VNG Realisatie

# Suwinet-guidance

## Handreiking ENSIA-verantwoording voor Suwinet

**VNG Realisatie**

Nassaulaan 12
2514 JS Den Haag

maart 2020

# Inhoud

# Inleiding Suwinet-guidance

Deze handreiking is uitgegeven door het ENSIA-team van VNG Realisatie (VNG R) en is ontwikkeld en afgestemd met NOREA, BKWI, SUWI-team VNG-R, IBD, Ministerie van SZW en de pilot gemeenten ENSIA BIO.

Deze handreiking is bedoeld als guidance voor de invuller van de met “IT-audit” aangemerkte vragen in de BIO-vragenlijst van ENSIA voor Suwinet. Het doel is richting geven voor de invuller bij het beantwoorden van IT-audit vragen en voor de auditor bij het beoordelen van de gegeven antwoorden. Het resultaat moet zijn dat gemeenten met de juiste scope de juiste antwoorden geven bij de BIO controls/maatregelen en bij de ENSIA vragen.

Deze guidance wordt jaarlijks bijgesteld als gevolg van input vanuit gebruikers ENSIA als de audit community (via de vakgroep van de NOREA). Het beheer van deze notitie ligt bij VNG Realisatie.

# 1. Achtergrond

Gemeenten verantwoorden zich jaarlijks volgens de ENSIA-systematiek. Zij geven zo inzicht in de mate waarin de gemeente compliant is aan de BIO. Door gemeenten wordt verantwoording afgelegd langs twee pijlers:

- Horizontaal ten behoeve van de verantwoording van het college aan de raad over de mate waarin de gemeentelijke bedrijfsvoering in control is op het gebied van informatiebeveiliging met als norm de BIO.
- Verticaal ten behoeve van de verantwoording aan de toezichthouders en stelselhouders van het Rijk.

Jaarlijks wordt door de Regieraad ENSIA vastgesteld op welke wijze en met welke scope extra zekerheid verkregen wordt door het laten controleren van een deel van de uitkomsten van de ENSIA-zelfevaluatie door een bij de NOREA aangesloten auditor. Het ministerie van SZW bepaalt de selectie van normen uit de BIO voor de verantwoording Suwinet (op basis van de SUWI-regeling art. 5.2.2. en art. 6.4). Deze selectie is bij het BKWI gepubliceerd als de Verantwoordingsrichtlijn Informatiebeveiliging GeVS. Deze guidance is alleen gericht op de verantwoording Suwinet.

# 2. Verantwoordingsproces

Het verantwoordingsproces bestaat uit een aantal te doorlopen stappen en kent een aantal spelers. Afhankelijk van de ontvanger van de verantwoording (horizontaal of verticaal) zijn er een aantal te volgen stappen. Voor de horizontale verantwoording ligt de nadruk ligt op de (gemeente-brede) interne verantwoording. Bij de verticale verantwoording ligt de nadruk op audit (assurance) van de collegeverklaring en het in te leveren/te uploaden bewijsmateriaal.

De verantwoording Suwinet vindt plaats op basis van een zelfevaluatie op de jaarlijkse BIO vragenlijst ENSIA. Deze fase ‘zelfevaluatie’ vindt plaats in de periode 1 juli tot en met 31 december. De gemeente voert de zelfevaluatie uit binnen de eigen organisatie en verwerkt de uitkomsten uit de te ontvangen Third Party Mededelingen (TPM’s) van serviceorganisaties (indien van toepassing). In de ENSIA fase ‘verantwoorden’ wordt de ENSIA uitkomsten geanalyseerd en getoetst door een IT-auditor. Voor 1 mei dienen de verantwoordingsdocumenten (vastgesteld door het College) te worden ge-upload in de ENSIA tooling. De verantwoording Suwinet wordt elektronische aangeleverd aan het BWKI. Het BKWI verwerkt de uitkomsten van de individuele gemeenten in een transparantierapportage voor het ministerie van SZW.

# 3. Spelers in het veld

Voor 2020 zijn de volgende stakeholders in beeld voor wat betreft de IT-audit rondom Suwinet.

| **Speler** | **Uitleg** |
|---|---|
| Gemeente | Spreekt voor zich. |
| Serviceorganisatie | De partij waar de gemeente in meerdere of mindere mate SUWI taken aan uitbesteed heeft. |
| Lijnmanager | De eindverantwoordelijke functionaris binnen een gemeente die verantwoordelijk is voor het uitvoeren van 1 of meer SUWI taken en zich ook daarover moet verantwoorden. |
| Security Officer / de gemandateerde/ intern controleur | De persoon die de lijnmanager ondersteunt met het uitvoeren van controles en die gemachtigd is specifieke rapportages of detail logging op te vragen bij BKWI. Deze functionaris is bij BKWI bekend. |
| Gebruikersbeheerder Suwinet | De functionaris bij de gemeente/uitvoeringsorganisatie die het uitvoerende werk doet rondom afmelden, wijzigen, aanmelden van gebruikers en het onderhouden van de gebruikers autorisatiematrix. |
| BKWI | De partij die de jaarlijkse rapportage maakt aan SZW, de beheerder van Suwinet-inkijk en Suwinet-inlezen. BKWI weet van alle aansluitingen wie de gebruikersadministratie uitvoert. De rol van gebruikersbeheerder wordt toebedeeld door het BKWI. |
| Inlichtingenbureau | De partij via welke DKD-inlezen verloopt. Zie ook: www.inlichtingenbureau.nl voor de routeervoorziening Digitaal Klantdossier. |

