ENSIA

Rapportage zelfevaluatie informatiebeveiliging 2024

Gemeente Doesburg

Colofon

ENSIA 2024

Dit rapport bevat de antwoorden van de Gemeente Doesburg op de onderwerpen uit de ENSIA-zelfevaluatie informatiebeveiliging BIO 2024.

Inhoudsopgave

Leeswijzer

In dit rapport zijn de vragen en ingevulde antwoorden opgenomen uit de ENSIA BIO-vragenlijst 2024. Het rapport is opgesteld in Word-formaat. U kunt de inhoud van de kolommen verder uitwerken om zo te komen tot een evaluatie en de bouwstenen voor een verbeterplan.

Houd bij het verspreiden van informatie telkens voor ogen welk detailniveau over informatiebeveiliging u vrijgeeft aan de doelgroep. Dit in verband met inzage in uw organisatiebeveiliging en de risico's die u daarbij loopt.

BIO-rapport

De rapportage bevat tabellen met daarin het nummer van de BIO-control en de omschrijving. Daaronder staan de maatregelen en daaronder in 3 kolommen uitgeschreven: Antwoord, Voldoet en Voldoet niet. Hieronder een voorbeeld. De kolommen worden hieronder toegelicht.

Control 6.2.1 Beleid voor mobiele apparatuur		
Maatregel 6.2.1.1 BBN 2 Mobiele apparatuur is zo ingericht dat geen bedrijfsinformatie 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.		
6.2.1.1a Is de mobiele apparatuur zo ingericht dat geen bedrijfsinformatie op het apparaaat wordt opgeslagen (zero footprint)?		
Antwoord	**Voldoet**	**Voldoet niet**
<gegeven antwoord>	✓ (bij antwoord ja)	✓ (bij antwoord nee)

Antwoord
Het door de gemeente ingevulde antwoord in de BIO-vragenlijst in de ENSIA-zelfevaluatie. Dit antwoord is het gemeentebrede interne antwoord op de hoofdvraag uit de vragenlijst. Er is immers maar één (gewogen) antwoord mogelijk dat vaak betrekking heeft op meerdere stelsels/systemen/situaties. Het algemene BIO-antwoord wijkt mogelijk af van het antwoord dat van toepassing is op het antwoord voor een specifiek normenkader. Zo kunt u gemeentebreed op basis van de BIO een antwoord "Nee" hebben gegeven, waar u bijvoorbeeld voor het gebruik van Suwinet wel voldoet en hier het antwoord "Ja" van toepassing is.

Voldoet / voldoet niet
De kolom "Voldoet" wordt vanuit de ENSIA-tool gevuld met een vink als het antwoord op de hoofdvraag een gekwalificeerde "Ja" of "Niet van toepassing" is. Als het antwoord "Nee" of een gekwalificeerde "Nee" is, wordt een vink geplaatst in de kolom "Voldoet niet".
Als er sprake is van subvragen die gericht zijn op verantwoording aan het Rijk, dan wordt voor iedere onderdeel (BRP, Reisdocumenten, Suwinet) per onderdeel aangegeven of aan de maatregel is voldaan of niet. De invulling vindt plaats op basis van datgene wat is ingevuld in de zelfevaluatie. Een interne beoordeling dat niet aan de maatregel is voldaan, zal waarschijnlijk leiden tot een verbeterplan.

Deel 1 - Achtergrond BIO

2. Opzet van de BIO		
2.1 Opzet van de BBN's De keuze voor een BBN wordt gemaakt door de proceseigenaar en is gebaseerd op risicomanagement.		
2.1.1. Worden BBN's toegekend door eigenaren van een proces?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

2.2 Controls In het geval een control voor een specifiek geval niet van toepassing kan zijn, is de control niet toepassing: de zogenaamde hardheidsbepaling.		
2.2.1. Is vastgelegd welke BIO-controls niet van toepassing zijn?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

2.4 Overheidsmaatregelen In het geval een maatregel voor een specifiek geval niet van toepassing kan zijn, vervalt de verplichting: de zogenaamde hardheidsbepaling.		
2.4.1. Is vastgelegd welke BIO-maatregelen niet van toepassing zijn?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

2.7 Rollen De BIO verplicht om de rollen die bij de controls en overheidsmaatregelen (die van toepassing zijn) staan intern toe te delen en hierbij rekening te houden met voldoende functiescheiding.		
2.7.1. Zijn alle BIO-controls en -maatregelen die van toepassing zijn toebedeeld aan een verantwoordelijke?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

4 . Verantwoording over de BIO		
De bestuurlijke verantwoording over de toepassing van de BIO is onderdeel van de verantwoording over de beveiliging van informatie(-systemen). Hier wordt ook verantwoording afgelegd aan de ketenpartners met wie afspraken over de beveiliging van informatie zijn gemaakt.		
4.0.1. Geeft de gemeente inzicht in de keten over de mate waarin zij voldoet aan de BIO?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

4.1 Verantwoordelijkheid afhankelijk van basisbeveiligingsniveau Voor BBN 3 geldt dat vooraf toestemming verleend moet worden door de secretaris/algemeen directeur voor het verwerken van bijzondere informatie (conform het VIR-BI).		
Indien processen en/of systemen geclassificeerd zijn boven BBN 2 voor vertrouwelijkheid, is dit dan afgestemd met de gemeentesecretaris?		
Antwoord	**Voldoet**	**Voldoet niet**
Niet van toepassing, er is geen sprake van een BBN3 classificatie	✓	

4.2 Explains op overheidsmaatregelen De organisatie dient te beschikken over een registratie van overheidsmaatregelen waaraan niet of nog niet geheel kan worden voldaan.		
4.2.1. Is vastgelegd welke verplichte overheidsmaatregelen niet zijn geïmplementeerd of waar niet geheel aan wordt voldaan?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Hoofdstuk 5 Informatiebeveiligingsbeleid

Control 5.1.1 Beleidsregels voor informatiebeveiliging		
Maatregel 5.1.1.1 BBN 1 Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.		
Is een informatiebeveiligingsbeleid vastgesteld dat voldoet aan de hieraan gestelde eisen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken Suwinet WGS	

Control 5.1.2 Beoordeling van het informatiebeveiligingsbeleid		
Maatregel 5.1.2.1 BBN 1 Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.		
Is het vastgestelde informatiebeveiligingsbeleid actueel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	

