

ENSIA
Rapportage zelfevaluatie informatiebeveiliging 2020
gemeente Almere

Deel 1 achtergrond BIO

Deel 1 achtergrond BIO

2. Opzet van de BIO

Algemene eisen en verplichtingen uit de BIO

2.1 Opzet van de BBN's
De keuze voor een BBN wordt gemaakt door de proceseigenaar en is gebaseerd op risicomanagement.

Vraag

Worden BBN's toegekend door eigenaren van een proces?

Antwoord

✓Ja
- Nee

Voldoet

Voldoet niet

Deel 1 achtergrond BIO

2.2 Controls

Algemene eisen en verplichtingen uit de BIO

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.

Vraag

Is vastgelegd welke controls niet van toepassing zijn?

Antwoord

- Ja
✓Nee

Voldoet

Voldoet niet

Deel 1 achtergrond BIO

2.4 Overheidsmaatregelen

Algemene eisen en verplichtingen uit de BIO

2.4 Overheidsmaatregelen
In het geval een maatregel voor een specifiek geval niet van toepassing kan zijn, vervalt de verplichting: de zogenaamde hardheidsbepaling.

Vraag

Is vastgelegd welke maatregelen niet van toepassing zijn?

Antwoord

- Ja
10(1)b, 10(2)g

Voldoet

Voldoet niet

Deel 1 achtergrond BIO

2.7 Rollen

Algemene eisen en verplichtingen uit de BIO

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.

Vraag

Zijn alle controls en maatregelen die van toepassing zijn toebedeeld aan een verantwoordelijke?

Antwoord

✓Ja
- Nee

Voldoet

Voldoet niet

Deel 1 achtergrond BIO

Inleiding hoofdstuk 4

Algemene eisen en verplichtingen uit de BIO	Vraag	Antwoord	Voldoet	Voldoet niet
Inleiding hoofdstuk 4 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.	Geeft de gemeente inzicht in de keten over de mate waarin zij voldoet aan de BIO?	- Ja ✓Nee		

Deel 1 achtergrond BIO

4.1 Verantwoordelijkheid

Algemene eisen en verplichtingen uit de BIO	Vraag	Antwoord	Voldoet	Voldoet niet
4.1 Verantwoordelijkheid afhankelijk van basisbeveiligingsniveau Voor BBN3 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 op BBN3, is dit dan afgestemd met de gemeentesecretaris?	- Ja - Nee ✓Niet van toepassing, er is geen sprake van een BBN3 classificatie		

Deel 1 achtergrond BIO

4.2 Explains

Algemene eisen en verplichtingen uit de BIO	Vraag	Antwoord	Voldoet	Voldoet niet
4.2 Explains op overheidsmaatregelen De organisatie dient te beschikken over een registratie van overheidsmaatregelen waaraan niet of nog niet geheel kan worden voldaan.	Zijn alle nog niet geïmplementeerde overheidsmaatregelen waar nog niet of niet geheel aan voldaan wordt vastgelegd?	- Ja ✓Nee		

Hoofdstuk 5

Control 5.1.1				
Beleidsregels voor informatiebeveiliging				
Maatregel 5.1.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
<p>Maatregel 5.1.1.1 BBN 1</p> <p>Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten:</p> <p>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;</p> <p>b) de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden;</p> <p>c) de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers;</p> <p>d) de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn;</p> <p>e) de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd;</p> <p>f) de bevordering van het beveiligingsbewustzijn.</p>	5.1.1.1 Is er een informatiebeveiligingsbeleid vastgesteld dat voldoet aan de voorwaarden uit de BIO?	<p>✓Ja</p> <p>- Nee</p>	<p>10(1)b, 10(2)g</p> <p></p> <p></p> <p></p> <p></p> <p></p> <p></p> <p></p>	

Control 5.1.2				
Beoordeling van het informatiebeveiligingsbeleid				
Maatregel 5.1.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
<p>Maatregel 5.1.2.1 BBN 1</p> <p>Het informatiebeveiligingsbeleid wordt periodiek en in</p>	5.1.2.1 Is het vastgestelde informatiebeveiligingsbeleid actueel?	<p>✓Ja</p> <p>- Nee</p>	<p>10(1)b, 10(2)g</p> <p></p> <p></p> <p></p>	

aansluiting bij de (bestaande) bestuurs- en P&C cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.			-10(1)b, 10(2)g  	
--	--	--	---	--

Hoofdstuk 6

Control 6.1.1				
Rollen en verantwoordelijkheden bij informatiebeveiliging				
Maatregel 6.1.1.1	Vraag	Antwoord	Voldoet 10(1)b, 10(2)g	Voldoe t niet
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?	✓Ja, verantwoordelijkheden en rollen - Nee, alleen verantwoordelijkheden - Nee, alleen rollen - Nee, niet door de leiding - Nee		
Maatregel 6.1.1.2	Vraag	Antwoord	Voldoet	Voldoe t niet
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?	✓Ja - Nee		
Maatregel 6.1.1.3	Vraag	Antwoord	Voldoet	Voldoe t niet
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?	✓Ja - Nee	- 10(1)b, 10(2)g	
Maatregel 6.1.1.4	Vraag	Antwoord	Voldoet	Voldoe t niet
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 in een functie conform het CISO-functieprofiel?	✓Ja, er is een CISO aangesteld conform het CISO-functieprofiel - Nee, er is een CISO aangesteld maar niet conform het CISO-functieprofiel		