# 4. Opbouw guidance

| Items | Uitleg |
|---|---|
| Hoofdstuk | Hoofdstuknummer en titel uit de BIO |
| Paragraaf | Paragraafnummer en titel uit de BIO |
| Control | Controlnummer en titel uit de BIO |
| Toelichting Control | Controltekst uit de BIO |
| Maatregel | Overheidsmaatregelnummer en tekst uit de BIO |
| Maatregel geldt voor | Toewijzing maatregel aan Suwinet-inkijk en/of Suwinet-inlezen en/of DKD-inlezen |
| Norm van toepassing op | Waar wordt de maatregel geïmplementeerd? |
| Nadere toelichting | Achtergrondinformatie |
| Betrokken rollen | Functionarissen betrokken bij de invulling van control en maatregel |
| Scope | Reikwijdte van de control en maatregel |
| Aandachtspunten | Dit zijn de aandachtspunten voor de gemeente en de auditor voor waarop gecontroleerd wordt |
| Testaanpak | **Dit zijn suggesties!** Concrete aanwijzingen voor het voorbereiden en uitvoeren van de test. |
| Relevante documenten | **Dit zijn suggesties!** Documenten die als bewijslast kunnen dienen voor de auditor. |

# 5. Suwinet guidance per BIO control

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 5 | Informatiebeveiligingsbeleid | | |
| **Paragraaf** | 5.1 | Aansturing door de directie van de informatiebeveiliging | | |
| **Control** | 5.1.1 | Beleidsregels voor informatiebeveiliging | | |
| **Toelichting control** | | Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen. | | |
| **Maatregel** | 5.1.1.1 | Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten:<br>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<br>b) De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden<br>c) De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers<br>d) De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn<br>e) De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd<br>f) de bevordering van het beveiligingsbewustzijn | | |
| **Maatregel geldt voor** | | | **Norm van toepassing op** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Serviceorganisatie |
| x | x | x | x | x |
| | | | | |
| **Betrokken rollen** | | CISO, Directie, College | | |
| | | | | |
| **Scope** | | Beleid | | |
| **Nadere toelichting** | | Let op de specifieke aandachtspunten voor de beveiliging van Suwinet gegevens en SUWI gerelateerde wetgeving (zie bijvoorbeeld het BIO OP product van de IBD - Handreiking informatiebeveiligingsbeleid, hoofdstuk 5.2)<br>De focus ligt op de governance (incl. afspraken over de wijze van verantwoording).<br>Er kan onderscheid gemaakt worden in een strategisch beleid en een tactisch beleid. | | |
| **Aandachtspunten** | | Er is een lijnmanager verantwoordelijk voor de uitvoering (van beleid en SUWI processen).<br>Deze verantwoordelijke lijnmanager(s) rapporteert/rapporteren aan de directie over informatiebeveiligingsaangelegenheden met betrekking tot het SUWI stelsel | | |

| | |
|---|---|
| | Deze lijnmanager is betrokken bij de behandeling van incidenten waarbij SUWI geraakt wordt.<br>In het beleid dient opgenomen te zijn dat de lijnmanager verantwoordelijk is voor de toegang tot de SUWI informatie en het juiste gebruikers beheer (laat uitvoeren) bij in-dienst/wijziging van functie/uit-dienst. |
| **Testaanpak** | Interview de verantwoordelijke functionarissen zoals opgenomen in beleid (of mandaatregister). Inspecteer het beveiligingsbeleid. |
| **Relevante documenten** | Vastgesteld beleid Informatieveiligheid, notulen collegeverklaring vaststelling. Hierbij kan gebruik gemaakt worden van een uitwerking in een specifiek informatiebeveiligingsbeleid op afdelings- of dienstniveau. Wijzigingen in algemeen beleid kunnen dan uitgewerkt worden naar beleid op afdelings- of dienstenniveaus zodat de verschillende documenten op elkaar blijven aansluiten.<br>Vaststellen van strategisch beleid door college (zie bijvoorbeeld het format informatiebeveiligingsbeleid van de IBD). |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 5 | Informatiebeveiligingsbeleid | | |
| **Paragraaf** | 5.1 | Aansturing door de directie van de informatiebeveiliging | | |
| **Control** | 5.1.2 | Beoordeling van het informatiebeveiligingsbeleid | | |
| **Toelichting control** | | 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. | | |
| **Maatregel** | 5.1.2.1 | Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| x | x | x | x | x |
| | | | | |
| **Betrokken rollen** | | CISO, Directie, College | | |
| **Scope** | | Beleid | | |
| **Nadere toelichting** | | De organisatie dient het (strategisch) beleid regelmatig te beoordelen en zo nodig bij te stellen.<br>De focus ligt op de frequentie van bijstelling. | | |
| **Aandachtspunten** | | NB: indien een gemeente in een structuur werkt van strategisch en tactisch beleid, dan kan het strategisch beleid ouder zijn, want het is dan generiek van opzet. Het beleid dient aan te sluiten bij een verkiezingscyclus (maximaal 5 jaar oud). | | |
| **Testaanpak** | | Controleer de datum van vaststelling van het informatiebeveiligingsbeleid.<br>Stel vast of het beleid wordt geëvalueerd Past dit binnen de wijzigingscyclus? Zo ja, dan hoeft het centrale beleid niet jonger te zijn dan 4 jaar. | | |
| **Relevante documenten** | | Beleid Informatieveiligheid, Notulen collegeverklaring vaststelling. Indien gebruik gemaakt wordt van een specifiek informatiebeveiligingsbeleid (beleidskader op dienstniveau incl. gelijke release. | | |