Hoofdstuk 6 Organiseren van informatiebeveiliging

Control 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging		
Maatregel 6.1.1.1 BBN 1 De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.		
6.1.1.1 Zijn de verantwoordelijkheden en rollen op het gebied van informatiebeveiliging vastgelegd door de leiding?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja, de bevoegdheden, verantwoordelijkheden en rollen	✓ BRP Reisdocumenten Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken Suwinet WGS	
Maatregel 6.1.1.2 BBN 1 De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.		
6.1.1.2 Zijn de vastgelegde verantwoordelijkheden en rollen gebaseerd op relevante voorschriften en wetten?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	
Maatregel 6.1.1.3 BBN 1 De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.		
6.1.1.3 Zijn de rol en verantwoordelijkheden van de CISO vastgelegd in een CISO-functieprofiel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ ✓ Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	
Maatregel 6.1.1.4 BBN 1 Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.		
6.1.1.4 Is er een CISO aangesteld conform het CISO-functieprofiel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja, er is een CISO aangesteld conform het CISO-functieprofiel	✓ Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	

Control 6.1.2 Scheiding van taken		
Maatregel 6.1.2.1 BBN 1 Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.		
6.1.2.1 Zijn er maatregelen getroffen om, door middel van scheiding van taken, onbedoelde of ongeautoriseerde wijziging of misbruik van bedrijfsmiddelen waar te nemen of te voorkomen, door scheiding van taken?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken Suwinet WGS	

Control 6.1.3 Contact met overheidsinstanties		
Maatregel 6.1.3.1 BBN 2 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.		
6.1.3.1 Bestaat een contactenlijst waarin staat welke functionarissen contact onderhouden met (overheids)instanties en toezichthouders over informatiebeveiligingsaangelegenheden?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Reisdocumenten	
Maatregel 6.1.3.2 BBN 2 Het contactoverzicht wordt jaarlijks geactualiseerd.		
6.1.3.2 Wordt het contactoverzicht jaarlijks geactualiseerd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 6.1.5 Informatiebeveiliging in projectbeheer

Control 6.2.1 Beleid voor mobiele apparatuur		
Maatregel 6.2.1.1 BBN 2 Mobiele apparatuur is zo ingericht dat geen bedrijfsinformatie 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.		
6.2.1.1.a Is de mobiele apparatuur zo ingericht dat geen bedrijfsinformatie op het apparaat wordt opgeslagen (zero footprint)?		
Antwoord	**Voldoet**	**Voldoet niet**
Dit is (nog) niet zo ingericht		✓
6.2.1.1.b Biedt een mobiel apparaat, bij het ontbreken van zero footprint, de mogelijkheid om toegang te beschermen door een toegangsbeveiligingsmechanisme en/of versleuteling van de gegevens?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja, met een toegangsbeveiligingsmechanisme en versleuteling (van vertrouwelijke gegevens op apparaat)	✓	

Control 6.2.1 Beleid voor mobiele apparatuur		
6.2.1.1.c Worden vertrouwelijke gegevens op mobiele apparatuur die binnen Burgerzaken wordt gebuikt versleuteld?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	
Maatregel 6.2.1.1 BBN 2 Mobiele apparatuur is zo ingericht dat geen bedrijfsinformatie 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.		
6.2.1.1.d Is het mogelijk om vertrouwelijke informatie op mobiele apparatuur 'op afstand' te wissen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	
Maatregel 6.2.1.2 BBN 2 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.		
6.2.1.2.a Komen gedragsaspecten van veilig mobiel werken aan de orde in bewustwordingsprogramma's?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
6.2.1.2.b Wordt patchmanagement en hardening toegepast op mobiele apparatuur?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja, er wordt patchmanagement en hardening toegepast	✓	
6.2.1.2.c Wordt mobiele apparatuur daar waar mogelijk beheerd en beveiligd via een MDM- of MAM-oplossing?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja, voor beheer en beveiliging	✓	
6.2.1.2.d Tekenen eindgebruikers een gebruikersovereenkomst voor mobiel werken, voorafgaand aan het verkrijgen van toegang tot bedrijfsgegevens?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 6.2.2 Telewerken		
Maatregel 6.2.2.1 BBN 2 Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.		
6.2.2.1 Is het telewerkbeleid geïmplementeerd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP	

Hoofdstuk 7 Veilig personeel

Control 7.1.1 Screening		
Maatregel 7.1.1.1 BBN1 Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan een Verklaring Omtrent Gedrag (VOG) gevraagd worden.		
7.1.1.1 Beschikt de organisatie over een vastgesteld screeningsbeleid?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓

Control 7.1.2 Arbeidsvoorwaarden		
Maatregel 7.1.2.1 BBN 1 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.		
7.1.2.1.a Worden medewerkers bij indiensttreding of bij functiewisseling gewezen op hun (gewijzigde) verantwoordelijkheden ten aanzien van informatiebeveiliging?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
7.1.2.1.b Zijn de geldende regelingen en instructies voor medewerkers ten aanzien van informatiebeveiliging eenvoudig toegankelijk?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 7.2.1 Directieverantwoordelijkheden		
Maatregel 7.2.1.1 BBN 1 Er is aansluiting bij een klokkenluidersregeling, zodat iedereen in staat is om anoniem en veilig beveiligingsissues te kunnen melden.		
7.2.1.1 Is iedereen in staat om anoniem en veilig beveiligingsissues te kunnen melden?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging		
Maatregel 7.2.2.1 BBN 1 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.		
7.2.2.1 Zijn medewerkers op de hoogte van de regels en verplichtingen met betrekking tot informatiebeveiliging en de verantwoordelijkheid die voor hun functie van toepassing is?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken Suwinet WGS	
Maatregel 7.2.2.2 BBN 1 Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.		

Control 7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging		
7.2.2.2 Volgen medewerkers binnen drie maanden na indiensttreding een training I-bewustzijn?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	
Maatregel 7.2.2.3 BBN 1 Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij haar medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.		
7.2.2.3 Wordt door het management het belang van deelname aan opleiding en training op het gebied van informatiebeveiliging benadrukt en gestimuleerd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 7.2.3 Disciplinaire procedures

Control 7.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband		
Aanvullende maatregel Het lijnmanagement heeft een procedure vastgesteld voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.		
7.3.1.am.2 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Hoofdstuk 8 Beheer van bedrijfsmiddelen

Control 8.1.1 Inventariseren van bedrijfsmiddelen

Control 8.1.2 Eigendom van bedrijfsmiddelen

Control 8.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Maatregel 8.1.3.1 BBN 1
Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.

8.1.3.1 Worden medewerkers gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen?

Antwoord	Voldoet	Voldoet niet
Ja	✓	

Maatregel 8.1.3.2 BBN 1
De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.

8.1.3.2 Zijn de gedragsregels voor het gebruik van bedrijfsmiddelen vastgelegd in contracten met extern personeel?

Antwoord	Voldoet	Voldoet niet
Ja	✓	

Control 8.1.4 Teruggeven van bedrijfsmiddelen

Control 8.2.1 Classificatie van informatie

Maatregel 8.2.1.1 BBN 1
De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.