		- Nee		
--	--	-------	--	--

Control 6.1.2

Scheiding van taken

Maatregel 6.1.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
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 onbedoelde of ongeautoriseerde wijziging of misbruik van bedrijfsmiddelen waar te nemen of te voorkomen, door scheiding van taken?	✓Ja - Nee - 11 (1)	10(1)b, 10(2)g	

Control 6.1.3

Contact met overheidsinstanties

Maatregel 6.1.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
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 Is er een contactoverzicht uitgewerkt dat aangeeft welke functionarissen contact onderhouden met (overheids) instanties en toezichthouders over informatiebeveiligingsaangelegenheden?	✓Ja - Nee		
Maatregel 6.1.3.2	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 6.1.3.2 BBN 2 Het contactoverzicht wordt jaarlijks geactualiseerd.	6.1.3.2 Wordt het contactoverzicht jaarlijks geactualiseerd?	✓Ja - Nee		

Control 6.2.1

Beleid voor mobiele apparatuur

Maatregel 6.2.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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	6.2.1.1a Is de mobiele apparatuur zo ingericht dat geen bedrijfsinformatie wordt opgeslagen (zero footprint)?	✓Ja, beoordeeld en geactualiseerd - Dit is (nog) niet zo ingericht		

(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.				
Maatregel 6.2.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 6.2.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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.	6.2.1.1c Worden vertrouwelijke gegevens op mobiele apparatuur versleuteld?	<p>- Ja</p> <p>- Nee</p> <p>10(1)b, 10(2)g</p> <p></p> <p></p> <p></p> <p></p> <p></p>		
Maatregel 6.2.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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	6.2.1.1d Is het mogelijk om vertrouwelijke informatie op mobiele apparatuur 'op afstand' te wissen?	<p>- Ja</p> <p>- Nee</p> <p>10(1)b, 10(2)g</p> <p></p>		

<p>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.</p>				
Maatregel 6.2.1.2	Vraag	Antwoord	Voldoet	Voldoet niet
<p>Maatregel 6.2.1.2 BBN 2 Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd:</p> <p>a) in bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde;</p> <p>b) het device maakt deel uit van patchmanagement en hardening;</p> <p>c) er wordt gebruik gemaakt van Mobile Device Management MDM of van Mobile Application Management (MAM)-oplossingen;</p> <p>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;</p> <p>e) periodiek wordt getoetst of de punten in lid b), c) en d) worden nageleefd.</p>	<p>6.2.1.2a Komen gedragsaspecten van veilig mobiel werken aan de orde in bewustwordingsprogramma's?</p>	<p>✓ Ja</p> <p>- Nee</p> <p>- Nee, er zijn geen bewustwordingsprogramma's</p>		
Maatregel 6.2.1.2	Vraag	Antwoord	Voldoet	Voldoet niet
<p>Maatregel 6.2.1.2 BBN 2 Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd:</p> <p>a) in bewustwordingsprogramma's</p>	<p>6.2.1.2b Wordt patchmanagement en hardening toegepast op mobiele apparatuur?</p>	<p>✓ Ja, er wordt patchmanagement en hardening toegepast.</p> <p>- Nee, er wordt alleen patchmanagement toegepast.</p>		

<p>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.</p>		<p>- Nee, er wordt alleen hardening toegepast.</p> <p>- Nee</p>		
Maatregel 6.2.1.2	Vraag	Antwoord	Voldoet	Voldoet niet
<p>Maatregel 6.2.1.2 BBN 2 Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd:</p> <p>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</p>	<p>6.2.1.2c Wordt mobiele apparatuur daar waar mogelijk beheerd en beveiligd via een MDM- of MAM-oplossing?</p>	<p>✓ Ja, voor beheer en beveiliging</p> <p>- Nee, alleen voor beheer</p> <p>- Nee, alleen voor beveiliging</p> <p>- Nee</p>		

medewerker zakelijk gebruikt; e) periodiek wordt getoetst of de punten in lid b), c) en d) worden nageleefd.				
Maatregel 6.2.1.2	Vraag	Antwoord	Voldoet	Voldoet niet
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.	6.2.1.2d Tekenend eindgebruikers een gebruikersovereenkomst voor mobiel werken, voorafgaand aan het verkrijgen van toegang tot bedrijfsgegevens?	✓ Ja - Nee		
Maatregel 6.2.1.2	Vraag	Antwoord	Voldoet	Voldoet niet
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;	6.2.1.2e Wordt periodiek getoetst of de punten b, c en d worden nageleefd?	✓ Ja - Nee		

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.				
--	--	--	--	--

Control 6.2.2

Telewerken

Maatregel 6.2.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 6.2.2.1 BBN 2 Er wordt beleid vastgesteld met daarin de uitwerking welke systemen niet en welke systemen wel vanuit de thuiswerkplek of andere telewerkvoorzieningen mogen worden geraadpleegd. Dit beleid wordt bij voorkeur ondersteund door een MDM- en/of MAM-oplossing. De control kent geen verplichte overheidsmaatregelen. Deze maatregel is richtinggevend.	6.2.2.1 Is het telewerkbeleid geïmplementeerd?	✓ Ja - Nee		

Hoofdstuk 7

Control 7.1.1				
Screening				
Maatregel 7.1.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		








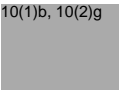


Control 7.1.2				
Arbeidsvoorwaarden				
Maatregel 7.1.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 7.1.2.1 BBN 1 Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.	7.1.2.1 Worden medewerkers bij indiensttreding of bij functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging?	✓Ja - Nee		
Maatregel 7.1.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
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 Zijn de geldende regelingen en instructies voor medewerkers ten aanzien van informatiebeveiliging eenvoudig toegankelijk?	✓Ja - Nee		

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

kunnen melden.