| | |
|---|---|
| | Vaststellen van strategisch beleid (zie bijvoorbeeld IBD OP product).<br>Ondertekening van het beleid conform mandaatregister of document waarin bevoegdheden zijn ingericht. |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 6 | Organiseren van informatiebeveiliging | | |
| **Paragraaf** | 6.1 | Interne organisatie | | |
| **Control** | 6.1.1 | Rollen en verantwoordelijkheden bij informatiebeveiliging | | |
| **Toelichting control** | | Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. | | |
| **Maatregel** | 6.1.1.1 | De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| x | x | x | x | x |
| | | | | |
| **Betrokken rollen** | | Verantwoordelijke voor Suwinet (lijnmanager), IT leverancier | | |
| **Scope** | | Beleid, afdelingsbeleid | | |
| **Nadere toelichting** | | De governance dient in het informatiebeveiligingsbeleid een plek te hebben. Maar specifiek voor Suwinet zijn er een aantal rollen die mogelijk niet in het centrale beleid uitgewerkt hoeven te zijn. Hiervoor dient de afdelingsmanager mogelijk aanvullend beleid te schrijven of in een afdelingsnotitie te hebben uitgewerkt welke rollen er onderkend zijn en wie deze uitvoeren. | | |
| **Aandachtspunten** | | De invulling van de specifieke Suwinet rollen kan op meerdere plekken uitgewerkt zijn.<br>Tenminste de volgende rollen moeten belegd zijn:<br>• Wie autoriseert toegang<br>• Wie controleert het gebruik van Suwinet<br>• Wie controleert de actualiteit van de gebruikersadministratie<br>• Wie meldt of verwerkt incidenten in relatie tot Suwinet. | | |
| **Testaanpak** | | Controleer de beschikbare documentatie op het aanwezig zijn van hierboven genoemde en belegde Suwinet rollen en verantwoordelijkheden. | | |
| **Relevante documenten** | | Suwinet-inkijk: Vastgestelde autorisatiematrix (rolbepaling), gebruikersadministratie.<br>Suwinet-inlezen: uit de logging van het systeem moet blijken dat de autorisatiematrix in lijn is met de logging.<br>DKD-Inlezen: uit de logging van het systeem moet blijken dat de autorisatiematrix in lijn is met de logging. | | |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 6 | Organiseren van informatiebeveiliging | | |
| **Paragraaf** | 6.1 | Interne organisatie | | |
| **Control** | 6.1.1 | Rollen en verantwoordelijkheden bij informatiebeveiliging | | |
| **Toelichting control** | | Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. | | |
| **Maatregel** | 6.1.1.3 | De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| x | x | x | x | x |
| | | | | |
| **Betrokken rollen** | | Bestuur, HRM | | |
| **Scope** | | Personeelsbeleid, informatiebeveiligingsbeleid | | |
| **Nadere toelichting** | | De governance dient in het informatiebeveiligingsbeleid een plek te hebben. De rol en de verantwoordelijkheden van de CISO dient beschreven te zijn in het beleid en de CISO is aangesteld (zie voorbeeld functieprofiel van de IBD). Als de gemeente gebruik maakt van HR21 (functiewaarderingssysteem voor gemeenten), dan is er gebruik gemaakt van de indelingsmotivering uit bijlage 1 van het BIO OP product Handreiking functieprofiel CISO van de IBD (aanwijzing, geen verplichting). | | |
| **Aandachtspunten** | | Tenminste de onafhankelijke positie moet zijn uitgewerkt:<br>• Mandaat<br>• Adviesfunctie<br>• Controle naleving beleid<br>• Rapportage in de lijn<br>• Ondersteuning in de lijn | | |
| **Testaanpak** | | Controleer het functieprofiel of het HR21 indelingsmotiveringsbesluit op de aanwezige punten. Er dient functiescheiding te zijn aangebracht daar waar sprake is van tegengestelde maatregelen, daar waar de functionaris meerdere rollen bekleed. | | |
| **Relevante documenten** | | Functieprofiel CISO | | |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 6 | Organiseren van informatiebeveiliging | | |
| **Paragraaf** | 6.1 | Interne organisatie | | |
| **Control** | 6.1.2 | Scheiding van taken | | |
| **Toelichting control** | | Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbedoeld of wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. | | |
| **Maatregel** | 6.1.2.1 | Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| x | x | x | x | x |
| | | | | |