8.2.1.1 Is informatie in informatiesystemen geclassificeerd zodat duidelijk is welke bescherming nodig is?

Antwoord	Voldoet	Voldoet niet
Ja	✓	

Control 8.2.2 Informatie labelen

Control 8.2.3 Behandelen van bedrijfsmiddelen

Control 8.3.1 Beheer van verwijderbare media

Maatregel 8.3.1.1 BBN 1
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. (ISO27002 – implementatierichtlijn 8.3.1.a).

8.3.1.1 Beschikt uw organisatie over een verwijderinstructie voor het verwijderen van gegevens op media die de organisatie verlaten?

Antwoord	Voldoet	Voldoet niet
Ja	✓ BRP Reisdocumenten	

Control 8.3.2 Verwijderen van media		
Maatregel 8.3.2.1 BBN 2 Media die vertrouwelijke informatie bevatten, zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden.		
8.3.2.1 Is media met vertrouwelijke informatie opgeslagen op een plek die niet toegankelijk is voor onbevoegden?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	
Maatregel 8.3.2.2 BBN 2 Verwijdering vindt plaats op een veilige manier, bijvoorbeeld door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie. (ISO 27002 - implementatierichtlijn 8.3.2.a)		
8.3.2.2 Worden media op een veilige manier verwijderd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 8.3.2.3 BBN 2 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.		
8.3.2.3 Wordt data op media onherstelbaar verwijderd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 8.3.3 Media fysiek overdragen		
Maatregel 8.3.3.1 BBN 2 Er is een vastgestelde procedure voor het fysiek transport van media		
8.3.3.1 Beschikt uw organisatie over een vastgestelde procedure voor het fysieke transport van media?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Reisdocumenten	
Maatregel 8.3.3.2 BBN 2 Het gebruik van koeriers of transporteurs van op BBN2 of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.		
8.3.3.2 Voldoen de door uw organisatie gebruikte koeriers of transporteurs aan de van tevoren opgestelde betrouwbaarheidseisen, wanneer zij BBN2 of hoger geclassificeerde informatie vervoeren?		
Antwoord	**Voldoet**	**Voldoet niet**
Niet van toepassing, wij maken geen gebruik van koeriers of transporteurs	✓ Reisdocumenten	

Hoofdstuk 9 Toegangsbeveiliging

Control 9.1.1 Beleid voor toegangsbeveiliging		
Maatregel 9.1.1.1 BBN 1 De organisatie beschikt over een uitgewerkt beleid voor de logische toegang tot informatie op basis van need-to-know en need-to-use. De control kent geen verplichte overheidsmaatregelen. Deze maatregel is richtinggevend.		
9.1.1.1 Is er vastgesteld beleid voor logische toegangsbeveiliging op basis van need-to-know en need-to-use?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	

Control 9.1.2 Toegang tot netwerken en netwerkdiensten		
Maatregel 9.1.2.1 BBN 1 Alleen geauthentiseerde apparatuur kan toegang krijgen tot een vertrouwde zone.		
9.1.2.1 Krijgt alleen geauthentiseerde apparatuur toegang tot een vertrouwde zone?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 9.1.2.2 BBN 1 Gebruikers met eigen of geauthentiseerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.		
9.1.2.2 Wordt voorkomen dat gebruikers met eigen of ongeauthenticeerde apparatuur toegang krijgen tot een vertrouwde zone?		
Ja	✓	

Control 9.2.1 Registratie en afmelden van gebruikers		
Maatregel 9.2.1.1 BBN 1 Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties		
9.2.1.1 Beschikt uw organisatie over een formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken Suwinet WGS	
Maatregel 9.2.1.2 BBN 1 Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.		
9.2.1.2 Is het gebruik van groepsaccounts gemotiveerd en vastgelegd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	

Control 9.2.2 Gebruikers toegang verlenen		
Maatregel 9.2.2.1 BBN 1 Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.		
9.2.2.1 Wordt toegang tot informatiesystemen alleen verleend na autorisatie door een bevoegd functionaris?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken Suwinet WGS	
Maatregel 9.2.2.2 BBN 1 Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.		
9.2.2.2 Worden toegangsrechten op basis van functiescheiding toegekend op grond van een risicoafweging?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken Suwinet WGS	
Maatregel 9.2.2.3 BBN 2 Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.		
9.2.2.3 Beschikt uw organisatie over een actueel mandaatregister of functieprofielen waaruit blijkt welke personen bevoegd functionaris zijn?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	

Control 9.2.3 Beheren van speciale toegangsrechten		
Maatregel 9.2.3.1 BBN 2 De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.		
9.2.3.1 Worden speciale bevoegdheden minimaal ieder kwartaal beoordeeld?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓

Control 9.2.4 Beheer van geheime authenticatie-informatie van gebruikers		
Aanvullende maatregel Ten aanzien van wachtwoorden geldt: Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker). Tijdelijke wachtwoorden of wachtwoorden die standaard in software of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord. Wachtwoorden zijn alleen bij de gebruiker bekend.		
9.2.4.am.2 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 9.2.5 Beoordeling van toegangsrechten van gebruikers		
Maatregel 9.2.5.1 BBN 1 Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.		
9.2.5.1 Worden boor BBN 1-systemen de toegangsrechten minimaal eenmaal per jaar beoordeeld?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 9.2.5.2 BBN 1 De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.		
9.2.5.2 Worden de bevindingen uit de beoordeling van toegangsrechten gedocumenteerd en behandeld als een beveiligingsincident?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 9.2.5.3 BBN 2 Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.		
9.2.5.3 Worden voor systemen met BBN 2 toegangsrechten minimaal eenmaal per halfjaar beoordeeld?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken Suwinet WGS	

Control 9.2.6 Toegangsrechten intrekken of aanpassen		
Maatregel 9.2.6.1 BBN 2 Het lijnmanagement heeft een procedure vastgesteld en geïmplementeerd voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie. De control kent geen verplichte overheidsmaatregelen. Deze maatregel is richtinggevend.		
9.2.6.1 Worden de toegangsrechten van gebruikers bij wijziging van functie aangepast?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	

