulier) waarvan dan in Topdesk een ticket wordt aangemaakt en alle acties en goedkeuringen worden vastgelegd. Voor OGD is er een overzicht wie welke rechten mogen aanvragen. Deze lijst is 16-2-2024 nog bijgewerkt	
Control BBN1	**A.9.2.2.2**	**Gebruikers toegang verlenen**	**Oordeel**
	Beheersmaatregel:	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.9.2.2.3**	**Gebruikers toegang verlenen**	**Oordeel**
	Beheersmaatregel:	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Topdesk - W2403 195 van tijdelijk naar vast - W2401 673 MS Visio 5.1.2e PG - Autorisaties - Autorisatieprocedure Contactpersonen rechten op netwerkmappen (d.d. 16-2-2024)	
	Interview met:	5.1.2e	
	Toelichting auditor	Voor OGD is er een overzicht wie welke rechten mogen aanvragen. Deze lijst is 16-2-2024 nog bijgewerkt	
	A.9.2.3	**Beheren van speciale toegangsrechten**	**Oordeel**
	Beheersmaatregel:	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	OGD Portal - Provincie Gelderland AD - Provincie Gelderland - overzicht Sys- accounts - Account instellingen 5.1.2e Accountbeleid_rapport_2024-02-19	
	Interview met:	5.1.2e	
	Toelichting auditor	Beheerders hebben naast hun normale gebruikers accounts ook aparte beheer accounts. Deze accounts worden ook automatisch geblokkeerd na 90 dagen inactiviteit. Binnen OGD heeft iedereen een persoonlijk Admin Account. Leden van het reguliere beheer team hebben admin accounts. Bij ondersteunende engineers / specialiste wordt er gebruik gemaakt van JIT Admin accounts. Bij de maandelijkse rapportage worden ook de Admin accounts beoordeeld (door OGD zelf en de Ciso).	
Control BBN2	**A.9.2.3.1**	**Beheren van speciale toegangsrechten**	**Oordeel**
	Beheersmaatregel:	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Geen afwijkingen
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	OGD Portal - Provincie Gelderland AD - Provincie Gelderland - overzicht Sys- accounts - Account instellingen 5.1.2e Accountbeleid_rapport_2024-02-19	
	Interview met:	5.1.2e	
	Toelichting auditor	Beheerders hebben naast hun normale gebruikers accounts ook aparte beheer accounts. Deze accounts worden ook automatisch geblokkeerd na 90 dagen inactiviteit. Binnen OGD heeft iedereen een persoonlijk Admin Account. Leden van het reguliere beheer team hebben admin accounts. Bij ondersteunende engineers / specialiste wordt er gebruik gemaakt van JIT Admin accounts. Bij de maandelijkse rapportage worden ook de Admin accounts beoordeeld (door OGD zelf en de Ciso).	
	A.9.2.4	**Beheer van geheime authenticatieinformatie van gebruikers**	**Oordeel**
	Beheersmaatregel:	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in steekproef van deze audit
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.9.2.5	**Beoordeling van toegangsrechten van gebruikers**	**Oordeel**
	Beheersmaatregel:	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	OA 5543 Controle Mutaties op autorisatie OA 6115 Controle Mutaties op autorisatie OA 5238 Contreoleren en verwijderen inactieven accounts Accountbeleid_rapport_2024-02-19	Geen afwijkingen
	Interview met:	5.1.2e	
	Toelichting auditor	Middels verschillende Operationele activiteiten in Topdesk worden rechten gecontroleerd. Deze rechten worden maandelijks of per kwartaal gecontroleerd. Alle domainadmins worden maandelijks beoordeeld door de CISO middels het_Accountbeleid_rapport.	
Control BBN1	**A.9.2.5.1**	**Beoordeling van toegangsrechten van gebruikers**	**Oordeel**
	Beheersmaatregel:	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	OA 5543 Controle Mutaties op autorisatie OA 6115 Controle Mutaties op autorisatie OA 5238 Contreoleren en verwijderen inactieven accounts Accountbeleid_rapport_2024-02-19	Geen afwijkingen
	Interview met:	5.1.2e	
	Toelichting auditor	Middels verschillende Operationele activiteiten in Topdesk worden rechten gecontroleerd. Deze rechten worden maandelijks of per kwartaal gecontroleerd. Alle domainadmins worden maandelijks beoordeeld door de CISO middels het_Accountbeleid_rapport.	
Control BBN1	**A.9.2.5.2**	**Beoordeling van toegangsrechten van gebruikers**	**Oordeel**
	Beheersmaatregel:	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in steekproef van deze audit
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	

	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.9.2.5.3**	**Beoordeling van toegangsrechten van gebruikers**	**Oordeel**
	Beheersmaatregel:	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	OA 5543 Controle Mutaties op autorisatie OA 6115 Controle Mutaties op autorisatie OA 5238 Contreoleren en verwijderen inactieven accounts Accountbeleid_rapport_2024-02-19	
	Interview met:	5.1.2e	
	Toelichting auditor	Middels verschillende Operationele activiteiten in Topdesk worden rechten gecontroleerd. Deze rechten worden maandelijks of per kwartaal gecontroleerd. Alle domainadmins worden maandelijks beoordeeld door de CISO middels het Accountbeleid_rapport.	
	A.9.2.6	**Toegangsrechten intrekken of aanpassen**	**Oordeel**
	Beheersmaatregel:	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.9.3.1	**Geheime authenticatie-informatie gebruiken**	**Oordeel**
	Beheersmaatregel:	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.9.3.1.1**	**Geheime authenticatie-informatie gebruiken**	**Oordeel**
	Beheersmaatregel:	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	DOC-BB-01L Richtlijn wachtwoordbeheer AD - Groups - APP_Keepass (2.52 1.37)	
	Interview met:	5.1.2e	
	Toelichting auditor	Alle medewerkers hebben de mogelijkheid om gebruik te maken van een wachtwoordkluis KeePass. Na een aanvraag worden ze toegevoegd aan een AD groep (APP-KeePass) en krijgen daarmee automatisch KeePass geïnstalleerd/beschikbaar.	
	A.9.4.1	**Beperking toegang tot informatie**	**Oordeel**
	Beheersmaatregel:	Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.9.4.1.1**	**Beperking toegang tot informatie**	**Oordeel**