Control 7.2.2

Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Maatregel 7.2.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓ Ja - Nee	10(1)b, 10(2)g       	
Maatregel 7.2.2.2	Vraag	Antwoord	Voldoet	Voldoet niet
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.	7.2.2.2 Volgen medewerkers binnen drie maanden na indiensttreding een training I-bewustzijn?	- Ja 10(1)b, 10(2)g 		- 11 (1) 
Maatregel 7.2.2.3	Vraag	Antwoord	Voldoet	Voldoet niet
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?	- Ja 10(1)b, 10(2)g 		

Hoofdstuk 8

Control 8.1.3				
Aanvaardbaar gebruik van bedrijfsmiddelen				
Maatregel 8.1.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 8.1.3.1 BBN 1 Alle medewerkers zijn aantoonbaar geweest op de gedragsregels voor het gebruik van bedrijfsmiddelen.	8.1.3.1 Worden medewerkers gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen?	✓Ja - Nee		
Maatregel 8.1.3.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee, niet overeenkomstig de huis- of gedragsregels - Nee		

Control 8.2.1				
Classificatie van informatie				
Maatregel 8.2.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Control 8.3.1				
Beheer van verwijderbare media				
Maatregel 8.3.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee, geen instructie voor onherstelbare verwijdering van onnodige informatie - Nee	- 10(1)b, 10(2)g	

Control 8.3.2				
Verwijderen van media				
Maatregel 8.3.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee	10(1)b, 10(2)g	
Maatregel 8.3.2.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		
Maatregel 8.3.2.3	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Control 8.3.3				
Media fysiek overdragen				
Maatregel 8.3.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee	- 10(1)b, 10(2)g	
Maatregel 8.3.3.2	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 8.3.3.2 BBN 2 Het gebruik van koeriers of transporteurs van op BBN2 of hoger geclassificeerde	8.3.3.2 Voldoen de door uw organisatie gebruikte koeriers of transporteurs aan de eisen?	✓Ja - Nee	-1 0 (

informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.	opgestelde betrouwbaarheidseisen, wanneer zij BBN2 of hoger geclassificeerde informatie vervoeren?	- Niet van toepassing, wij maken geen gebruik van koeriers of transporteurs		
---	--	---	--	--

Hoofdstuk 9

Control 9.1.1				
Beleid voor toegangsbeveiliging				
Maatregel 9.1.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee	10(1)b, 10(2)g	

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

Control 9.2.1				
Registratie en afmelden van gebruikers				
Maatregel 9.2.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee	10(1)b, 10(2)g	
Maatregel 9.2.1.2	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 9.2.1.2 BBN 1 Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt	9.2.1.2 Is het gebruik van groepsaccounts gemotiveerd en vastgelegd?	- Ja 10(1)b, 10(2)g	-10(1)b, 10(2)g	

gemotiveerd en vastgelegd door de proceseigenaar.			-10(1)b, 10(2)g	
---	--	--	-----------------	--

Control 9.2.2

Gebruikers toegang verlenen

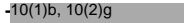



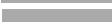



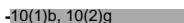







Maatregel 9.2.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 9.2.2.1 BBN 1 Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	9.2.2.1 Wordt toegang tot informatiesystemen alleen verleend na autorisatie door een bevoegd functionaris?	✓Ja - Nee	10(1)b, 10(2)g [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted]	
Maatregel 9.2.2.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee	-10(1)b, 10(2)g [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted]	
Maatregel 9.2.2.3	Vraag	Antwoord	Voldoet	Voldoet niet
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 bevoegdheden hebben voor het verlenen van toegangsrechten?	✓Ja - Nee		

Control 9.2.3

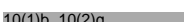





Beheren van speciale toegangsrechten

Maatregel 9.2.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Control 9.2.5**Beoordeling van toegangsrechten van gebruikers**

Maatregel 9.2.5.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 9.2.5.1 BBN 1 Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	9.2.5.1 Worden toegangsrechten minimaal eenmaal per jaar beoordeeld?	✓Ja - Nee	-10(1)b, 10(2)g        	
Maatregel 9.2.5.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee, wel gedocumenteerd maar niet behandeld als beveiligingsincident - Nee, niet gedocumenteerd, wel behandeld als beveiligingsincident - Nee		
Maatregel 9.2.5.3	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 9.2.5.3 BBN 2 Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	9.2.5.3 Worden toegangsrechten minimaal eenmaal per halfjaar beoordeeld?	✓Ja - Nee	-10(1)b, 10(2)g        	