Control 9.3.1 Geheime authenticatie-informatie gebruiken		
Maatregel 9.3.1.1 BBN 2 Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.		
9.3.1.1 Beschikt uw organisatie over een wachtwoordenkluis voor medewerkers ter ondersteuning van het beheren van hun wachtwoorden?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 9.4.1 Beperking toegang tot informatie		
Maatregel 9.4.1.1 BBN 2 Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.		
9.4.1.1 Zijn er maatregelen genomen om informatie met specifiek belang fysiek en/of logisch te isoleren?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja, fysiek en logisch	✓ Reisdocumenten	
Maatregel 9.4.1.2 BBN 2 Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.		
9.4.1.2 Is de toegang tot informatie met een specifiek belang beperkt tot medewerkers die deze informatie nodig hebben voor de uitoefening van hun taak?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 9.4.2 Beveiligde inlogprocedures		
Maatregel 9.4.2.1 BBN 1 Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.		
9.4.2.1 Worden inlogschermen die publiek of openbaar toegankelijk zijn minimaal afgeschermd met tenminste een 2FA-toegangscontrole mechanisme?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 9.4.2.2 BBN 2 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.		
9.4.2.2.a Krijgen leveranciers toegang tot het gemeentelijk netwerk op basis van een risicoafweging?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 9.4.2.2 BBN 2 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.		
9.4.2.2.b Wordt geregistreerd welke toegangsrechten een externe leverancier heeft gekregen?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓

Control 9.4.3 Systeem voor wachtwoordbeheer		
Maatregel 9.4.3.1 BBN 1 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.		
9.4.3.1.a Wordt afgedwongen dat, als two-factor authenticatie niet mogelijk is, dat wachtwoorden voldoen aan aanvullende complexiteitseisen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	
Maatregel 9.4.3.1 BBN 1 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.		
9.4.3.1.b Heeft u vastgelegd op welke wijze u omgaat met mislukte pogingen tot inloggen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 9.4.3.2 BBN 2 In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.).		
9.4.3.2 Worden wachtwoorden minimaal halfjaarlijks vernieuwd indien two-factor authenticatie niet mogelijk is?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 9.4.3.3 BBN 2 De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.		
9.4.3.3 Worden de eisen aan wachtwoorden geautomatiseerd afgedwongen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 9.4.3.4 BBN 2 Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.		
9.4.3.4.a Voldoen initiële wachtwoorden aan de gestelde eisen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
9.4.3.4.b Voldoen geresette wachtwoorden aan de gestelde eisen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 9.4.3.5 BBN 2 Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.		
9.4.3.5 Hebben wachtwoorden die voldoen aan het wachtwoordbeleid een maximale geldigheidsduur van een jaar en waar het beleid niet toepasbaar is een halfjaar?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 9.4.4 Speciale systeemhulpmiddelen gebruiken		
Maatregel 9.4.4.1 BBN 1 Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.		
9.4.4.1 Heeft alleen bevoegd personeel toegang tot systeemhulpmiddelen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 9.4.4.2 BBN 2 Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.		
9.4.4.2 Wordt het gebruik van systeemhulpmiddelen gelogd en is de logging gedurende een halfjaar beschikbaar gesteld voor onderzoek?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓

Control 9.4.5 Toegangsbeveiliging op programmacodebron

Hoofdstuk 10 Cryptografie

Control 10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen		
Maatregel 10.1.1.1 BBN 2 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 inter-organisatie communicatie wordt het beleid onderling vastgesteld.		
10.1.1.1 Beschikt uw organisatie over een cryptografiebeleid waarin de onder a t/m d genoemde onderwerpen zijn opgenomen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	
Maatregel 10.1.1.2 BBN 2 Cryptografische toepassingen voldoen aan passende standaarden.		
10.1.1.2 Voldoen cryptografische toepassingen aan passende standaarden?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	

Control 10.1.2 Sleutelbeheer		
Maatregel 10.1.2.1 BBN 2 Ingeval van PKIoverheid-certificaten: hanteer de PKIoverheid-eisen t.a.v. het sleutelbeheer. In overige situaties: hanteer de standaard ISO-11770 voor het beheer van cryptografische sleutels.		
10.1.2.1.a Hanteert uw organisatie de PKIoverheid-eisen t.a.v. sleutelbeheer?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 10.1.2.1 BBN 2 Ingeval van PKIoverheid-certificaten: hanteer de PKIoverheid-eisen t.a.v. het sleutelbeheer. In overige situaties: hanteer de standaard ISO-11770 voor het beheer van cryptografische sleutels.		
10.1.2.1.b Hanteert uw organisatie de ISO-11770 eisen t.a.v. sleutelbeheer ingeval u geen gebruik maakt van een PKIoverheids-certificaat?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 10.1.2.2 BBN 2 Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.		
10.1.2.2 Zijn op basis van een risicoafweging afspraken gemaakt over reservecertificaten met een tweede leverancier?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Hoofdstuk 11 Fysieke beveiliging en beveiliging van de omgeving

Control 11.1.1 Fysieke beveiligingszone		
Maatregel 11.1.1.1 BBN 1 Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.		
11.1.1.1 Wordt er voor het inrichten van beveiligde zones gebruik gemaakt van standaarden?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	

Control 11.1.2 Fysieke toegangsbeveiliging		
Maatregel 11.1.2.1 BBN 2 In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.		
11.1.2.1 Worden er bij concrete beveiligingsrisico's waarschuwingen, conform de onderlinge afspraken, verzonden aan de verantwoordelijke (facilitaire) dienst voor beveiliging?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	

Control 11.1.3 Kantoren, ruimten en faciliteiten beveiligen		
Maatregel 11.1.3.1 BBN 1 Sleutelbeheer is ingericht op basis van een sleutelplan.		
11.1.3.1 Is het fysieke sleutelbeheer in uw organisatie ingericht op basis van een sleutelplan?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	

Control 11.1.4 Beschermen tegen bedreigingen van buitenaf		
Maatregel 11.1.4.1 BBN 1 De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.		
11.1.4.1 Zijn op basis van een expliciete risicoafweging beveiligingsmaatregelen genomen tegen bedreigingen van buitenaf?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 11.1.4.2 BBN 1 Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.		
11.1.4.2 Is bij de huisvesting van IT-apparatuur rekening gehouden met de gevolgen van rampen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 11.1.5 Werken in beveiligde gebieden		
Maatregel 11.1.5.1 BBN 2 Medewerkers die zelf niet geautoriseerd zijn mogen alleen onder begeleiding van bevoegd personeel en als er een duidelijke noodzaak voor is, toegang krijgen tot fysiek beveiligde ruimten waarin ICT-voorzieningen zijn geplaatst of waarin met vertrouwelijke informatie wordt gewerkt.		
11.1.5.1 Zijn er procedures voor het werken in beveiligde gebieden?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	

Control 11.1.6 Laad- en loslocatie

Control 11.2.1 Plaatsing en bescherming van apparatuur

Control 11.2.2 Nutsvoorzieningen

Control 11.2.3 Beveiliging van bekabeling		
Aanvullende maatregel Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd conform de norm NEN 1010.		
11.2.3.am.2 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 11.2.4 Onderhoud van apparatuur		
Aanvullende maatregel Reparatie en onderhoud van apparatuur (hardware) vindt op locatie plaats door bevoegd personeel, tenzij er geen data op het apparaat aanwezig of toegankelijk is.		
11.2.4.am.2 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 11.2.5 Verwijdering van bedrijfsmiddelen		
Maatregel 11.2.5.1 BBN 1 Er zijn huisregels waarin aan de orde komt hoe moet worden omgegaan met apparatuur, informatie en software die van de locatie moeten worden meegenomen. De control kent geen verplichte overheidsmaatregelen. Deze maatregel is richtinggevend.		
11.2.5.1 Zijn er regels voor het meenemen van apparatuur buiten de gebruikelijke locatie?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	