	Beheersmaatregel:	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.9.4.1.2**	**Beperking toegang tot informatie**	**Oordeel**
	Beheersmaatregel:	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Nieuw MMF proces (medewerkers mutatie formulier) Accountbeleid_rapport 2023_03_20 OA 5543 Controle Mutaties op autorisatie DocBase	
	Interview met:	5.1.2e	
	Toelichting auditor	Met betrekking tot de afdeling SBA (Bibob proces) , alleen medewerker hebben toegang tot de zaaknummers in Docbase waartoe zijn gemachtigd zijn.	
	A.9.4.2	**Beveiligde inlogprocedures**	**Oordeel**
	Beheersmaatregel:	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Azure AD - Identity Protection Weekly Digest Azure AD - Conditional Access Policies	
	Interview met:	5.1.2e	
	Toelichting auditor	Alle medewerkers loggen in met een AD account waarop MFA actief is.	
Control BBN1	**A.9.4.2.1**	**Beveiligde inlogprocedures**	**Oordeel**
	Beheersmaatregel:	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Azure AD - Identity Protection Weekly Digest Azure AD - Conditional Access Policies	
	Interview met:	5.1.2e	
	Toelichting auditor	Er kan alleen toegang gekregen via Citrix Desktop. Indien via een niet vertrouwd netwerk toegang wordt verkregen tot de Citrix Desktop dan wordt MFA afgedwongen.	
Control BBN2	**A.9.4.2.2**	**Beveiligde inlogprocedures**	**Oordeel**
	Beheersmaatregel:	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.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.9.4.3	**Systeem voor wachtwoordbeheer**	**Oordeel**

	Beheersmaatregel:	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	KeePass Accountbeleid_rapport_2024-02-19 Accountbeleid (24-1-2024) DOC-BB-01L Richtlijn Wachtwoorden. AD - Policies - Password Policy Intune Admin Center Intune App Protection	
	Interview met:	5.1.2e	
	Toelichting auditor	Voor wachtwoord beheer kunnen alle medewerkers het gebruik van KeePass aanvragen. Alle medewerkers hebben in basis maar één account waarvan binnen de AD wordt afgedwongen dat deze een sterk wachtwoord heeft	
Control BBN1	**A.9.4.3.1**	**Systeem voor wachtwoordbeheer**	**Oordeel**
	Beheersmaatregel:	Als er geen gebruik wordt gemaakt van two-factor authenticatie, is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal foutieve inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen, is vastgelegd	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	KeePass Accountbeleid_rapport_2024-02-19 Accountbeleid (24-1-2024) DOC-BB-01L Richtlijn Wachtwoorden. AD - Policies - Password Policy Intune Admin Center Intune App Protection	
	Interview met:	5.1.2e	
	Toelichting auditor	Voor wachtwoord beheer kunnen alle medewerkers het gebruik van KeePass aanvragen. Alle medewerkers hebben is basis maar een account waarvan binnen de AD wordt afgedwongen dat dit een sterk wachtwoord is. Gewone account moeten o.a. minimaal 9 karakters zijn en service accounts 12 karakters	
Control BBN2	**A.9.4.3.2**	**Systeem voor wachtwoordbeheer**	**Oordeel**
	Beheersmaatregel:	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1).	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	KeePass Accountbeleid_rapport_2024-02-19 Accountbeleid (24-1-2024) DOC-BB-01L Richtlijn Wachtwoorden. AD - Policies - Password Policy Intune Admin Center Intune App Protection	
	Interview met:	5.1.2e	
	Toelichting auditor	Wachtwoorden moeten ieder 90 dagen aangepast worden (laatste 10 worden onthouden)	
Control BBN2	**A.9.4.3.3**	**Systeem voor wachtwoordbeheer**	**Oordeel**
	Beheersmaatregel:	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	

	Bewijslast:	KeePass Accountbeleid_rapport_2024-02-19 Accountbeleid (24-1-2024) DOC-BB-01L Richtlijn Wachtwoorden. AD - Policies - Password Policy Intune Admin Center Intune App Protection	Geen afwijkingen
	Interview met:	5.1.2e	
	Toelichting auditor	Voor wachtwoord beheer kunnen alle medewerkers het gebruik van KeePass aanvragen. Alle medewerkers hebben is basis maar een account waarvan binnen de AD wordt afgedwongen dat dit een sterk wachtwoord is. Gewone account moeten o.a. minimaal 9 karakters zijn en service accounts 12 karakters	
Control BBN2	**A.9.4.3.4**	**Systeem voor wachtwoordbeheer**	**Oordeel**
	Beheersmaatregel:	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	KeePass Accountbeleid_rapport_2024-02-19 Accountbeleid (24-1-2024) DOC-BB-01L Richtlijn Wachtwoorden. AD - Policies - Password Policy Intune Admin Center Intune App Protection	
	Interview met:	5.1.2e	
	Toelichting auditor	Er is afgedwongen in de AD dat wachtwoorden na de eerste inlog moeten worden aangepast.	
Control BBN2	**A.9.4.3.5**	**Systeem voor wachtwoordbeheer**	**Oordeel**
	Beheersmaatregel:	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 zes maanden.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	=AUDIT!I211	
	Bewijslast:	=AUDIT!J211	
	Interview met:	=AUDIT!K211	
	Toelichting auditor	=AUDIT!L211	
	A.9.4.4	**Speciale systeemhulpmiddelen gebruiken**	**Oordeel**
	Beheersmaatregel:	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.9.4.4.1**	**Speciale systeemhulpmiddelen gebruiken**	**Oordeel**
	Beheersmaatregel:	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.9.4.4.2**	**Speciale systeemhulpmiddelen gebruiken**	**Oordeel**
	Beheersmaatregel:	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	

	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.9.4.5	**Toegangsbeveiliging op programmabroncode**	**Oordeel**
	Beheersmaatregel:	Toegang tot de programmabroncode moet worden beperkt.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.10.1.1	**Beleid inzake het gebruik van cryptografische beheersmaatregelen**	**Oordeel**
	Beheersmaatregel:	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.10.1.1.1**	**Beleid inzake het gebruik van cryptografische beheersmaatregelen**	**Oordeel**
	Beheersmaatregel:	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.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.10.1.1.2**	**Beleid inzake het gebruik van cryptografische beheersmaatregelen**	**Oordeel**
	Beheersmaatregel:	Cryptografische toepassingen voldoen aan passende standaarden	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.10.1.2	**Sleutelbeheer**	**Oordeel**
	Beheersmaatregel:	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.10.1.2.1**	**Sleutelbeheer**	**Oordeel**
	Beheersmaatregel:	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.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.10.1.2.2**	**Sleutelbeheer**	**Oordeel**
	Beheersmaatregel:	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.11.1.1	**Fysieke beveiligingszone**	**Oordeel**
	Beheersmaatregel:	Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie-verwerkende faciliteiten bevatten.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.11.1.1.1**	**Fysieke beveiligingszone**	**Oordeel**
	Beheersmaatregel:	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.11.1.2	**Fysieke toegangs-beveiliging voor beveiligde gebieden**	**Oordeel**
	Beheersmaatregel:	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.11.1.2.1**	**Fysieke toegangs-beveiliging voor beveiligde gebieden**	**Oordeel**
	Beheersmaatregel:	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.11.1.3	**Kantoren, ruimten en faciliteiten beveiligen**	**Oordeel**
	Beheersmaatregel:	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.11.1.3.1**	**Kantoren, ruimten en faciliteiten beveiligen**	**Oordeel**
	Beheersmaatregel:	Sleutelbeheer is ingericht op basis van een sleutelplan.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.11.1.4	**Beschermen tegen bedreigingen van buitenaf**	**Oordeel**
	Beheersmaatregel:	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.11.1.4.1**	**Beschermen tegen bedreigingen van buitenaf**	**Oordeel**
	Beheersmaatregel:	De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.11.1.4.2**	**Beschermen tegen bedreigingen van buitenaf**	**Oordeel**
	Beheersmaatregel:	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.11.1.5	**Werken in beveiligde gebieden**	**Oordeel**
	Beheersmaatregel:	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.11.1.6	**Laad- en Loslocatie**	**Oordeel**
	Beheersmaatregel:	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	

Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
A.11.2.1	**Plaatsing en bescherming van apparatuur**	**Oordeel**
Beheersmaatregel:	Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
A.11.2.2	**Nutsvoorzieningen**	**Oordeel**
Beheersmaatregel:	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen..	
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
A.11.2.3	**Beveiliging van bekabeling**	**Oordeel**
Beheersmaatregel:	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
A.11.2.4	**Onderhoud van apparatuur**	**Oordeel**
Beheersmaatregel:	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
A.11.2.5	**Verwijdering van bedrijfsmiddelen**	**Oordeel**
Beheersmaatregel:	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
A.11.2.6	**Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein**	**Oordeel**
Beheersmaatregel:	Bedrijfsmiddelen die zich buiten het terrein bevinden moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.11.2.7	**Veilig verwijderen of hergebruiken van apparatuur**	**Oordeel**
	Beheersmaatregel:	Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.11.2.8	**Onbeheerde gebruikersapparatuur**	**Oordeel**
	Beheersmaatregel:	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.11.2.9	**'Clear desk'- en 'clear screen'-beleid**	**Oordeel**
	Beheersmaatregel:	Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.11.2.9.1**	**'Clear desk'- en 'clear screen'-beleid**	**Oordeel**
	Beheersmaatregel:	Een onbemensde werkplek is altijd vergrendeld.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.11.2.9.2**	**'Clear desk'- en 'clear screen'-beleid**	**Oordeel**
	Beheersmaatregel:	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.11.2.9.3**	**'Clear desk'- en 'clear screen'-beleid**	**Oordeel**
	Beheersmaatregel:	Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.11.2.9.4**	**'Clear desk'- en 'clear screen'-beleid**	**Oordeel**
	Beheersmaatregel:	Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.11.2.9.5**	**'Clear desk'- en 'clear screen'-beleid**	**Oordeel**
	Beheersmaatregel:	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingslock automatisch geactiveerd	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.1.1	**Gedocumenteerde bedieningsprocedures**	**Oordeel**
	Beheersmaatregel:	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.1.2	**Wijzigingsbeheer**	**Oordeel**
	Beheersmaatregel:	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.1.2.1**	**Wijzigingsbeheer**	**Oordeel**
	Beheersmaatregel:	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: a.het administreren van wijzigingen; b.risicoafweging van mogelijke gevolgen van de wijzigingen; c.goedkeuringsprocedure voor wijzigingen.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.1.3	**Capaciteitsbeheer**	**Oordeel**

	Beheersmaatregel:	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.1.4	**Scheiding van ontwikkel-, test- en productieomgevingen**	**Oordeel**
	Beheersmaatregel:	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.12.1.4.1**	**Scheiding van ontwikkel-, test- en productieomgevingen**	**Oordeel**
	Beheersmaatregel:	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.12.1.4.2**	**Scheiding van ontwikkel-, test- en productieomgevingen**	**Oordeel**
	Beheersmaatregel:	Wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.2.1	**Beheersmaatregelen tegen malware**	**Oordeel**
	Beheersmaatregel:	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.2.1.1**	**Beheersmaatregelen tegen malware**	**Oordeel**
	Beheersmaatregel:	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.2.1.2**	**Beheersmaatregelen tegen malware**	**Oordeel**
	Beheersmaatregel:	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.2.1.3**	**Beheersmaatregelen tegen malware**	**Oordeel**
	Beheersmaatregel:	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.2.1.4**	**Beheersmaatregelen tegen malware**	**Oordeel**
	Beheersmaatregel:	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.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.2.1.5**	**Beheersmaatregelen tegen malware**	**Oordeel**
	Beheersmaatregel:	De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.3.1	**Back-up van informatie**	**Oordeel**
	Beheersmaatregel:	Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.3.1.1**	**Back-up van informatie**	**Oordeel**
	Beheersmaatregel:	Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.3.1.2**	**Back-up van informatie**	**Oordeel**

	Beheersmaatregel:	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.12.3.1.3**	**Back-up van informatie**	**Oordeel**
	Beheersmaatregel:	In het back-upbeleid staan minimaal de volgende eisen: a.Dataverlies bedraagt maximaal 28 uur. b.Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.12.3.1.4**	**Back-up van informatie**	**Oordeel**
	Beheersmaatregel:	Het back-upproces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.12.3.1.5**	**Back-up van informatie**	**Oordeel**
	Beheersmaatregel:	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.4.1	**Gebeurtenissen registreren**	**Oordeel**
	Beheersmaatregel:	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligings-gebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.4.1.1**	**Gebeurtenissen registreren**	**Oordeel**
	Beheersmaatregel:	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.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	