| | |
|---|---|
| **Betrokken rollen** | Verantwoordelijke voor Suwinet (lijnmanager), HRM |
| **Scope** | Personeelsbeleid, proces en procedurecontrole gegevensgebruik |
| **Nadere toelichting** | Voor deze maatregel worden de beveiligingsrollen uit 6.1.1.3 getoetst. |
| **Aandachtspunten** | Scheiding van taken (*segregation of duties*)<br>Onafhankelijke controle van het gegevensgebruik en autorisatiebeheer |
| **Testaanpak** | Toets of het gebruik van gegevens uit Suwinet door iemand anders wordt gecontroleerd dan een gebruiker. |
| **Relevante documenten** | Functie- en taakomschrijvingen. |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 7 | Veilig personeel | | |
| **Paragraaf** | 7.2 | Tijdens het dienstverband | | |
| **Control** | 7.2.2 | Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging | | |
| **Toelichting control** | | Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. | | |
| **Maatregel** | 7.2.2.1 | 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. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| x | x | x | x | x |

| | |
|---|---|
| **Betrokken rollen** | Verantwoordelijke voor Suwinet (lijnmanager) |
| **Scope** | Bewustwording |
| **Nadere toelichting** | Bewustwording is essentieel in het werken met persoonsgegevens. De organisatie dient een bewustwordingsprogramma te hebben. |
| **Aandachtspunten** | Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar mogelijk ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders).<br>Het kan zijn dat de afdeling meeloopt in een organisatie-breed programma, dit is ook goed.<br>Zijn specifieke Suwinet risico's ook meegenomen in het bewustwordingstraject? |
| **Testaanpak** | Interview de verantwoordelijke voor Suwinet en vraag hoe hij/zij binnen zijn afdeling omgaat met deze maatregel<br>Onderzoek de organisatie agenda op het aanwezig zijn van bewustwordingsactiviteiten.<br>Mogelijk financiële uitgaven in het kader van bewustwording<br>Interview een willekeurige gebruiker (ten minste 3) en vraag hem wanneer hij/zij iets gedaan heeft aan bewustwording.<br>Bewijs van deelname aan e-learning en/of bewustzijnscampagne. |
| **Relevante documenten** | Huisregels, e-learning, domeinspecifieke verplichtingen in aanvulling op huisregels (voor zover niet elders in de organisatie uitgewerkt). |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 9 | Toegangsbeveiliging | | |
| **Paragraaf** | 9.2 | Beheer van toegangsrechten van gebruikers | | |
| **Control** | 9.2.1 | Registratie en afmelden van gebruikers | | |
| **Toelichting control** | | Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. | | |
| **Maatregel** | 9.2.1.1 | Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| x | x | x | x | x |
| | | | | |
| **Betrokken rollen** | | Verantwoordelijke voor Suwinet (lijnmanager), HRM, gebruikersbeheerder | | |
| **Scope** | | Toegangsverlening Suwinet | | |
| **Nadere toelichting** | | Hangt samen met maatregel 6.1.1.1<br>Worden gebruikers van Suwinet gegevens altijd op dezelfde manier geautoriseerd tot de Suwinet omgeving en is dat proces mogelijk organisatie-breed uitgewerkt?<br>De afdelingsmanager heeft een belangrijke rol, hij moet toezien op het juiste gebruik van Suwinet en ervoor zorgen dat er niet te veel mensen toegang hebben, en ook dat ze niet te lang toegang hebben. | | |
| **Aandachtspunten** | | Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar mogelijk ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders).<br>Het kan zijn dat de afdeling meeloopt in een organisatie-breed programma (bijvoorbeeld Identity and Access Management (IAM) programma bij HR en of IT), dit is ook goed.<br>Deze maatregel heeft betrekking op de processen voor In dienst, doorstroom en uitstroom.<br>In het proces van nieuwe accounts geeft de manager opdracht om een account aan te maken. Hierbij wordt opgeven welke rol moet worden toegekend. Indien dit een aanvullende rol betreft op de bestaande autorisatiematrix, dan dient deze te worden opgenomen. | | |
| **Testaanpak** | | Interview de verantwoordelijke voor Suwinet en vraag hoe hij/zij binnen zijn afdeling omgaat met deze maatregel.<br>De lokale Suwinet administratie voor gebruikersbeheer dient synchroon te zijn aan de autorisatiematrix bij Suwinet Inkijk. Controleer hoe ervoor gezorgd wordt dat de lijnmanager periodiek controleert welke gebruikers waartoe geautoriseerd zijn, en of de beide administraties synchroon lopen. | | |
| **Relevante documenten** | | autorisatiematrix in vergelijking met de autorisatie tot Suwinet Inkijk | | |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 9 | Toegangsbeveiliging | | |
| **Paragraaf** | 9.2 | Beheer van toegangsrechten van gebruikers | | |
| **Control** | 9.2.1 | Registratie en afmelden van gebruikers | | |
| **Toelichting control** | | Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. | | |
| **Maatregel** | 9.2.1.2 | Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| n.v.t. | x | x | x | x |
| | | | | |
| **Betrokken rollen** | | Verantwoordelijke voor Suwinet (lijnmanager), IT, leverancier | | |
| **Scope** | | Toegangsverlening Suwinet, gebruikersaccounts | | |
| **Nadere toelichting** | | Hangt samen met 6.1.1.1 en 9.2.1.1 | | |
| **Aandachtspunten** | | Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar mogelijk ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders).<br>Het kan zijn dat de afdeling meeloopt in een organisatie-brede procedure.<br>Indien gebruik gemaakt wordt van groepsaccount dient de afdelingsmanager Suwinet/sociaal domein speciaal toegang geven. | | |
| **Testaanpak** | | Interview de verantwoordelijke voor de processen met Suwinet en vraag hoe hij/zij binnen zijn afdeling omgaat met deze maatregel.<br>Onderzoek de organisatie of er een specifieke procedure is voor het aan- en afmelden van gebruikers met toegang tot de gegevens van Suwinet.<br>Onderzoek de AD/LDAP/SSO op het bestaan van groepsaccounts.<br>Onderzoek of de leverancier gebruik maakt van speciale beheer accounts. | | |
| **Relevante documenten** | | Autorisatiematrix (bestaan groepsaccounts), gebruikersoverzicht. | | |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 9 | Toegangsbeveiliging | | |
| **Paragraaf** | 9.2 | Beheer van toegangsrechten van gebruikers | | |
| **Control** | 9.2.2 | Gebruikers toegang verlenen | | |
| **Toelichting control** | | Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. | | |
| **Maatregel** | 9.2.2.1 | Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| x | x | x | x | x |
| | | | | |
| **Betrokken rollen** | | Verantwoordelijke voor Suwinet (lijnmanager), IT, leverancier | | |
| **Scope** | | Toegangsverlening Suwinet, gebruikersaccounts | | |
| **Nadere toelichting** | | Hangt samen met 6.1.1.1 en 9.2.1.1 | | |