Control 11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein		
Maatregel 11.2.6.1 BBN 1 Op basis van een expliciete risicoafweging worden passende maatregelen genomen om bedrijfsmiddelen die zich buiten het terrein bevinden te beschermen. De control kent geen verplichte overheidsmaatregelen. Deze maatregel is richtinggevend.		
11.2.6.1 Worden bedrijfsmiddelen buiten het terrein voldoende beschermd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	

Control 11.2.7 Veilig verwijderen of hergebruiken van apparatuur		
Aanvullende maatregel Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de beheersorganisatie ingeleverd. De beheerorganisatie zorgt voor een verantwoorde afvoer zodat er geen data op het apparaat aanwezig of toegankelijk is. Als dit niet kan wordt het apparaat of de informatiedrager fysiek vernietigd. Het afvoeren of vernietigen wordt per bedrijfseenheid geregistreerd.		
11.2.7.am.2 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 11.2.8 Onbeheerde gebruikersapparatuur		
Aanvullende maatregel De gebruiker vergrendelt de werkplek tijdens afwezigheid.		
11.2.8.am.2 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 11.2.9 'Clear desk'- en 'clear screen'-beleid		
Maatregel 11.2.9.1 BBN 2 Een onbemensde werkplek is altijd vergrendeld.		
11.2.9.1 Is een onbemensde werkplek altijd vergrendeld?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	
Maatregel 11.2.9.2 BBN 2 Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.		
11.2.9.2 Wordt de werkplek vergrendeld na inactiviteit van maximaal 15 minuten?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	
Maatregel 11.2.9.3 BBN 2 Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.		
11.2.9.3 Worden sessies op remote werkplekken na een vastgestelde periode vergrendeld?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP	

Control 11.2.9 'Clear desk'- en 'clear screen'-beleid		
Maatregel 11.2.9.4 BBN 2 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.		
11.2.9.4 Is, alleen na het maken van een expliciete risicoafweging, het overnemen van een sessie vanaf remote werkplekken op een ander werkplek alleen mogelijk via dezelfde beveiligde loginprocedure als die waarmee de sessie is gecreëerd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 11.2.9.5 BBN 2 Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van de token de toegangsbeveiligingslock automatisch geactiveerd.		
11.2.9.5 Wordt met het verwijderen van een chipcardtoken de toegang tot systemen automatisch vergrendeld?		
Antwoord	**Voldoet**	**Voldoet niet**
Niet van toepassing, wij maken geen gebruik van chipcardtoken	✓	

Hoofdstuk 12 Beveiliging bedrijfsvoering

Control 12.1.1 Gedocumenteerde bedieningsprocedures		
Maatregel 12.1.1.1 BBN 1 Er zijn bedieningsprocedures voor alle gebruikers. De control kent geen verplichte overheidsmaatregelen. Deze maatregel is richtinggevend.		
12.1.1.1 Wordt er alleen gewerkt met gedocumenteerde bedieningsprocedures of handleidingen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken Suwinet WGS	

Control 12.1.2 Wijzigingsbeheer		
Maatregel 12.1.2.1 BBN 1 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.		
12.1.2.1 Beschikt uw organisatie over een procedure voor wijzigingenbeheer die voldoet aan de gestelde eisen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 12.1.3 Capaciteitsbeheer		
Aanvullende maatregel De dienstenleverancier heeft voorzieningen geïmplementeerd die de aanwezigheid en beschikbare capaciteit van componenten bewaakt. Er worden beperkingen aan gebruikers opgelegd zodat ze niet meer middelen kunnen opeisen dan nodig is voor de uitvoering van zijn of haar taken zodat de beschikbaarheid van deze middelen voor andere gebruikers gewaarborgd blijft.		
12.1.3.am.2 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 12.1.4 Scheiding van ontwikkel-,test- en productieomgevingen		
Maatregel 12.1.4.1 BBN 2 In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.		
12.1.4.1 Wordt er getest in een andere omgeving dan de productieomgeving?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja, er wordt niet in de productieomgeving getest	✓	
Maatregel 12.1.4.2 BBN 2 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.		
12.1.4.2 Worden wijzigingen in de productieomgeving getest voordat ze in productie worden genomen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 12.2.1 Beheersmaatregelen tegen malware		
Maatregel 12.2.1.1 BBN 1 Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.		
12.2.1.1 Wordt het downloaden van bestanden beheerst en beperkt op basis van risico?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 12.2.1.2 BBN 1 Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.		
12.2.1.2 Worden gebruikers voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 12.2.1.3 BBN 1 De gebruikte antimalware software en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.		
12.2.1.3 Is de gebruikte antimalware software en herstelsoftware actueel en wordt deze periodiek geüpdatet?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 12.2.1.4 BBN 1 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.		
12.2.1.4 Worden computers en media routinematig gescand conform de gestelde eisen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 12.2.1.5 BBN 1 De malware scan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.		
12.2.1.5 Wordt de malware scan op verschillende omgevingen uitgevoerd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 12.3.1 Back-up van informatie		
Maatregel 12.3.1.1 BBN 1 Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld.		
12.3.1.1 Is er een vastgesteld back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	
Maatregel 12.3.1.2 BBN 1 Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.		
12.3.1.2 Is op basis van een expliciete risicoafweging bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 12.3.1 Back-up van informatie		
Maatregel 12.3.1.3 BBN 2 In het back-up beleid 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.		
12.3.1.3 Voldoet het restore beleid aan de minimaal gestelde eisen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 12.3.1.4 BBN 2 Het back-up proces 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.		
12.3.1.4 Voldoet het back-up proces aan de gestelde eisen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 12.3.1.5 BBN 2 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.		
12.3.1.5 Wordt de restore-procedure minimaal jaarlijks getest en eerder na een grote wijziging?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 12.4.1 Gebeurtenissen registreren		
Maatregel 12.4.1.1 BBN 1 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.		
12.4.1.1 Is logging zo ingericht dat de logregels voldoen aan het logbeleid?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee	Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	✓
Maatregel 12.4.1.2 BBN 1 Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.		
12.4.1.2 Voldoen logregels aan de eis van het niet bevatten van gegevens die tot het doorbreken van de beveiliging kunnen leiden?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	
Maatregel 12.4.1.3 BBN 2 De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze wordt ingezet		