	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.4.1.2**	**Gebeurtenissen registreren**	**Oordeel**
	Beheersmaatregel:	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.12.4.1.3**	**Gebeurtenissen registreren**	**Oordeel**
	Beheersmaatregel:	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.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.12.4.1.4**	**Gebeurtenissen registreren**	**Oordeel**
	Beheersmaatregel:	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.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.12.4.1.5**	**Gebeurtenissen registreren**	**Oordeel**
	Beheersmaatregel:	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.4.2	**Beschermen van informatie in logbestanden**	**Oordeel**
	Beheersmaatregel:	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.4.2.1**	**Beschermen van informatie in logbestanden**	**Oordeel**
	Beheersmaatregel:	Er is een overzicht van logbestanden die worden gegenereerd.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.4.2.2**	**Beschermen van informatie in logbestanden**	**Oordeel**
	Beheersmaatregel:	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.12.4.2.3**	**Beschermen van informatie in logbestanden**	**Oordeel**
	Beheersmaatregel:	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.12.4.2.4**	**Beschermen van informatie in logbestanden**	**Oordeel**
	Beheersmaatregel:	Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.4.3	**Logbestanden van beheerders en operators**	**Oordeel**
	Beheersmaatregel:	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.4.4	**Kloksynchronisatie**	**Oordeel**
	Beheersmaatregel:	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.5.1	**Software installeren op operationele systemen**	**Oordeel**
	Beheersmaatregel:	Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.6.1	**Beheersing van technische kwetsbaarheden**	**Oordeel**
	Beheersmaatregel:	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.12.6.1.1**	**Beheersing van technische kwetsbaarheden**	**Oordeel**
	Beheersmaatregel:	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.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.6.2	**Beperkingen voor het installeren van software**	**Oordeel**
	Beheersmaatregel:	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.12.6.2.1**	**Beperkingen voor het installeren van software**	**Oordeel**
	Beheersmaatregel:	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan wat via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.12.7.1	**Beheersmaatregelen betreffende audits van informatiesystemen**	**Oordeel**
	Beheersmaatregel:	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.13.1.1	**Beheersmaatregelen voor netwerken**	**Oordeel**
	Beheersmaatregel:	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Geen afwijkingen
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	OGD SLA FMO versie 1.5	
	Interview met:	5.1.2e	
	Toelichting auditor	Het beheer van het netwerk is uitbesteed aan OGD	
	A.13.1.2	**Beveiliging van netwerkdiensten**	**Oordeel**
	Beheersmaatregel:	Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Geen afwijkingen
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	OGD SLA FMO versie 1.5 PRTG Portal Netscaler Portal	
	Interview met:	5.1.2e	
	Toelichting auditor	Het netwerk wordt beschermd middels Firewalls en Citrix Netscaler	
Control BBN2	**A.13.1.2.1**	**Beveiliging van netwerkdiensten**	**Oordeel**
	Beheersmaatregel:	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.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Geen afwijkingen
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Palo Alto Firewall FOX-IT meldingen December 2023 (meldingen naar aanleiding van Pentest)	
	Interview met:	5.1.2e	
	Toelichting auditor	Middels een NG Firewall wordt al het verkeer bewaakt. FOX-IT bewaakt al het verkeer voor GLD	
Control BBN2	**A.13.1.2.2**	**Beveiliging van netwerkdiensten**	**Oordeel**
	Beheersmaatregel:	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).	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Geen afwijkingen
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	FOX-IT Portal FOX-IT_contract_-_OFF-O-154372_MSS_NL_GLD	
	Interview met:	5.1.2e	
	Toelichting auditor	De CISO doet alle meldingen naar NCSC	
Control BBN2	**A.13.1.2.3**	**Beveiliging van netwerkdiensten**	**Oordeel**
	Beheersmaatregel:	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.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Geen afwijkingen
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Palo Alto Firewall PG- Netwerk overzichtstekening v4.5 Clearpass Policy Manager (NAC oplossing) Aruba	

	Interview met:	5.1.2e	
	Toelichting auditor	Er wordt gewerkt met Citrix Desktop waarbij de verbinding altijd versleuteld is. Middels een NAC oplossing wordt bepaald of een apparaat direct toegang heeft tot de Datacenters (via DarkFiber verbindingen) of alleen tot Internet (via de normale internetlijnen)	
Control BBN1	**A.13.1.2.4**	**Beveiliging van netwerkdiensten**	**Oordeel**
	Beheersmaatregel:	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.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Image - Traffic network requests OGD SLA FMO versie 1.5	
	Interview met:	5.1.2e	
	Toelichting auditor	Er wordt gebruik gemaakt van de NAWAS dienst via Equinix. Dit is onderdeel van de overeenkomst met OGD (Equinix)	
	A.13.1.3	**Scheiding in netwerken**	**Oordeel**
	Beheersmaatregel:	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Palo Alto Firewall PG- Netwerk overzichtstekening v4.5 Clearpass Policy Manager (NAC oplossing)	
	Interview met:	5.1.2e	
	Toelichting auditor	Het netwerk is opgesplitst in verschillende VLAN's en VRF's om scheiding aan te brengen in de verschillende onderdelen. Middels een NAC-oplossing wordt er bepaald welke toegang een systeem krijgt. Bijvoorbeeld alleen toegang internet of direct toegang tot het datacenter.	
Control BBN2	**A.13.1.3.1**	**Scheiding in netwerken**	**Oordeel**
	Beheersmaatregel:	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Palo Alto Firewall PG- Netwerk overzichtstekening v4.5 Clearpass Policy Manager (NAC oplossing) Aruba	
	Interview met:	5.1.2e	
	Toelichting auditor	Het netwerk is opgesplitst in verschillende VLAN's en VRF's om scheiding aan te brengen in de verschillende onderdelen. Middels een NAC-oplossing wordt er bepaald welke toegang een systeem krijgt. Bijvoorbeeld alleen toegang internet of direct toegang tot het datacenter.	
	A.13.2.1	**Beleid en procedures voor informatietransport (via communicatie-faciliteiten)**	**Oordeel**
	Beheersmaatregel:	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.13.2.2	**Overeenkomsten over informatietransport (met externe partijen.)**	**Oordeel**
	Beheersmaatregel:	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in steekproef van deze audit
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.13.2.3	**Elektronische berichten**	**Oordeel**
	Beheersmaatregel:	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in steekproef van deze audit
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.13.2.3.1**	**Elektronische berichten**	**Oordeel**
	Beheersmaatregel:	Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en afluisteren op de 'pas toe of leg uit'- lijst van het Forum. Voor beveiliging van websiteverkeer gelden de open standaarden tegen afluisteren op de 'pas toe of leg uit'-lijst van het Forum.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Geen afwijkingen
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Citrix Netscaler Portal	
	Interview met:	5.1.2e	
	Toelichting auditor	Oudere Cipher encrypties zijn standaard geblokkeerd in de Netscaler	
Control BBN2	**A.13.2.3.2**	**Elektronische berichten**	**Oordeel**
	Beheersmaatregel:	Voor veilige berichtenuitwisseling met basisregistraties wordt, conform de 'pas toe of leg uit'-lijst van het Forum, gebruik gemaakt van de actuele versie van Digikoppeling.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in steekproef van deze audit
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.13.2.3.3**	**Elektronische berichten**	**Oordeel**
	Beheersmaatregel:	Maak gebruik van PKIoverheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in steekproef van deze audit
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.13.2.3.4**	**Elektronische berichten**	**Oordeel**
	Beheersmaatregel:	Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard. Toepassing bij: Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in steekproef van deze audit
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	