| | |
|---|---|
| **Aandachtspunten** | Het gaat om het controleren van de administratie van toegangsverlening en of de lijnmanager inderdaad de toegang tot Suwinet autoriseert of laat autoriseren.<br>Het kan zijn dat de afdeling meeloopt in een organisatie-brede procedure. |
| **Testaanpak** | Interview de verantwoordelijke voor Suwinet en vraag hoe hij/zij binnen zijn afdeling omgaat met deze maatregel. |
| **Relevante documenten** | Vastgestelde autorisatiematrix, gebruikersoverzicht. |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 9 | Toegangsbeveiliging | | |
| **Paragraaf** | 9.2 | Beheer van toegangsrechten van gebruikers | | |
| **Control** | 9.2.2 | Gebruikers toegang verlenen | | |
| **Toelichting control** | | Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. | | |
| **Maatregel** | 9.2.2.2 | Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| x | x | x | x | x |
| | | | | |
| **Betrokken rollen** | | Verantwoordelijke voor Suwinet (lijnmanager) | | |
| **Scope** | | Toegangsverlening Suwinet, speciale Suwinet accounts (speciale bevoegdheden zijn het kunnen zoeken met andere zoeksleutels dan het BSN zoals bijv. op naam of kenteken).<br>Andere speciale accounts zijn: die van de gebruikersbeheerder, die kan accounts aanmaken en verwijderen en rollen maken. Die van de Security Officer of de gemandateerde, die kan specifieke rapportage opvragen (die is niet geanonimiseerd)). | | |
| **Nadere toelichting** | | Hangt samen met 6.1.1.1 en 9.2.1.1 | | |
| **Aandachtspunten** | | Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar mogelijk ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders).<br>Het kan zijn dat de afdeling meeloopt in een organisatie-brede procedure voor toegangsverlening.<br>Let op bij kleine gemeenten en afdelingen: de kans bestaat dat sommige controle taken niet goed gescheiden worden. | | |
| **Testaanpak** | | Interview de verantwoordelijke voor Suwinet en vraag hoe hij/zij binnen zijn afdeling omgaat met deze maatregel.<br>Onderzoek of er rollen binnen de Suwinet autorisatie zijn die eigenlijk niet samen kunnen gaan en waarom dat dit zo is. Zie ook: www.bkwi.nl voor het 'Overzicht autorisaties op Suwinet Inkijk voor GSD'.<br>Controleer of de lijnmanager voldoende waarborgen of mitigerende maatregelen genomen heeft om de risico's van het mogelijk samengaan van beheren functies en/of beschikken functies en/of controleren functies te beheersen (vier ogen principe, extra interne controle, controle via een andere afdeling). | | |