Control 9.2.6**Toegangsrechten intrekken of aanpassen**

Maatregel 9.2.6.1	Vraag	Antwoord	Voldoet	Voldoet niet
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	9.2.6.1 Worden de toegangsrechten van gebruikers bij wijziging van functie aangepast?	✓Ja - Nee	10(1)b, 10(2)g      	

meer nodig zijn na het beëindigen van de oude functie. De control kent geen verplichte overheidsmaatregelen. Deze maatregel is richtinggevend.				
--	--	--	--	--

Control 9.3.1

Geheime authenticatie-informatie gebruiken

Maatregel 9.3.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	- Ja ✓Nee		

Control 9.4.1

Beperking toegang tot informatie

Maatregel 9.4.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja, fysiek en logisch - Ja, fysiek - Ja, logisch - Nee	-10(1)b, 10(2)g	
Maatregel 9.4.1.2	Vraag	Antwoord	Voldoet	Voldoet niet
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 Kunnen gebruikers alleen informatie met specifiek belang inzien en verwerken indien zij deze informatie nodig hebben voor de uitoefening van hun taak?	✓Ja - Nee		

Control 9.4.2

Beveiligde inlogprocedures

Maatregel 9.4.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 9.4.2.1 BBN 1 Als vanuit een onvertrouwde zone toegang wordt verleend	9.4.2.1 Wordt toegang vanuit een onvertrouwde omgeving naar een	✓Ja - Ja, anders,		

naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	vertrouwde zone alleen verleend op basis van minimaal two-factor authenticatie?	zie toelichting - Nee		
Maatregel 9.4.2.2	Vraag	Antwoord	Voldoet	Voldoet niet
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.	9.4.2.2a Krijgen leveranciers toegang tot het netwerk op basis van risicoafweging?	✓Ja - Nee		
Maatregel 9.4.2.2	Vraag	Antwoord	Voldoet	Voldoet niet
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.	9.4.2.2b Wordt in een registratie bijgehouden welke externe leverancier welke rechten toegekend heeft gekregen voor toegang?	✓Ja - Nee		







Control 9.4.3				
Systeem voor wachtwoordbeheer				
Maatregel 9.4.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
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.	9.4.3.1a Wordt gebruik gemaakt van wachtwoorden die aan de gestelde eisen voldoen?	✓Ja - Nee - 10 (1) B [redacted] [redacted] [redacted] [redacted]	- 10(1)b, 10(2)g [redacted]	

Maatregel 9.4.3.1 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.	Vraag 9.4.3.1b Heeft u vastgelegd op welke wijze u omgaat met mislukte pogingen tot inloggen?	Antwoord - Ja ✓Nee	Voldoet	Voldoet niet
Maatregel 9.4.3.2 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.).	Vraag 9.4.3.2 Worden wachtwoorden minimaal halfjaarlijks vernieuwd indien two-factor authenticatie niet mogelijk is?	Antwoord - Ja - Nee ✓Niet van toepassing, er wordt gebruikt gemaakt van two-factor authenticatie	Voldoet	Voldoet niet
Maatregel 9.4.3.3 Maatregel 9.4.3.3 BBN 2 De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	Vraag 9.4.3.3 Worden de eisen aan wachtwoorden geautomatiseerd afgedwongen?	Antwoord ✓Ja - Ja, anders. Zie toelichting. - Nee	Voldoet	Voldoet niet
Maatregel 9.4.3.4 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.	Vraag 9.4.3.4 Voldoen initiële wachtwoorden aan de gestelde eisen?	Antwoord ✓Ja - Nee, geen maximale geldigheidsduur wel verplichte wijziging bij eerste gebruik - Nee, geen verplichte wijziging bij eerste gebruik, wel maximale geldigheidsduur	Voldoet	Voldoet niet

Maatregel 9.4.3.4 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.	Vraag 9.4.3.4 Voldoen geresette wachtwoorden aan de gestelde eisen?	Antwoord - Nee ✓Ja - Nee, geen maximale geldigheidsduur wel verplichte wijziging bij eerste gebruik - Nee, geen verplichte wijziging bij eerste gebruik, wel maximale geldigheidsduur - Nee	Voldoet	Voldoet niet
Maatregel 9.4.3.5 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.	Vraag 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 ✓Ja - Nee	Voldoet	Voldoet niet

Control 9.4.4				
Speciale systeemhulpmiddelen gebruiken				
Maatregel 9.4.4.1 Maatregel 9.4.4.1 BBN 1 Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	Vraag 9.4.4.1 Heeft alleen bevoegd personeel toegang tot systeemhulpmiddelen?	Antwoord ✓Ja - Nee	Voldoet	Voldoet niet
Maatregel 9.4.4.2 Maatregel 9.4.4.2 BBN 2 Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	Vraag 9.4.4.2 Wordt het gebruik van systeemhulpmiddelen gelogd en is de logging gedurende een halfjaar beschikbaar gesteld voor onderzoek?	Antwoord - Ja 10(1)b, 10(2)g - Nee	Voldoet	Voldoet niet

Hoofdstuk 10

Control 10.1.1				
Beleid inzake het gebruik van cryptografische beheersmaatregelen				
Maatregel 10.1.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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 f genoemde onderwerpen zijn opgenomen?	✓Ja - Nee	-10(1)b, 10(2)g      	
Maatregel 10.1.1.2	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 10.1.1.2 BBN 2 Cryptografische toepassingen voldoen aan passende standaarden.	10.1.1.2 Voldoen cryptografische toepassingen aan passende standaarden?	✓Ja - Nee - Nee, er wordt geen gebruik gemaakt van cryptografische toepassingen		