	Interview met:	0	
	Toelichting auditor	0	
	A.13.2.4	**Vertrouwelijkheids- of geheimhoudingsovereenkomst**	**Oordeel**
	Beheersmaatregel:	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.14.1.1	**Analyse en specificatie van informatiebeveiligingseisen**	**Oordeel**
	Beheersmaatregel:	De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.14.1.1.1**	**Analyse en specificatie van informatiebeveiligingseisen**	**Oordeel**
	Beheersmaatregel:	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.14.1.2	**Toepassingsdiensten op openbare netwerken beveiligen**	**Oordeel**
	Beheersmaatregel:	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.14.1.3	**Transacties van toepassingsdiensten beschermen**	**Oordeel**
	Beheersmaatregel:	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.14.2.1	**Beleid voor beveiligd ontwikkelen**	**Oordeel**
	Beheersmaatregel:	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	

	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.14.2.1.1**	**Beleid voor beveiligd ontwikkelen**	**Oordeel**
	Beheersmaatregel:	De gangbare principes rondom 'security by design' zijn uitgangspunt voor de ontwikkeling van software en systemen.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	Als uitgangspunten voor ontwikkelen wordt de OWASP top 10 . Deze zijn echter niet meer geactualiseerd en levert een KVV	
	Bewijslast:	O&O Ontwikkelrichtlijnen v1.3 d.d. 1-5-2023	
	Interview met:	5.1.2e	
	Toelichting auditor	De O&O Ontwikkelrichtlijnen zijn aangepast en verwijzen nu wel naar de OWASP richtlijnen van 2021. De voorgaande KVV is hiermee effectief opgelost.	
	A.14.2.2	**Procedures voor wijzigingsbeheer met betrekking tot systemen**	**Oordeel**
	Beheersmaatregel:	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.14.2.2.1**	**Procedures voor wijzigingsbeheer met betrekking tot systemen**	**Oordeel**
	Beheersmaatregel:	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.14.2.3	**Technische beoordeling van toepassingen na wijzigingen bedieningsplatform**	**Oordeel**
	Beheersmaatregel:	Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.14.2.4	**Beperkingen op wijzigingen aan softwarepakketten**	**Oordeel**
	Beheersmaatregel:	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.14.2.5	**Principes voor engineering van beveiligde systemen**	**Oordeel**
	Beheersmaatregel:	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	

	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.14.2.5.1**	**Principes voor engineering van beveiligde systemen**	**Oordeel**
	Beheersmaatregel:	Zie overheidsmaatregel 14.2.1.1 : Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.14.2.6	**Beveiligde ontwikkelingsomgeving**	**Oordeel**
	Beheersmaatregel:	Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.14.2.6.1**	**Beveiligde ontwikkelingsomgeving**	**Oordeel**
	Beheersmaatregel:	Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.14.2.7	**Uitbestede software- ontwikkeling**	**Oordeel**
	Beheersmaatregel:	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.14.2.7.1**	**Uitbestede software- ontwikkeling**	**Oordeel**
	Beheersmaatregel:	Een voorwaarde voor uitbestedingstrajecten is een expliciete risico afweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.14.2.8	**Testen van systeembeveiliging**	**Oordeel**
	Beheersmaatregel:	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	

	A.14.2.9	**Systeemacceptatietests**	**Oordeel**
	Beheersmaatregel:	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.14.2.9.1**	**Systeemacceptatietests**	**Oordeel**
	Beheersmaatregel:	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.14.2.9.2**	**Systeemacceptatietests**	**Oordeel**
	Beheersmaatregel:	Van de resultaten van de testen wordt verslag gemaakt.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.14.3.1	**Bescherming van testgegevens**	**Oordeel**
	Beheersmaatregel:	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.15.1.1	**Informatiebeveiligings-beleid voor leveranciersrelaties**	**Oordeel**
	Beheersmaatregel:	Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.	Kans voor verbetering
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	Het programma van eisen wordt altijd bepaald aan de hand van de ICO Wizard. De werkwijze en afspraken zijn niet expliciet vastgelegd/beschreven. Er zijn acties gepland om dit te formaliseren maar nog niet uitgevoerd. De voorgaande KVV is nog niet effectief opgelost en blijft staan.	
	Bewijslast:	AIV GLD 2018 voor leveringen en diensten ICO Wizard ICO-Export Datamask (DM) Advies nodig aanbesteding Meetnet (ICO export)	
	Interview met:	5.1.2e	
	Toelichting auditor	Het programma van eisen wordt altijd bepaald aan de hand van de ICO Wizard. De werkwijze en afspraken zijn niet expliciet vastgelegd/beschreven. Er zijn acties gepland om dit te formaliseren maar nog niet uitgevoerd. De voorgaande KVV is nog niet effectief opgelost en blijft staan.	
Control BBN1	**A.15.1.1.1**	**Informatiebeveiligings-beleid voor leveranciersrelaties**	**Oordeel**
	Beheersmaatregel:	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen ten aanzien van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.15.1.1.2**	**Informatiebeveiligings-beleid voor leveranciersrelaties**	**Oordeel**
	Beheersmaatregel:	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekking tot leverancierstoegang tot bedrijfsinformatie vastgesteld.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.15.1.1.3**	**Informatiebeveiligings-beleid voor leveranciersrelaties**	**Oordeel**
	Beheersmaatregel:	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.15.1.2	**Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten**	**Oordeel**
	Beheersmaatregel:	Alle relevante informatiebeveiligings-eisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuur-elementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.15.1.2.1**	**Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten**	**Oordeel**
	Beheersmaatregel:	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.15.1.2.2**	**Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten**	**Oordeel**
	Beheersmaatregel:	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.15.1.2.3**	**Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten**	**Oordeel**

	Beheersmaatregel:	In situaties waarin contractvoorwaarden worden opgelegd door leveranciers, is voorafgaand aan het tekenen van het contract met een risicoafweging helder gemaakt wat de consequenties hiervan zijn voor de organisatie. Expliciet is gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd moeten zijn bij het aangaan van de overeenkomst.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.15.1.2.4**	**Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten**	**Oordeel**
	Beheersmaatregel:	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaardvoorwaarden voor inkoop gehanteerd.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.15.1.2.5**	**Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten**	**Oordeel**
	Beheersmaatregel:	Voordat een contract wordt afgesloten, wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.15.1.2.6**	**Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten**	**Oordeel**
	Beheersmaatregel:	In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst. Een audit is niet nodig als de contractant door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.15.1.3	**Toeleveringsketen van informatie- en communicatie-technologie**	**Oordeel**
	Beheersmaatregel:	Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligings-risico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.15.1.3.1**	**Toeleveringsketen van informatie- en communicatie-technologie**	**Oordeel**
	Beheersmaatregel:	Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	