Control 12.4.1 Gebeurtenissen registreren		
op basis van een risico-inschatting, mede aan de hand van en de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.		
12.4.1.3 Maakt uw organisatie gebruik van voorzieningen voor het detecteren van aanvallen, waarbij dit gebruik gebaseerd is op een risico-inschatting?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	
Maatregel 12.4.1.4 BBN 2 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.		
12.4.1.4 Worden ontdekte dreigingen gedeeld met de IBD via het passende kanaal?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 12.4.1.5 BBN 2 De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.		
12.4.1.5 Indien u gebruik maakt van SIEM en/of SOC, heeft de SIEM en/of SOC dan regels voor het rapporteren van incidenten aan het verantwoordelijk management?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 12.4.2 Beschermen van informatie in logbestanden		
Maatregel 12.4.2.1 BBN 1 Er is een overzicht van logbestanden die worden gegenereerd.		
12.4.2.1 Beschikt uw organisatie over een overzicht van logbestanden die worden gegenereerd?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee	Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	✓
Maatregel 12.4.2.2 BBN 1 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.		
12.4.2.2 Is de bewaarperiode van logbestanden bepaald op basis van een expliciete risicoafweging?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee	Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	✓
Maatregel 12.4.2.3 BBN 2 Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.		

Control 12.4.2 Beschermen van informatie in logbestanden		
12.4.2.3 Worden logbestanden minimaal half jaarlijks gecontroleerd door een onafhankelijk functionaris?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓ Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken
Maatregel 12.4.2.4 BBN 2 Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.		
12.4.2.4 Worden wijzigingen of pogingen om logfiles te wijzigen zo snel mogelijk gemeld via de vastgestelde procedure?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓

Control 12.4.3 Logbestanden van beheerders en operators

Control 12.4.4 Kloksynchronisatie		
Aanvullende maatregel Systeemklokken worden gesynchroniseerd op basis van het NTP-protocol.		
12.4.4.am.2 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 12.5.1 De integriteit van operationele systemen waarborgen		
Maatregel 12.5.1.1 BBN 1 Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.		
12.5.1.1 Zijn er procedures voor het installeren van software op operationele systemen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Reisdocumenten	

Control 12.6.1 Beheer van technische kwetsbaarheden		
Maatregel 12.6.1.1 BBN 1 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.		
12.6.1.1.a Worden bij een hoge kans op misbruik en een hoge kans op schade patches uiterlijk binnen een week geïnstalleerd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 12.6.1.1 BBN 1 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.		
12.6.1.1.b Worden in afwachting van het installeren van patches op basis van een expliciete risicoafweging risicobeperkende genomen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 12.6.2 Beperkingen voor het installeren van software		
Maatregel 12.6.2.1 BBN 2 Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).		
12.6.2.1 Kunnen gebruikers alleen toegestane software installeren?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 12.7.1 Beheersmaatregelen betreffende audits van informatiesystemen		
Aanvullende maatregel De proceseigenaar is betrokken bij en geeft zijn toestemming voordat een audit uitgevoerd wordt. Audits mogen bedrijfsprocessen niet verstoren.		
12.7.1.am.2 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓
Aanvullende maatregel De proceseigenaar is betrokken bij en geeft zijn toestemming voordat een audit uitgevoerd wordt. Audits mogen bedrijfsprocessen niet verstoren.		
12.7.1.am.4 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**

Hoofdstuk 13 Communicatiebeveiliging

Control 13.1.1 Beheersmaatregelen voor netwerken		
Aanvullende maatregel Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau komt.		
13.1.1.am.2 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 13.1.2 Beveiliging van netwerkdiensten		
Maatregel 13.1.2.1 BBN 2 Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectie-oplossingen), 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.		
13.1.2.1 Wordt het in- en uitgaande dataverkeer bewaakt / geanalyseerd op kwaadaardige elementen middels detectie-voorzieningen zoals de toelichting uit de maatregel voorschrijft?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 13.1.2.2 BBN 2 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).		
13.1.2.2 Worden bij dreigingen meldingen gedaan bij de passende CERT?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 13.1.2.3 BBN 2 Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptie middelen waarvoor het NBV een positief inzetadvies heeft afgegeven.		
13.1.2.3 Wordt gebruik gemaakt van encryptie bij verbindingen door onvertrouwde zones?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 13.1.2.4 BBN 1 In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijv. DDoS attacks, Distributed Denial of Service attacks) te signaleren en hierop te reageren.		
13.1.2.4 Zijn er maatregelen getroffen in koppelpunten om aanvallen die de beschikbaarheid negatief beïnvloeden te signaleren en hierop te reageren?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 13.1.3 Scheiding in netwerken		
Maatregel 13.1.3.1 BBN 2 Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.		
13.1.3.1 Wordt segmentatie toegepast in netwerken om verschillende groepen van elkaar te scheiden?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 13.2.1 Beleid en procedures voor informatietransport

Control 13.2.2 Overeenkomsten voor informatietransport

Control 13.2.3 Elektronische berichten

Maatregel 13.2.3.1 BBN 1
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.

13.2.3.1 Wordt voor de beveiliging van elektronische (e-mail)berichten en websiteverkeer gebruik gemaakt van de vastgestelde open standaarden op de 'PTOLU'-lijst van het Forum?

Antwoord	Voldoet	Voldoet niet
Ja	✓	

Maatregel 13.2.3.2 BBN 2
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.

13.2.3.2 Wordt voor veilige berichtenuitwisseling met basisregistraties gebruik gemaakt van de actuele versie van Digikoppeling?

Antwoord	Voldoet	Voldoet niet
Ja	✓	

Maatregel 13.2.3.3 BBN 2
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.

13.2.3.3 Wordt er gebruik gemaakt van ten minste publiek vertrouwde Domain Validated-certificaten bij web- en mailverkeer van gevoelige gegevens?

Antwoord	Voldoet	Voldoet niet
Ja	✓	

Maatregel 13.2.3.4 BBN 2
Om zekerheid te bieden over de integriteit van het elektronische bericht wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.

13.2.3.4 Wordt bij elektronische handtekeningen gebruik gemaakt van de standaard?

Antwoord	Voldoet	Voldoet niet
Ja	✓	

Control 13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst

Maatregel 13.2.4.1 BBN 1
De algemene geheimhoudingsplicht voor ambtenaren is geregeld in de Ambtenarenwet art. 125a, lid 3.
Personen die te maken hebben met Bijzondere Informatie en die niet onder de Ambtenarenwet vallen dienen een geheimhoudingsverklaring te ondertekenen, daaronder valt ook vertrouwelijke informatie. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding. De control kent geen verplichte overheidsmaatregelen. Deze maatregel is richtinggevend.