Control 10.1.2				
Sleutelbeheer				
Maatregel 10.1.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 10.1.2.1 BBN 2 Ingeval van PKI-overheid-certificaten: hanteer de PKI-overheid-eisen t.a.v. het sleutelbeheer. In overige situaties: hanteer de standaard ISO-11770 voor het beheer van cryptografische sleutels.	10.1.2.1a Hanteert uw organisatie de PKI-overheid-eisen t.a.v. sleutelbeheer?	✓Ja - Nee - Niet van toepassing, er wordt geen gebruik gemaakt van PKI-Overheidscertificaten		

Maatregel 10.1.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
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.	10.1.2.1b Hanteert uw organisatie de ISO-11770 eisen t.a.v. sleutelbeheer in geval u geen gebruik maakt van een PKIoverheids-certificaat?	<p>✓Ja</p> <p>- Niet van toepassing, wij gebruiken enkel PKIOverheids-certificaten</p> <p>- Nee</p> <p>- Nee, er wordt geen gebruik gemaakt van cryptografische sleutels</p>		
Maatregel 10.1.2.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	<p>- Ja</p> <p>- Ja, op basis van een risico-afweging is niet overgegaan tot het maken van afspraken</p> <p>10(1)b, 10(2)g</p> <p>- Niet van toepassing, er wordt geen gebruik gemaakt van PKIOverheids-certificaten</p>		

Hoofdstuk 11

Control 11.1.1

Fysieke beveiligingszone

Maatregel 11.1.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓ Ja - Nee	10(1)b, 10(2)g	

Control 11.1.2

Fysieke toegangsbeveiliging

Maatregel 11.1.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓ Ja - Nee, er worden wel waarschuwingen verzonden, we hebben hier geen afspraken over - Nee	10(1)b, 10(2)g	

Control 11.1.3

Kantoren, ruimten en faciliteiten beveiligen

Maatregel 11.1.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 11.1.3.1 BBN 1 Sleutelbeheer is ingericht op basis van een sleutelplan.	11.1.3.1 Is het sleutelbeheer in uw organisatie ingericht op basis van een sleutelplan?	✓ Ja - Nee	10(1)b, 10(2)g	

Control 11.1.4

Beschermen tegen bedreigingen van buitenaf

Maatregel 11.1.4.1	Vraag	Antwoord	Voldoet	Voldoet niet
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	11.1.4.1 Zijn op basis van een expliciete risicoafweging beveiligingsmaatregelen genomen tegen bedreigingen van buitenaf?	- Ja - Nee 10(1)b, 10(2)g		

expliciete risicoafweging.		10(1)b, 10(2)g		
Maatregel 11.1.4.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Control 11.1.5

Werken in beveiligde gebieden

Maatregel 11.1.5.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 11.1.5.1 BBN 1 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?	✓Ja - Nee	- 10(1)b, 10(2)g	

Control 11.2.5

Verwijdering van bedrijfsmiddelen

Maatregel 11.2.5.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee	- 10(1)b, 10(2)g	

Control 11.2.6

Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein

Maatregel 11.2.6.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 11.2.6.1 BBN 1 Op basis van een expliciete risicoafweging worden	11.2.6.1 Worden bedrijfsmiddelen buiten het terrein	✓Ja - Nee	- 10(1)b, 10(2)g	

passende maatregelen genomen om bedrijfsmiddelen die zich buiten het terrein bevinden te beschermen. De control kent geen verplichte overheidsmaatregelen. Deze maatregel is richtinggevend.	voldoende beschermd?			
--	----------------------	--	--	--

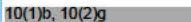

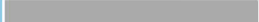



Control 11.2.9				
'Clear desk'- en 'clear screen'-beleid				
Maatregel 11.2.9.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 11.2.9.1 BBN 2 Een onbemende werkplek is altijd vergrendeld.	11.2.9.1 Is een onbemende werkplek altijd vergrendeld?	✓Ja - Nee	- 10(1)b, 10(2)g	
Maatregel 11.2.9.2	Vraag	Antwoord	Voldoet	Voldoet niet
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 informatie automatisch ontoegankelijk gemaakt na inactiviteit van maximaal 15 minuten?	✓Ja - Nee	- 10(1)b, 10(2)g	
Maatregel 11.2.9.3	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee	- 10(1)b, 10(2)g	
Maatregel 11.2.9.4	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee - Niet van toepassing, het overnemen van sessies is niet mogelijk		
Maatregel 11.2.9.5	Vraag	Antwoord	Voldoet	Voldoet

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?	- Ja - Nee ✓Niet van toepassing, wij maken geen gebruik van chipcardtoken	niet
---	---	--	------

Hoofdstuk 12

Control 12.1.1

Gedocumenteerde bedieningsprocedures

Maatregel 12.1.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓ Ja - Nee	10(1)b, 10(2)g        	