	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.15.2.1	**Monitoring en beoordeling van dienstverlening van leveranciers**	**Oordeel**
	Beheersmaatregel:	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.15.2.1.1**	**Monitoring en beoordeling van dienstverlening van leveranciers**	**Oordeel**
	Beheersmaatregel:	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.15.2.2	**Beheer van veranderingen in dienstverlening van leveranciers**	**Oordeel**
	Beheersmaatregel:	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.16.1.1	**Verantwoordelijkheden en procedures**	**Oordeel**
	Beheersmaatregel:	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatie-beveiligingsincidenten te bewerkstelligen.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.16.1.2	**Rapportage van informatiebeveiligings-gebeurtenissen**	**Oordeel**
	Beheersmaatregel:	Informatiebeveiligings-gebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.16.1.2.1**	**Rapportage van informatiebeveiligings-gebeurtenissen**	**Oordeel**
	Beheersmaatregel:	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.	
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	

	Toelichting auditor	0	
Control BBN1	**A.16.1.2.2**	**Rapportage van informatiebeveiligings-gebeurtenissen**	**Oordeel**
	Beheersmaatregel:	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.16.1.2.3**	**Rapportage van informatiebeveiligings-gebeurtenissen**	**Oordeel**
	Beheersmaatregel:	Alle medewerkers en contractanten hebben aantoonbaar kennisgenomen van de meldingsprocedure van incidenten.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.16.1.2.4**	**Rapportage van informatiebeveiligings-gebeurtenissen**	**Oordeel**
	Beheersmaatregel:	Incidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.16.1.2.5**	**Rapportage van informatiebeveiligings-gebeurtenissen**	**Oordeel**
	Beheersmaatregel:	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.16.1.2.6**	**Rapportage van informatiebeveiligings-gebeurtenissen**	**Oordeel**
	Beheersmaatregel:	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.16.1.2.7**	**Rapportage van informatiebeveiligings-gebeurtenissen**	**Oordeel**
	Beheersmaatregel:	Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	

	Interview met:	0	
	Toelichting auditor	0	
	A.16.1.3	**Rapportage van zwakke plekken in de informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.16.1.3.1**	**Rapportage van zwakke plekken in de informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	Een Coordinated Vulnerability Disclosure (CVD) procedure is gepubliceerd en ingericht.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.16.1.4	**Beoordeling van en besluitvorming over informatiebeveiligings-gebeurtenissen**	**Oordeel**
	Beheersmaatregel:	Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.16.1.4.1**	**Beoordeling van en besluitvorming over informatiebeveiligings-gebeurtenissen**	**Oordeel**
	Beheersmaatregel:	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.16.1.5	**Respons op informatiebeveiligings-incidenten**	**Oordeel**
	Beheersmaatregel:	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.16.1.6	**Lering uit informatiebeveiligings-incidenten**	**Oordeel**
	Beheersmaatregel:	Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	

	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.16.1.6.1**	**Lering uit informatiebeveiligings-incidenten**	**Oordeel**
	Beheersmaatregel:	Beveiligingsincidenten worden geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.16.1.6.2**	**Lering uit informatiebeveiligings-incidenten**	**Oordeel**
	Beheersmaatregel:	De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.16.1.7	**Verzamelen van bewijsmateriaal**	**Oordeel**
	Beheersmaatregel:	De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.16.1.7.1**	**Verzamelen van bewijsmateriaal**	**Oordeel**
	Beheersmaatregel:	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.17.1.1	**Informatiebeveiligingscontinuïteit plannen**	**Oordeel**
	Beheersmaatregel:	De organisatie moet haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	Niet-kritieke afwijking
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	Naast het BCP plan van OGD (voor herstel van de datacenter omgeving) is er nu een "crisismanagementstrategie en plan" opgezet voor de fysieke locatie. Er zit echter geen samenhang tussen alle verschillende stukken waardoor er ook geen eenduidig informatiebeveiligingscontinuïteit plan aanwezig is. Deze KVV is niet effectief opgepakt en levert nu een NKA.	
	Bewijslast:	16. SERVICE CONTINUÏTEITSPLAN PROVINCIE GELDERLAND v1.0 20220901 v1 Plan van aanpak crisismanagementstrategie en plan	
	Interview met:	5.1.2e	
	Toelichting auditor	Het verbetertraject voor het herzien van het BCP loopt nog en zal naar verwachting eind 2024 zijn afgerond. Deze KVV is nog niet effectief opgepakt en de NKA blijft nog staan.	
	A.17.1.2	**Informatiebeveiligings-continuïteit implementeren**	**Oordeel**
	Beheersmaatregel:	De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	

	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	Niet in audit scope
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.17.1.3	**Informatiebeveiligings-continuïteit verifiëren, beoordelen en evalueren**	**Oordeel**
	Beheersmaatregel:	De organisatie moet de ten behoeve van informatiebeveiligings-continuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	In het BCP zijn 3 tests opgenomen welke conform de overeenkomst tussen Prov. Gelderland en OGD uitgevoerd zouden moeten worden. Deze test zijn de afgelopen jaren niet aantoonbaar uitgevoerd en levert een NKA.	
	Bewijslast:	16. SERVICE CONTINUÏTEITSPLAN PROVINCIE GELDERLAND v1.0 DR test februari 2024	
	Interview met:	5.1.2e	
	Toelichting auditor	Door OGD is er een restore test uitgevoerd over een aantal server met als uitwijk van DC Amsterdam naar DC Zwolle. Deze test is met zijn bevindingen beschikbaar geteld aan prv. Gelderland. De voorgaande NKA is effectief opgelost.	
Control BBN2	**A.17.1.3.1**	**Informatiebeveiligings-continuïteit verifiëren, beoordelen en evalueren**	**Oordeel**
	Beheersmaatregel:	Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	In het BCP zijn 3 tests opgenomen welke conform de overeenkomst tussen Prov. Gelderland en OGD uitgevoerd zouden moeten worden. Deze test zijn de afgelopen jaren niet aantoonbaar uitgevoerd en levert een NKA.	
	Bewijslast:	16. SERVICE CONTINUÏTEITSPLAN PROVINCIE GELDERLAND v1.0 DR test februari 2024	
	Interview met:	5.1.2e	
	Toelichting auditor	Door OGD is er een restore test uitgevoerd over een aantal server met als uitwijk van DC Amsterdam naar DC Zwolle. Deze test is met zijn bevindingen beschikbaar geteld aan prv. Gelderland. De voorgaande NKA is effectief opgelost.	
Control BBN2	**A.17.1.3.2**	**Informatiebeveiligings-continuïteit verifiëren, beoordelen en evalueren**	**Oordeel**
	Beheersmaatregel:	Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN2	**A.17.1.3.3**	**Informatiebeveiligings-continuïteit verifiëren, beoordelen en evalueren**	**Oordeel**
	Beheersmaatregel:	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten uiterlijk binnen een week hersteld.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.17.2.1	**Beschikbaarheid van informatieverwerkende faciliteiten**	**Oordeel**
	Beheersmaatregel:	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Niet in audit scope
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	

Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	0	
Interview met:	0	
Toelichting auditor	0	
A.18.1.1	**Vaststellen van toepasselijke wetgeving en contractuele eisen**	**Oordeel**
Beheersmaatregel:	Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	AIV GLD 2018 voor leveringen en diensten Overzicht informatiewetgeving PB-B-01 Beheren Beleid informatiebeveiliging PB-BB-01 Beheren Richtlijnen	
Interview met:	5.1.2e	
Toelichting auditor	De organisatie heeft geen formele contracten van opdrachtgevers/klanten. Afnemers zijn overheden en burgers. Daarmee zijn geen formele contractuele eisen. De provincie heeft eigen inkoopvoorwaarden. Deze worden altijd afgedwongen. De jurist heeft een overzicht gemaakt van alle relevante wet en regelgeving. Middels het proces B-01 en BB-01 is geborgd dat Wet en Regelgeving altijd mee wordt genomen bij het bepalen van het IB-Beleid en alle richtlijnen. Relatie tussen wet en regelgeving en de richtlijn is explicit bij de richtlijnen meegenomen en opgenomen in het Overzicht informatiewetgeving.	
A.18.1.2	**Intellectuele eigendomsrechten**	**Oordeel**
Beheersmaatregel:	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele-eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	PG- Netwerk overzichtstekening v4.5 Beeldbank.Gelderland.nl	
Interview met:	5.1.2e	
Toelichting auditor	De organisatie voldoet aan de intellectuele eigendomsrechten. Alle software wordt gebruikt met de daarvoor benodigde licenties. Medewerkers hebben op de centrale omgeving geen mogelijkheid tot het installeren van illegale of niet gelicentieerde software. Voor beeldmateriaal heeft prov. Gelderland een eigen beeldbank gevuld met eigen beeldmateriaal.	
A.18.1.3	**Beschermen van registraties**	**Oordeel**
Beheersmaatregel:	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	Trustbound.com Jaarrapportage 20223 van de FG (maart 2024)	
Interview met:	5.1.2e	
Toelichting auditor	Trustbound wordt gebruikt als het PIMS systeem welke medio 2023 is ingevoerd. De traject loopt nog en de FG heeft hierover een rapportage opgemaakt en aangeboden aan de directie.	
Control BBN2 **A.18.1.3.1**	**Beschermen van registraties**	**Oordeel**
Beheersmaatregel:	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	Trustbound.com Jaarrapportage 20223 van de FG (maart 2024)	

	Interview met:	5.1.2e	
	Toelichting auditor	Trustbound wordt gebruikt als het PIMS systeem welke medio 2023 is ingevoerd. De traject loopt nog en de FG heeft hierover een rapportage opgemaakt en aangeboden aan de directie. Bewaartermijnen zijn hierin ook opgenomen.	
	A.18.1.4	**Privacy en bescherming van persoonsgegevens**	**Oordeel**
	Beheersmaatregel:	Privacy en bescherming van persoonsgegevens moeten, voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Kans voor verbetering
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	Als verbetertraject voor het verwerkingsregister wordt nu Trustbound gebruikt als het PIMS systeem welke medio 2023 is ingevoerd. De traject loopt nog en de FG heeft hierover een rapportage opgemaakt en aangeboden aan de directie. Het traject zal na verwachting eind 2024 worden afgerond. De voorgaande KVV loopt nog. Middels een koppeling tussen Topdesk en TrustBound waarmee geborgd wordt dat alle datalekken direct worden opgenomen in Trustbound. De huidige FG is aangemeld bij de AP in het FG register onder FG-001976 (per 26 juni 2023). De voorgaande KVV is opgelost. Website bezoekers hebben de mogelijkheid om via de cookiebanner op een vrijelijke, specifieke en ondubbelzinnig wijze toestemming te geven voor het gebruik van cookies of deze juist niet te accepteren. Uit de tool Digitalinsightsplatform.nl is op te maken dat er nu geen cookies meer worden geplaatst zonder toestemming. De KVV is effectief opgelost.	
	Bewijslast:	Privacy beleid 2023-2025 Prov. Gelderland Trutbound Portal FG Registratie www.gelderland.nl app.Digitalinsightsplatform.nl	
	Interview met:	5.1.2e	
	Toelichting auditor	Als verbetertraject voor het verwerkingsregister wordt nu Trustbound gebruikt als het PIMS systeem welke medio 2023 is ingevoerd. De traject loopt nog en de FG heeft hierover een rapportage opgemaakt en aangeboden aan de directie. Het traject zal na verwachting eind 2024 worden afgerond. De voorgaande KVV loopt nog. Middels een koppeling tussen Topdesk en TrustBound waarmee geborgd wordt dat alle datalekken direct worden opgenomen in Trustbound. De huidige FG is aangemeld bij de AP in het FG register onder FG-001976 (per 26 juni 2023). De voorgaande KVV is opgelost. Website bezoekers hebben de mogelijkheid om via de cookiebanner op een vrijelijke, specifieke en ondubbelzinnig wijze toestemming te geven voor het gebruik van cookies of deze juist niet te accepteren. Uit de tool Digitalinsightsplatform.nl is op te maken dat er nu geen cookies meer worden geplaatst zonder toestemming. De KVV is effectief opgelost.	
Control BBN1	**A.18.1.4.1**	**Privacy en bescherming van persoonsgegevens**	**Oordeel**
	Beheersmaatregel:	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Privacy beleid 2023-2025 Prov. Gelderland FG Registratie www.gelderland.nl	
	Interview met:	5.1.2e	
	Toelichting auditor	De organisatie heeft een onafhankelijke FG aangesteld. 5.1.2e Aangemeld bij de AP voor het FG register - FG-001976 (per 26 juni 2023) In de privacy verklaring is het e-mail adres van de FG opgenomen (FG@Gelderland.nl.)	
Control BBN2	**A.18.1.4.2**	**Privacy en bescherming van persoonsgegevens**	**Oordeel**