13.2.4.1 Wordt er gebruik gemaakt van geheimhoudingsovereenkomsten conform de Ambtenarenwet?

Antwoord	Voldoet	Voldoet niet
Ja	✓ BRP Reisdocumenten	

Hoofdstuk 14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Control 14.1.1 Analyse en specificatie van informatiebeveiligingseisen		
Maatregel 14.1.1.1 BBN 1 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.		
14.1.1.1 Vindt een expliciete risicoafweging plaats bij nieuwe informatiesystemen en wijzigingen op bestaande informatiesystemen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 14.1.2 Toepassingen op openbare netwerken beveiligen

Control 14.1.3 Transacties van toepassingen beschermen		
Aanvullende maatregel Een transactie is versleuteld, de partijen zijn geauthentiseerd en de privacy van betrokken partijen is gewaarborgd.		
14.1.3.am.2 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 14.2.1 Beleid voor beveiligd ontwikkelen		
Maatregel 14.2.1.1 BBN 1 De gangbare principes rondom 'security by design' zijn uitgangspunt voor de ontwikkeling van software en systemen.		
14.2.1.1 Zijn bij de ontwikkeling van software en systemen de gangbare principes van 'security bij design' het uitgangspunt?		
Antwoord	**Voldoet**	**Voldoet niet**
Niet van toepassing, wij ontwikkelen geen software	✓	

Control 14.2.2 Procedure voor wijzigingsbeheer met betrekking tot systemen		
Maatregel 14.2.2.1 BBN 1 Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerde beheerframework.		
14.2.2.1 Vindt wijzigingsbeheer plaats op basis van een algemeen geaccepteerd beheerframework?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 14.2.3 Technische beoordeling van toepassingen na wijzigingen besturingsplatform

Control 14.2.5 Principes voor engineering van beveiligde systemen

Control 14.2.6 Beveiligde ontwikkelomgeving		
Maatregel 14.2.6.1 BBN 1 Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging.		
14.2.6.1 Worden ontwikkelomgevingen voor systemen passend beveiligd op basis van een expliciete risicoafweging?		
Antwoord	**Voldoet**	**Voldoet niet**
Niet van toepassing, wij beschikken niet over systeemontwikkelomgevingen	✓	

Control 14.2.7 Uitbestede softwareontwikkeling		
Maatregel 14.2.7.1 BBN 1 Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.		
14.2.7.1 Worden passende en noodzakelijke beveiligingsmaatregelen aan de leverancier opgelegd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 14.2.8 Testen van systeembeveiliging		
Aanvullende maatregel Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd. Van de resultaten van de testen wordt verslag gemaakt. (BBN 1		
14.2.8.am.2 Voldoet uw organisatie aan deze aanvullende maatregel?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓

Control 14.2.9 Systeemacceptatietests		
Maatregel 14.2.9.1 BBN 1 Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.		
14.2.9.1 Vinden acceptatietesten van systemen op basis van gestructureerde testmethodieken plaats?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 14.2.9.2 BBN 1 Van de resultaten van de testen wordt verslag gemaakt.		
14.2.9.2 Worden testverslagen gemaakt waarin de resultaten van het testen worden vastgelegd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 14.3.1 Bescherming van testgegevens

Hoofdstuk 15 Leveranciersrelaties

Control 15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties		
Maatregel 15.1.1.1 BBN 1 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.		
15.1.1.1 Worden eisen t.a.v. informatie(voorziening) benoemd in offerteaanvragen, waarbij deze eisen zijn gebaseerd op een expliciete risicoafweging?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 15.1.1.2 BBN 2 Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekking tot leverancierstoegang tot bedrijfsinformatie vastgesteld.		
15.1.1.2 Worden de beheersmaatregelen m.b.t. leverancierstoegang tot bedrijfsinformatie vastgesteld op basis van een expliciete risicoafweging?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee, niet op basis van een expliciete risicoafweging		✓
Maatregel 15.1.1.3 BBN 2 Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.		
15.1.1.3 Worden met alle leveranciers, indien van toepassing, verwerkersovereenkomsten gesloten waarin alle wettelijke vereiste afspraken zijn vastgelegd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	

Control 15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten		
Maatregel 15.1.2.1 BBN 1 De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.		
15.1.2.1 Worden de beveiligingseisen uit offerteaanvragen expliciet opgenomen in (inkoop) contracten waarbij informatie een rol speelt?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 15.1.2.2 BBN 1 In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.		
15.1.2.2 Worden in inkoopcontracten expliciet prestatie-indicatoren en bijbehorende verantwoordingsrapportages opgenomen?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓
Maatregel 15.1.2.3 BBN 1 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.		

Control 15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten		
15.1.2.3 Worden consequenties van door leveranciers opgelegde contractvoorwaarden, voorafgaand aan het tekenen van een contract, door middel van een risico analyse, inzichtelijk gemaakt?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 15.1.2.4 BBN 1 Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaardvoorwaarden voor inkoop gehanteerd.		
15.1.2.4 Worden bij IT-aankopen standaard inkoopvoorwaarden gehanteerd ter waarborging van vertrouwelijkheid of geheimhouding?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 15.1.2.5 BBN 2 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.		
15.1.2.5.a Wordt voor het afsluiten van een contract op basis van risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 15.1.2.5 BBN 2 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.		
15.1.2.5.b Maakt een expliciete exit-strategie een vast onderdeel uit van contracten?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 15.1.2.6 BBN 2 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.		
15.1.2.6 Bevatten inkoopcontracten het 'right to audit'?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓

Control 15.1.3 Toeleveringsketen van informatie- en communicatietechnologie		
Maatregel 15.1.3.1 BBN 2 Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.		
15.1.3.1.a Maken de leveranciers van uw organisatie hun keten van toeleveranciers bekend?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
15.1.3.1.b Zijn de leveranciers van uw keten transparant over de maatregelen die zij genomen hebben om de opgelegde eisen door te vertalen naar hun toeleveranciers?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers		
Maatregel 15.2.1.1 BBN 2 Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.		
15.2.1.1 Worden de prestaties van leveranciers op het gebied van informatiebeveiliging jaarlijks beoordeeld op vooraf vastgestelde prestatie-indicatoren?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓ BRP Reisdocumenten