| | |
|---|---|
| **Relevante documenten** | Autorisatiematrix. |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 9 | Toegangsbeveiliging | | |
| **Paragraaf** | 9.2 | Beheer van toegangsrechten van gebruikers | | |
| **Control** | 9.2.5 | Beoordeling van toegangsrechten van gebruikers | | |
| **Toelichting control** | | Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen. | | |
| **Maatregel** | 9.2.5.3 | Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| x | x | x | x | x |
| | | | | |
| **Betrokken rollen** | | Verantwoordelijke voor Suwinet (lijnmanager) | | |
| **Scope** | | Toegangsverlening Suwinet, speciale Suwinet accounts (speciale bevoegdheden zijn het kunnen zoeken met andere zoeksleutels dan het BSN zoals bijv. op naam of kenteken.<br>Andere speciale accounts zijn: die van de gebruikersbeheerder, die kan accounts aanmaken en verwijderen en rollen maken. Die van de Security Officer of de gemandateerde, die kan specifieke rapportage opvragen (die is niet geanonimiseerd)). | | |
| **Nadere toelichting** | | Het Ministerie van SZW heeft in haar selectie voor verantwoording eveneens maatregel 9.2.5.1 opgenomen (BBN1). Maatregel 9.2.5.3 vergt een halfjaarlijkse controle. Hiermee wordt eveneens aan maatregel 9.2.5.1 (jaarlijkse controle) voldaan.<br>Hangt samen met 6.1.1.1 (inrichting) en 9.2.1.1 (procedure) | | |
| **Aandachtspunten** | | Geen | | |
| **Testaanpak** | | Controleer of de afdelingsmanager minimaal 1 keer per 6 maanden de toegangsrechten (laat) controleren. Dit moet blijken uit een rapportage van de controle aan of van de lijnmanager. | | |
| **Relevante documenten** | | Rapportage controle toegangsrechten. | | |

| | | |
|---|---|---|
| **Hoofdstuk** | 9 | Toegangsbeveiliging |
| **Paragraaf** | 9.2 | Beheer van toegangsrechten van gebruikers |
| **Control** | 9.2.6 | Toegangsrechten intrekken of aanpassen |
| **Toelichting control** | | De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast. |
| **Maatregel** | 9.2.6.1 | Deze control kent in de BIO geen maatregel.<br>NB: voor deze control is een aanvullende maatregel opgesteld in de ENSIA vragenlijst: |

| | | | | |
|---|---|---|---|---|
| | | 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. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| x | x | x | x | x |
| | | | | |
| **Betrokken rollen** | | Verantwoordelijke voor Suwinet (lijnmanager), HRM, IT | | |
| **Scope** | | Toegangsverlening Suwinet | | |
| **Nadere toelichting** | | Deze maatregel hangt samen met 6.1.1.1 en 9.2.1.1<br>Worden de toegangsrechten van gebruikers bij wijziging van functie aangepast?<br>Worden alle gebruikers van Suwinet gegevens altijd binnen een dag afgemeld uit het systeem als ze de toegang tot Suwinet gegevens niet meer nodig hebben?<br>Omdat de control geen verplichte overheidsmaatregelen kent, is er een zekere keuzevrijheid bij de organisatie over de exacte uitwerking van deze control in maatregelen. | | |
| **Aandachtspunten** | | Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders).<br>Het kan zijn dat de afdeling meeloopt in een organisatie-breed programma voor toegangsbeleid (HR en of IT).<br>Rechten dienen in tijd goed volgordelijk doorgevoerd te worden bij wijziging van functie om te voorkomen dat een te brede set aan rechten aan de gebruiker wordt toegekend. | | |
| **Testaanpak** | | Interview de verantwoordelijke voor Suwinet en vraag hoe hij binnen zijn afdeling omgaat met deze maatregel.<br>Onderzoek de organisatie of er een generieke procedure is voor het aan- en afmelden van gebruikers.<br>Laat een uitdraai maken van de huidige lijst van geautoriseerde gebruikers, controleer of deze gebruikers nog werkzaam zijn binnen het SUWI domein. Neem een willekeurige steekproef van 5 % van de gebruikers. | | |
| **Relevante documenten** | | Procedure in dienst, uit dienst en bij wijziging van functie, gebruikersoverzicht, autorisatiematrix. | | |