Control 12.1.2

Wijzigingsbeheer

Maatregel 12.1.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓ Ja - Nee		

Control 12.1.4

Scheiding van ontwikkel-, test- en productieomgevingen

Maatregel 12.1.4.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	- Ja, er wordt niet in de productie omgeving getest ✓ Ja, in de productieomgeving wordt alleen getest met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan - Nee, we testen (ook) in de productieomgeving		
Maatregel 12.1.4.2	Vraag	Antwoord	Voldoet	Voldoet

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?	<p>✓ Ja</p> <p>- Ja, 10(1)b, 10(2)g</p> <p></p> <p></p> <p></p> <p></p> <p></p> <p></p> <p></p> <p></p>		niet
		- Nee		

Control 12.2.1

Beheersmaatregelen tegen malware

Maatregel 12.2.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	<p>✓ Ja</p> <p>- Nee</p>		
Maatregel 12.2.1.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	<p>✓ Ja</p> <p>- Nee</p>		
Maatregel 12.2.1.3	Vraag	Antwoord	Voldoet	Voldoet niet
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?	<p>✓ Ja</p> <p>- Nee</p>		
Maatregel 12.2.1.4	Vraag	Antwoord	Voldoet	Voldoet niet
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?	<p>✓ Ja</p> <p>- Nee</p>		

Maatregel 12.2.1.5	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Control 12.3.1				
Back-up van informatie				
Maatregel 12.3.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee	-10(1)b. 10(2)g	
Maatregel 12.3.1.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	- Ja ✓Nee, ten dele - Nee		
Maatregel 12.3.1.3	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		
Maatregel 12.3.1.4	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Maatregel 12.3.1.5	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓ Ja - Nee		

Control 12.4.1				
Gebeurtenissen registreren				
Maatregel 12.4.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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 Voldoen logregels aan de gestelde eisen?	✓ Ja - Nee	- 10(1)b, 10(2)g [redacted] [redacted] [redacted] [redacted] [redacted]	
Maatregel 12.4.1.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓ Ja - Nee		
Maatregel 12.4.1.3	Vraag	Antwoord	Voldoet	Voldoet niet
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 op basis van een risico-inschatting, mede aan de hand van en de aard van de te beschermen gegevens en informatiesystemen, zodat	12.4.1.3 Maakt uw organisatie gebruik van voorzieningen voor het detecteren van aanvallen, waarbij dit gebruik gebaseerd is op een risico-inschatting?	- Ja 10(1)b, 10(2)g [redacted] [redacted] [redacted] [redacted] [redacted] - Nee		

aanvallen kunnen worden gedetecteerd.				
Maatregel 12.4.1.4	Vraag	Antwoord	Voldoet	Voldoet niet
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 binnen de juridische kaders gedeeld met de IBD via het passende kanaal?	✓Ja - Nee		
Maatregel 12.4.1.5	Vraag	Antwoord	Voldoet	Voldoet niet
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 Beschikt de SIEM en/of SOC over regels voor het rapporteren van incidenten aan het verantwoordelijk management?	- Ja - Nee 10(1)b, 10(2)g		

Control 12.4.2

Beschermen van informatie in logbestanden

Maatregel 12.4.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		
Maatregel 12.4.2.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee	10(1)b, 10(2)g	
Maatregel 12.4.2.3	Vraag	Antwoord	Voldoet	Voldoet

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.	12.4.2.3 Worden logbestanden minimaal half jaarlijks gecontroleerd door een onafhankelijk functionaris?	✓Ja - Nee		niet
Maatregel 12.4.2.4	Vraag	Antwoord	Voldoet	Voldoet niet
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 daartoe zo snel mogelijk gemeld via de vastgestelde procedure?	✓Ja - Nee		

Control 12.6.1

Beheer van technische kwetsbaarheden

Maatregel 12.6.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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.	12.6.1.1a Worden bij een hoge kans op misbruik en een hoge kans op schade patches uiterlijk binnen een week geïnstalleerd?	✓Ja - Nee		
Maatregel 12.6.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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.	12.6.1.1b Worden in afwachting van het installeren van patches op basis van een expliciete risicoafweging mitigerende maatregelen genomen?	✓Ja - Nee		

Control 12.6.2

Beperkingen voor het installeren van software

Maatregel 12.6.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 12.6.2.1 BBN 2 Gebruikers kunnen op hun	12.6.2.1 Kunnen gebruikers alleen	✓Ja		

werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	toegestane software installeren?	- Nee		
--	----------------------------------	-------	--	--

Hoofdstuk 13

Control 13.1.2				
Beveiliging van netwerkdiensten				
Maatregel 13.1.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
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 detectievoorzieningen zoals de toelichting uit de maatregel voorschrijft?	✓Ja - Nee, niet op basis van een risico-inschatting - Nee		
Maatregel 13.1.2.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		
Maatregel 13.1.2.3	Vraag	Antwoord	Voldoet	Voldoet niet
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 buiten het gecontroleerd gebied?	✓Ja - Nee		
Maatregel 13.1.2.4	Vraag	Antwoord	Voldoet	Voldoet niet
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,	13.1.2.4 Zijn er maatregelen getroffen in koppelpunten om aanvallen die de beschikbaarheid negatief beïnvloeden te signaleren en hierop te reageren?	✓Ja - Nee - Nee, wel te signaleren, maar er zijn geen		

Distributed Denial of Service attacks) te signaleren en hierop te reageren.		maatregelen getroffen om hierop te reageren		
---	--	---	--	--