Control 15.2.2 Beheer van veranderingen in dienstverlening van leveranciers

Hoofdstuk 16 Beheer van informatiebeveiligingsincidenten

Control 16.1.1 Verantwoordelijkheden en procedures

Control 16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen		
Maatregel 16.1.2.1 BBN 1 Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.		
16.1.2.1 Beschikt uw organisatie over een meldloket waar beveiligingsincidenten kunnen worden gemeld?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 16.1.2.2 BBN 1 Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.		
16.1.2.2 Beschikt uw organisatie over een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 16.1.2.3 BBN 1 Alle medewerkers en contractanten hebben aantoonbaar kennisgenomen van de meldingsprocedure van incidenten.		
16.1.2.3 Zijn interne en externe medewerkers op de hoogte van de meldingsprocedure van incidenten?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Reisdocumenten	
Maatregel 16.1.2.4 BBN 1 Incidenten worden zo snel als mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.		
16.1.2.4 Worden incidenten uiterlijk binnen 24 uur intern gemeld?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 16.1.2.5 BBN 1 De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.		
16.1.2.5 Is de proceseigenaar gewezen op zijn verantwoordelijkheid voor het oplossen van beveiligingsincidenten?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 16.1.2.6 BBN 1 De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.		
16.1.2.6 Wordt de opvolging maandelijks gerapporteerd aan de verantwoordelijke?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 16.1.2.7 BBN 1 Informatie afkomstig uit de Coordinated Vulnerability Disclosure-procedure (CVD) is onderdeel van de incidentrapportage.		
16.1.2.7 Maakt informatie uit de Coordinated Vulnerability Disclosure (CVD) onderdeel uit van de incidentrapportage?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging		
Maatregel 16.1.3.1 BBN 1 Een Coordinated Vulnerability Disclosure (CVD) procedure is gepubliceerd en ingericht.		
16.1.3.1 Beschikt uw organisatie over een gepubliceerde en ingerichte Coordinated Vulnerability Disclosure (CVD) procedure?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen		
Maatregel 16.1.4.1 BBN 2 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.		
16.1.4.1 Worden beveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beveiliging (BIV) van informatieverwerkende systemen, uiterlijk binnen 72 uur gemeld aan de sectorale CERT?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 16.1.5 Respons uit informatiebeveiligingsincidenten

Control 16.1.6 Lering uit informatiebeveiligingsincidenten		
Maatregel 16.1.6.1 BBN 2 Beveiligingsincidenten worden geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.		
16.1.6.1 Wordt de informatie verkregen uit het beoordelen van beveiligingsmeldingen, geëvalueerd met als doel beheersmaatregelen te verbeteren?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	
Maatregel 16.1.6.2 BBN 2 De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.		
16.1.6.2 Worden de resultaten van de beoordeling van de beveiligingsincidenten, gedeeld met partners om herhaling en toekomstige incidenten te voorkomen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 16.1.7 Verzamelen van bewijsmateriaal		
Maatregel 16.1.7.1 BBN 2 In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.		
16.1.7.1 Wordt in geval van een vermoed informatiebeveiligingsincident de gelogde incidentinformatie minimaal drie jaar bewaard?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓

Hoofdstuk 17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Control 17.1.1 Informatiebeveiligingscontinuïteit plannen		
Maatregel 17.1.1.1 BBN 1 Er is een Business Impact Analyse (BIA) waarin de gebeurtenissen worden geïdentificeerd die kunnen leiden tot discontinuïteit in het bedrijfsproces. De control kent geen verplichte overheidsmaatregelen. Deze maatregel is richtinggevend.		
17.1.1.1 Is er een calamiteitenplan om de continuïteit van de bedrijfsvoering te waarborgen?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee	BRP Reisdocumenten	✓

Control 17.1.2 Informatiebeveiligingscontinuïteit implementeren

Control 17.1.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren		
Maatregel 17.1.3.1 BBN 2 Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.		
17.1.3.1 Worden continuiteïtsplannen jaarlijks getest op geldigheid en bruikbaarheid?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓ BRP Reisdocumenten
Maatregel 17.1.3.2 BBN 2 Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.		
17.1.3.2 Zijn de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd op basis van een expliciete risicoafweging?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee		✓
Maatregel 17.1.3.3 BBN 2 De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten uiterlijk binnen een week hersteld.		
17.1.3.3 Wordt de dienstverlening van bedrijfskritische onderdelen bij calamiteiten uiterlijk binnen een week hersteld?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten

Hoofdstuk 18 Naleving

Control 18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen		
Maatregel 18.1.1.1 BBN 1 Er is vastgesteld welke wetten en wettelijke maatregelen van toepassing zijn op de organisatie of organisatieonderdelen. De control kent geen verplichte overheidsmaatregelen. Deze maatregel is richtinggevend.		
18.1.1.1 Heeft u de eisen uit relevante wetgeving vertaald naar maatregelen?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	

Control 18.1.2 Intellectuele-eigendomsrechten

Control 18.1.3 Beschermen van registraties		
Maatregel 18.1.3.1 BBN 2 De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.		
18.1.3.1 Is per soort informatie uitgewerkt wat de bewaartermijn is?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 18.1.4 Privacy en bescherming van persoonsgegevens		
Maatregel 18.1.4.1 BBN 1 In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.		
18.1.4.1 Is een Functionaris Gegevensbescherming aangesteld met voldoende mandaat?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	
Maatregel 18.1.4.2 BBN 2 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.		
18.1.4.2.a Wordt de naleving van het privacy beleid regelmatig gecontroleerd?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	
Maatregel 18.1.4.2 BBN 2 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.		
18.1.4.2.b Wordt de logging van de verwerking van persoonsgegevens regelmatig gecontroleerd op rechtmatig gebruik?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten Suwinet P-wet (IOAZ/IOAW) Suwinet Burgerzaken	

Control 18.1.5 Beschermen van registraties		
Maatregel 18.1.5.1 BBN 1 Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de ‘pas toe of leg uit’-lijst van het Forum.		
18.1.5.1 Sluiten de cryptografische beheersmaatregelen expliciet aan bij de standaarden op de 'PTOLU'-lijst van het Forum?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓	

Control 18.2.1 Onafhankelijke beoordeling van informatiebeveiliging		
Maatregel 18.2.1.1 BBN 2 Er is een information security information system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.		
18.2.1.1 Beschikt uw organisatie over een ISMS waarmee aantoonbaar de gehele PDCA-cyclus wordt afgedekt?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	
Maatregel 18.2.1.2 BBN 2 Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.		
18.2.1.2 Is er een vastgesteld auditplan?		
Antwoord	**Voldoet**	**Voldoet niet**
Nee	 BRP Reisdocumenten	✓

Control 18.2.2 Naleving van beveiligingsbeleid en -normen		
Maatregel 18.2.2.1 BBN 1 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.		
18.2.2.1 Is er een werkend systeem van controle en rapportages over informatiebeveiliging aan het bestuur?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	

Control 18.2.3 Beoordeling van technische naleving		
Maatregel 18.2.3.1 BBN 2 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.		
18.2.3.1 Worden informatiesystemen jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van veiligheid?		
Antwoord	**Voldoet**	**Voldoet niet**
Ja	✓ BRP Reisdocumenten	