| | | |
|---|---|---|
| **Hoofdstuk** | 10 | Cryptografie |
| **Paragraaf** | 10.1 | Cryptografische beheersmaatregelen |
| **Control** | 10.1.1 | Gedocumenteerde bedieningsprocedures |
| **Toelichting control** | | Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen. |
| **Maatregel** | 10.1.1.1 | In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt:<br>(a) Wanneer cryptografie ingezet wordt.<br>(b) Wie verantwoordelijk is voor de implementatie.<br>(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.<br>(e) De wijze waarop het beschermingsniveau vastgesteld wordt.<br>(f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.<br>*www.forumstandaardisatie.nl | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| n.v.t. | x | x | x | x |
| | | | | |
| **Betrokken rollen** | IT-manager | | | |
| **Scope** | Cryptografie Suwinet inlezen en DKD inlezen | | | |
| **Nadere toelichting** | Cryptografie is een essentiële maatregel om de vertrouwelijkheid te waarborgen van Suwinet gegevens. Cryptografie wordt toegepast op vele vlakken: opslag, transport en daar waar het niet kan worden gegarandeerd dat de vertrouwelijkheid van de gegevens kan worden gewaarborgd.<br>Voor Suwinet inkijk geldt dat de webpagina die gehost wordt door BKWI al voorzien is van HTTPS, deze pagina is onder beheer van BKWI en is dus buiten scope.<br>In scope zijn de applicaties die Suwinet-inlezen of DKD inlezen gebruiken en het transport naar die applicaties. De maatregel richt zich op het bestaan van cryptografiebeleid. | | | |
| **Aandachtspunten** | Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar mogelijk ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders).<br>Het kan zijn dat de afdeling meeloopt in een organisatie-breed programma (HR en of IT), dit is ook goed. | | | |
| **Testaanpak** | Interview de verantwoordelijke voor Suwinet of zijn (IT) beveiligingsmanager en vraag hoe cryptografie wordt toegepast in het kader van Suwinet bij DKD-inlezen en Suwinet-inlezen.<br>Als gegevens verwerkt worden in de cloud of het bedrijfsproces is uitbesteed, is het ook van belang te onderzoeken hoe bij het transport van gegevens de vertrouwelijkheid van de gegevens gewaarborgd is.<br>Onderzoek de organisatie of er een cryptografiebeleid is dat voldoet aan de punten genoemd in de BIO. | | | |
| **Relevante documenten** | Cryptografiebeleid. | | | |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 12 | Beveiliging bedrijfsvoering | | |
| **Paragraaf** | 12.1 | Bedieningsprocedures en verantwoordelijkheden | | |
| **Control** | 12.1.1 | Gedocumenteerde bedieningsprocedures | | |
| **Toelichting control** | | Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben. | | |
| **Maatregel** | 12.1.1.1 | Deze control kent in de BIO geen maatregel<br>NB: voor deze control is een aanvullende maatregel opgesteld in de ENSIA vragenlijst:<br>Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| n.v.t. | x | x | x | x |
| | | | | |
| **Betrokken rollen** | | IT-manager, functioneel beheer, manager I&A. | | |
| **Scope** | | Beheer procedures | | |
| **Nadere toelichting** | | Bedieningsprocedures bestaan op alle gebieden, functioneel en technisch. Voor Suwinet geldt dat de organisatie niet zonder bedieningsprocedures kan, zo moet er voor alle handelingen waarbij Suwinet gebruikt wordt ook een bedieningshandleiding of werkinstructie aanwezig zijn. Idealiter worden deze gemaakt op basis van beleid, maar daar ligt hier niet de focus.<br>Gebruikersprocedures zijn bij deze control buiten scope: het gaat alleen om beheer. Alleen beheer procedures bij de IT-afdeling en eventueel bij functioneel beheer zijn in scope.<br>Omdat de control geen maatregelen kent is er een zekere keuzevrijheid bij de organisatie over de exacte uitwerking van deze control in maatregelen. | | |
| **Aandachtspunten** | | Dit is een kapstokartikel dat binnen 12.1 in diverse controls uitgewerkt is.<br>Focus specifiek op de IT-afdeling en functioneel beheer | | |
| **Testaanpak** | | Interview de verantwoordelijke voor IT/FB en vraag welke bedieningsprocedures aanwezig zijn voor het gebruik van Suwinet gegevens, dit kunnen zijn: functioneel beheer procedures.<br>Bijvoorbeeld: Installatie van systemen, Back-up, Restore, Monitoring, Afhandeling van fouten met betrekking tot Suwinet. | | |
| **Relevante documenten** | | Bedieningsprocedures voor beheer. | | |

| | | |
|---|---|---|
| **Hoofdstuk** | 12 | Beveiliging bedrijfsvoering |
| **Paragraaf** | 12.4 | Verslaglegging en monitoren |
| **Control** | 12.4.1 | Gebeurtenissen registreren |
| **Toelichting control** | | Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld. |
| **Maatregel** | 12.4.1.1 | Een logregel bevat minimaal:<br>(a) de gebeurtenis; |