Control 13.1.3

Scheiding in netwerken

Maatregel 13.1.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Control 13.2.3

Elektronische berichten

Maatregel 13.2.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 13.2.3.1 BBN 1 Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en af luisteren op de 'pas toe of leg uit'-lijst van het Forum. Voor beveiliging van websiteverkeer gelden de open standaarden tegen af luisteren 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?	✓Ja - Nee		
Maatregel 13.2.3.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee - Niet van toepassing, wij maken geen gebruik van Digikoppeling.		
Maatregel 13.2.3.3	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 13.2.3.3 BBN 2 Maak gebruik van PKI-overheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn	13.2.3.3 Wordt er gebruik gemaakt van PKI-overheid-certificaten bij web- en mailverkeer van gevoelige gegevens?	✓Ja - Nee		

onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlelen.				
Maatregel 13.2.3.4	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Control 13.2.4				
Vertrouwelijkheids- of geheimhoudingsovereenkomst				
Maatregel 13.2.4.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 13.2.4.1 BBN 2 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?	✓Ja - Nee	10(1)b, 10(2)g	

Hoofdstuk 14

Control 14.1.1				
Analyse en specificatie van informatiebeveiligingseisen				
Maatregel 14.1.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee, niet expliciet - Nee		

Control 14.2.1				
Beleid voor beveiligd ontwikkelen				
Maatregel 14.2.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	- Ja - Nee ✓Niet van toepassing, wij ontwikkelen geen software		

Control 14.2.2				
Procedure voor wijzigingsbeheer met betrekking tot systemen				
Maatregel 14.2.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Control 14.2.5				
Beveiligde ontwikkelomgeving				
Maatregel 14.2.5.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 14.2.5.1 BBN 1 Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging.	14.2.5.1 Worden ontwikkelomgevingen voor systemen passend beveiligd op basis van een expliciete	- Ja - 10(1)b, 10(2)g [redacted] [redacted]		

	risicoafweging?	- Nee ✓Niet van toepassing, wij beschikken niet over syteemontwikkelomgevingen		
--	-----------------	---	--	--

Control 14.2.6

Uitbestede softwareontwikkeling

Maatregel 14.2.6.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 14.2.6.1 BBN 1 Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.	14.2.6.1 Worden passende en noodzakelijke beveiligingsmaatregelen aan de leverancier opgelegd?	✓Ja - Nee		

Control 14.2.8

Systeemacceptatietests

Maatregel 14.2.8.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 14.2.8.1 BBN 1 Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	14.2.8.1 Vinden acceptatietesten van systemen op basis van gestructureerde testmethodieken plaats?	✓Ja - Nee		
Maatregel 14.2.8.2	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 14.2.8.2 BBN 1 Van de resultaten van de testen wordt verslag gemaakt.	14.2.8.2 Worden testverslagen gemaakt waarin de resultaten van het testen worden vastgelegd?	✓Ja - Nee		

Hoofdstuk 15

Control 15.1.1				
Informatiebeveiligingsbeleid voor leveranciersrelaties				
Maatregel 15.1.1.1	Vraag	Antwoord	Voldoet	Voldoe t niet
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?	✓Ja - Nee, niet op basis van een expliciete risicoafweging - Nee		
Maatregel 15.1.1.2	Vraag	Antwoord	Voldoet	Voldoe t niet
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?	- Ja 10(1)b, 10(2)g - Nee		
Maatregel 15.1.1.3	Vraag	Antwoord	Voldoet	Voldoe t niet
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?	✓Ja - Nee	10(1)b, 10(2)g	

Control 15.1.2				
Opnemen van beveiligingsaspecten in leveranciersovereenkomsten				
Maatregel 15.1.2.1	Vraag	Antwoord	Voldoe t	Voldoe t niet
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?	✓Ja - Nee		
Maatregel 15.1.2.2	Vraag	Antwoord	Voldoe t	Voldoe t niet

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?	✓Ja - Nee - Nee, wel prestatie-indicatoren geen verantwoordingsrapportage - Nee, wel verantwoordingsrapportage, geen prestatie-indicatoren		
Maatregel 15.1.2.3	Vraag	Antwoord	Voldoet	Voldoet niet
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.	15.1.2.3 Worden consequenties van door leveranciers opgelegde contractvoorwaarden, voorafgaand aan het tekenen van een contract, door middel van een risicoanalyse, inzichtelijk gemaakt?	✓Ja - Nee, niet expliciet - Nee, niet voorafgaand aan het tekenen van een contract - Nee - Niet van toepassing, wij accepteren geen opgelegde contractvoorwaarden van leveranciers		
Maatregel 15.1.2.4	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		
Maatregel 15.1.2.5	Vraag	Antwoord	Voldoet	Voldoet niet
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.	15.1.2.5a Wordt voor het afsluiten van een contract op basis van risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is?	✓Ja - Nee		
Maatregel 15.1.2.5	Vraag	Antwoord	Voldoet	Voldoet niet

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.	15.1.2.5b Maakt een expliciete exit-strategie een vast onderdeel uit van contracten?	✓Ja - Nee, niet expliciet - Nee		
Maatregel 15.1.2.6	Vraag	Antwoord	Voldoet	Voldoet niet
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'?	✓Ja - Nee		