	Beheersmaatregel:	Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.18.1.5	**Voorschriften voor het gebruik van cryptografische beheersmaatregelen**	**Oordeel**
	Beheersmaatregel:	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
Control BBN1	**A.18.1.5.1**	**Voorschriften voor het gebruik van cryptografische beheersmaatregelen**	**Oordeel**
	Beheersmaatregel:	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de 'pas toe of leg uit'-lijst van het Forum.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.18.2.1	**Onafhankelijk beoordeling van informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SCC Verslag interne audit - 17-3-2023 Tussen resultaten interne audit GLD. SCC -Activiteiten jaarplan 2023 - interne NEN-ISO 27001 audits SCC -Activiteiten jaarplan 2024 - interne NEN-ISO 27001 audits	
	Interview met:	5.1.2e	
	Toelichting auditor	Er is een interne audit uitgevoerd over de volledige norm door een externe ingehuurde consultant. De punten uit de interne audit zijn als actie punten opgenomen in SCC. Voor het meer jaren plan zijn voor de 1e en 2e controle audits auditplannen opgenomen in het SCC .	
Control BBN2	**A.18.2.1.1**	**Onafhankelijk beoordeling van informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SCC Verslag interne audit - 17-3-2023 Tussen resultaten interne audit GLD. SCC -Activiteiten jaarplan 2023 - interne NEN-ISO 27001 audits SCC -Activiteiten jaarplan 2024 - interne NEN-ISO 27001 audits	

	Interview met:	5.1.2e	
	Toelichting auditor	De organisatie heeft een PDCA cyclus en beoordeeld op regelmatige wijze de werking van het ISMS. Managers/verantwoordelijke leggen in het ISMS (SCC) de bewijslast vast dat er wordt voldaan aan de eisen van de ISO7001 norm en de BIO.	
Control BBN2	**A.18.2.1.2**	**Onafhankelijk beoordeling van informatiebeveiliging**	**Oordeel**
	Beheersmaatregel:	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	SCC Verslag interne audit - 17-3-2023 Tussen resultaten interne audit GLD. SCC -Activiteiten jaarplan 2023 - interne NEN-ISO 27001 audits SCC -Activiteiten jaarplan 2024 - interne NEN-ISO 27001 audits	
	Interview met:	5.1.2e	
	Toelichting auditor	Er is een auditplan vastgesteld voor de komende jaren (3 jarige cyclus)	
	A.18.2.2	**Naleving van beveiligingsbeleid en -normen**	**Oordeel**
	Beheersmaatregel:	[A11>Leidinggevenden moeten regelmatig de naleving van de informatieverwerking en -procedures binnen hun[<A11] verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	In het SCC en middels de processen zou geborgd worden dat leidinggevende bewijslast aanleveren of er voldaan wordt aan de ISO27001 norm en BIO. Er is echter niet aantoonbaar dat die de afgelopen periode ook is uitgevoerd. Deze input zou dan ook worden meegenomen in directiebeoordeling. Dat dit niet aantoonbaar is uitgevoerd levert een NKA (zie ook H7.2 en H9.3 voor de bijbehorende KA's)	
	Bewijslast:	PB-B-04 Directiebeoordeling ISMS Verslag directiebeoordeling IB 23-3-2023	
	Interview met:	5.1.2e	
	Toelichting auditor	Het gehele SCC systeem is opnieuw ingericht en passend gemaakt bij de organisatie. Daarnaast is bepaald en uitgevoerd dat alle bewijslast opgeslagen wordt in SCC en dat SCC gebruikt wordt als "IB waarheid". De voorgaande NKA is hiermee effectief opgelost.	
Control BBN1	**A.18.2.2.1**	**Naleving van beveiligingsbeleid en -normen**	**Oordeel**
	Beheersmaatregel:	In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.	Niet in steekproef van deze audit
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	0	
	Interview met:	0	
	Toelichting auditor	0	
	A.18.2.3	**Beoordeling van technische naleving**	**Oordeel**
	Beheersmaatregel:	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Geen afwijkingen
	Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
	Relevante bevinding uit vorige audit(s):	0	
	Bewijslast:	Prv.Gelderland-interne-Pentest-Rapport v1.0 (19-12-2023)	
	Interview met:	5.1.2e	
	Toelichting auditor	Jaarlijks wordt er een Pentest uitgevoerd . Eind 2023 is er een pentest uitgevoerd door Secura op het interne netwerk om de desktop omgeving. In eerste instantie bleek uit de pentest dat de omgeving afdoende was beschermd. Aanvullende bevindingen (naar aanleiding van de opdracht uitbreiding) zijn wel enkele bevindingen gedaan welke samen met OGD worden opgepakt.	
Control BBN2	**A.18.2.3.1**	**Beoordeling van technische naleving**	**Oordeel**

Beheersmaatregel:	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.	Geen afwijkingen
Beschrijving uitgevoerde onderzoek:	Onderzocht: 1) hoe de organisatie deze beheersmaatregel heeft vertaald naar eigen eisen 2) of de eigen eisen aansluiten bij de vastgestelde risico's (6.1.3) 3) of de vastgestelde eigen eisen volledig aansluiten bij de norm eisen 4) of de eigen eisen onderdeel uitmaken van de interne audit (zie 9.2a1) 5) of er afwijkingen zijn ten opzichte van de eigen eisen	
Relevante bevinding uit vorige audit(s):	0	
Bewijslast:	Pry.Gelderland-interne-Pentest-Rapport v1.0 (19-12-2023)	
Interview met:	5.1.2e	
Toelichting auditor	Jaarlijks wordt er een Pentest uitgevoerd . Eind 2023 is er een pentest uitgevoerd door Secura op het interne netwerk om de desktop omgeving. In eerste instantie bleek uit de pentest dat de omgeving afdoende was beschermd. Aanvullende bevindingen (naar aanleiding van de opdracht uitbreiding) zijn wel enkele bevindingen gedaan welke samen met OGD worden opgepakt.	

Auditprogramma

	INIT	Controle 1	Controle 2	HER
Managementsysteem				
H4	x	-	x	x
H5	x	-	x	x
H6	x	x	-	x
H7	x	x	-	x
H8	x	x	-	x
H9	x	x	x	x
H10	x	x	x	x
Annex A controls				
A5	x	x	-	x
A6	x	x	-	x
A7	x	x	-	x
A8	x	x	-	x
A9	x	x	x	x
A10	x	-	x	x
A11	x	-	x	x
A12	x	-	x	x
A13	x	x	-	x
A14	x	-	x	x
A15	x	-	x	x
A16	x	-	x	x
A17	x	-	x	x
A18	x	x	x	x

EINDE DOCUMENT