| | | | | |
|---|---|---|---|---|
| | | (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon;<br>(c) het gebruikte apparaat;<br>(d) het resultaat van de handeling;<br>(e) een datum en tijdstip van de gebeurtenis. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| n.v.t. | x | x | x | x |
| | | | | |
| **Betrokken rollen** | | IT manager | | |
| **Scope** | | Logging | | |
| **Nadere toelichting** | | Dit is een kapstokartikel, deze control is de inleiding op de andere controls van 12.4<br>Logging is essentieel voor het vastleggen van gebruikers en systeembeheer handelingen, maar ook voor het vastleggen uitzonderingen, gebeurtenissen en alles wat maar relevant kan zijn voor een gecontroleerde werking van het systeem en dat achteraf kunnen aantonen. | | |
| **Aandachtspunten** | | Controleer ook logging met betrekking van de toegang van gebruikers tot Suwinet gegevens. Dit zal veelal binnen applicaties geregeld zijn, let op mogelijke overlap met 18.1.4<br>De logging op de servers van BKWI voor Suwinet inkijk is niet in scope.<br>Accountgegevens van medewerkers die de logging controleren dienen altijd persoonsgebonden te zijn. | | |
| **Testaanpak** | | Interview het hoofd IT en vraag hoe logging geregeld is binnen de organisatie, hoe het wordt opgeslagen, welke gebeurtenissen worden vastgelegd en hoe de logregel opgebouwd is.<br>Onderzoek de logging van Suwinet-inlezen of DKD-inlezen (servers en applicaties). | | |
| **Relevante documenten** | | Logbeleid, autorisatiematrix, logbestanden. | | |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 12 | Beveiliging bedrijfsvoering | | |
| **Paragraaf** | 12.4 | Verslaglegging en monitoren | | |
| **Control** | 12.4.2 | Beschermen van informatie in logbestanden | | |
| **Toelichting control** | | Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang. | | |
| **Maatregel** | 12.4.2.2 | 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. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| n.v.t. | x | x | x | x |

| | |
|---|---|
| **Betrokken rollen** | IT manager |
| **Scope** | Logging |
| **Nadere toelichting** | Logging is essentieel voor het vastleggen van gebruikers en systeembeheer handelingen, maar ook voor het vastleggen uitzonderingen, gebeurtenissen en alles wat maar relevant kan zijn voor een gecontroleerde werking van het systeem en dat achteraf kunnen aantonen. |
| **Aandachtspunten** | Focus specifiek op de IT-afdeling<br>Controleer ook logging met betrekking van de toegang van gebruikers tot Suwinet gegevens. |
| **Testaanpak** | Interview het hoofd IT en vraag hoe lang logging wordt bewaard en hoe het wordt bewaard.<br>Onderzoek alleen de logging van Suwinet-inlezen of DKD-inlezen (servers en applicaties en eventuele message broker).<br>Onderzoek of de logging adequaat wordt beschermd tegen ongewenste manipulatie.<br>De logging op de servers van BKWI voor Suwinet inkijk zijn niet in scope. |
| **Relevante documenten** | Logbeleid. |

| | | | | |
|---|---|---|---|---|
| **Hoofdstuk** | 18 | Naleving | | |
| **Paragraaf** | 18.1 | Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen. | | |
| **Control** | 18.1.4 | Privacy en bescherming van persoonsgegevens | | |
| **Toelichting control** | | Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met de relevante wet- en regelgeving. | | |
| **Maatregel** | 18.1.4.2 | 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. | | |
| **Maatregel geldt voor:** | | | **Norm van toepassing op:** | |
| Suwinet Inkijk | Suwinet Inlezen | DKD Inlezen | Eigen organisatie | Service organisatie |
| x | x | x | x | n.v.t. |

| | |
|---|---|
| **Betrokken rollen** | Verantwoordelijke voor Suwinet (lijnmanager), Security Officer, gemandateerde, intern controleur, privacyfunctionaris Suwinet, |
| **Scope** | Privacy controle, inlezen en inkijk |
| **Nadere toelichting** | Het is essentieel om het gebruik van persoonsgegevens te monitoren, te loggen en regelmatig te beoordelen. Het betreft systemen waarbinnen Suwinet gegevens verwerkt worden... |
| **Aandachtspunten** | Focus op applicatie specifieke logging, zoals die van Suwinet inkijk, maar let vooral op de (zaak)systemen achter Suwinet en DKD inlezen.<br>Controleer of deze logging regelmatig beoordeeld wordt op het rechtmatig verwerken van persoonsgegevens. Zie hiervoor de handreiking van VNG |

| | |
|---|---|
| | Realisatie. Indien nog niet voldoende privacy logging aanwezig is, vraag dan aan de organisatie op welke termijn maatregelen genomen worden in (zaak)systemen. |
| **Testaanpak** | Interview de Suwinet verantwoordelijke lijnmanager en de privacy functionaris Suwinet op het bestaan van logging en de controle daarop<br>Is het privacy-beleid vastgesteld?<br>Onderzoek de procedures voor controle van de applicatie logging. |
| **Relevante documenten** | Het gaat natuurlijk om meer dan alleen logging: een goed uitgangspunt is de controle of de organisatie beschikt over een actueel en vastgesteld privacybeleid.<br>In het kader van naleving: controle generieke gebruikersrapportage en mogelijk opgevraagde specifieke rapportages bij BKWI. Zie ook de 'Handreiking Gebruikersrapportage Suwinet-Inkijk' op www.vngrealisatie.nl. |