Control 15.1.3

Toeleveringsketen van informatie- en communicatietechnologie

Maatregel 15.1.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
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.	15.1.3.1a Maken de leveranciers van uw organisatie hun keten van toeleveranciers bekend?	✓Ja - Nee		
Maatregel 15.1.3.1	Vraag	Antwoord	Voldoet	Voldoet niet

Control 15.2.1

Monitoring en beoordeling van dienstverlening van leveranciers

Maatregel 15.2.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 15.2.1.1 BBN 2 Jaarlijks wordt de prestatie van leveranciers op het gebied van	15.2.1.1 Worden de prestaties van leveranciers op het gebied van	✓Ja - Nee	10(1)b, 10(2)g.	

informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie- indicatoren, zoals in het contract opgenomen is.	informatiebeveiliging jaarlijks beoordeeld op vooraf vastgestelde prestatie-indicatoren?			
---	---	--	--	--

Hoofdstuk 16

Control 16.1.2				
Rapportage van informatiebeveiligingsgebeurtenissen				
Maatregel 16.1.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		
Maatregel 16.1.2.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		
Maatregel 16.1.2.3	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee, interne medewerkers wel, externe medewerkers niet - Nee	1 0 10(1)b, 10(2)g	
Maatregel 16.1.2.4	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee, niet binnen uiterlijk 24 uur - Nee		
Maatregel 16.1.2.5	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		
Maatregel 16.1.2.6	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 16.1.2.6 BBN 1 De opvolging van incidenten wordt	16.1.2.6 Wordt de opvolging maandelijks gerapporteerd aan de	✓Ja - Nee		

maandelijks gerapporteerd aan de verantwoordelijke.	verantwoordelijke?	- Nee, wij rapporteren niet		
Maatregel 16.1.2.7	Vraag	Antwoord	Voldoet	Voldoet niet
		✓ Ja - Nee		

Control 16.1.3

Rapportage van zwakke plekken in de informatiebeveiliging

Maatregel 16.1.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓ Ja - Nee, wel gepubliceerd maar niet ingericht - Nee, wel ingericht maar niet gepubliceerd - Nee		

Control 16.1.4

Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen

Maatregel 16.1.4.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓ Ja - Nee, niet binnen 72 uur - Nee		

Control 16.1.6

Lering uit informatiebeveiligingsincidenten

Maatregel 16.1.6.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 16.1.6.1 BBN 2 Beveiligingsincidenten worden	16.1.6.1 Wordt de informatie verkregen uit het	✓ Ja		

geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.	beoordelen van beveiligingsmeldingen, geëvalueerd met als doel beheersmaatregelen te verbeteren?	- Nee		
Maatregel 16.1.6.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Control 16.1.7

Verzamelen van bewijsmateriaal

Maatregel 16.1.7.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	- Ja ✓Nee		

Hoofdstuk 17

Control 17.1.1				
Informatiebeveiligingscontinuïteit plannen				
Maatregel 17.1.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee	10(1)b, 10(2)g	

Control 17.1.3				
Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren				
Maatregel 17.1.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 17.1.3.1 BBN 2 Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.	17.1.3.1 Worden continuïteitsplannen jaarlijks getest op geldigheid en bruikbaarheid?	✓Ja - Nee	10(1)b, 10(2)g	
Maatregel 17.1.3.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		
Maatregel 17.1.3.3	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Hoofdstuk 18

Control 18.1.1				
Vaststellen van toepasselijke wetgeving en contractuele eisen				
Maatregel 18.1.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee	10(1)b, 10(2)g	

Control 18.1.3				
Beschermen van registraties				
Maatregel 18.1.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Control 18.1.4				
Privacy en bescherming van persoonsgegevens				
Maatregel 18.1.4.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		
Maatregel 18.1.4.2	Vraag	Antwoord	Voldoet	Voldoet niet
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.	18.1.4.2a Wordt de naleving van het privacy beleid regelmatig gecontroleerd?	✓Ja - Nee	10(1)b, 10(2)g	
Maatregel 18.1.4.2	Vraag	Antwoord	Voldoet	Voldoet niet

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.	18.1.4.2b Wordt de logging van de verwerking van persoonsgegevens regelmatig gecontroleerd op rechtmatig gebruik?	✓Ja - Nee	10(1)b, 10(2)g	
--	---	------------------	----------------	--

Control 18.1.5

Beschermen van registraties

Maatregel 18.1.5.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		

Control 18.2.1

Onafhankelijke beoordeling van informatiebeveiliging

Maatregel 18.2.1.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee		
Maatregel 18.2.1.2	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓Ja - Nee	10(1)b, 10(2)g	

Control 18.2.2

Naleving van beveiligingsbeleid en -normen

Maatregel 18.2.2.1	Vraag	Antwoord	Voldoet	Voldoet niet
Maatregel 18.2.2.1 BBN 1 In de P&C-cyclus wordt	18.2.2.1 Is er een werkend systeem van controle en	✓Ja		

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.	rapportages over informatiebeveiliging aan het bestuur?	- Nee		
--	---	-------	--	--

Control 18.2.3

Beoordeling van technische naleving

Maatregel 18.2.3.1	Vraag	Antwoord	Voldoet	Voldoet niet
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?	✓ Ja - Nee	10(1)b, 10(2)g	