INFORMATIE
BEVEILIGINGS
DIENST

Factsheet

Assurance

Omgaan met verantwoording vanuit leveranciers over informatiebeveiliging en privacy.

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Factsheet assurance

Versienummer
1.0

Versiedatum
07-01-2018

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie:

Versie	Door	Wijziging / Actie
1.0	IBD	Eerste versie

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Doel

Het doel van dit document is lezers meer inzicht te geven in de verschillende vormen van assurance, waardoor ze zich beter een mening kunnen vormen over welke certificering/ verklaring het beste past bij een af te nemen dienst. Daarnaast is het doel lezers te helpen bij het kunnen inschatten of een afgegeven certificaat/ verklaring past bij het risico van de afgenomen dienst.

Doelgroep

Dit document is van belang voor het management van de gemeente, informatiebeveiligingsmedewerkers, de systeemeigenaren, applicatiebeheerders, inkopers/ contractmanagers en de ICT-afdeling.

Relatie met overige producten

- De factsheet inkopen SAAS dienst
- De inkoopvoorwaarden beveiliging
- De handreiking contractmanagement
- De model verwerkersovereenkomst
- GIBIT

Inhoudsopgave

1 Inleiding

Gemeenten maken voor het uitvoeren van hun processen en hun IT voorzieningen veelvuldig gebruik van externe leveranciers en brengen taken onder in samenwerkingsverbanden (gemeenschappelijke regelingen). Deze leveranciers en gemeenschappelijke regelingen verwerken vaak (privacy) gevoelige gegevens. De beveiliging van de IT voorzieningen en de processen moet voldoen aan de normen uit de Baseline Informatiebeveilinging Nederlandse Gemeenten (BIG). De vraag is hoe een gemeente kan toezien op de naleving van beveiligingsvoorschriften bij ketenpartners en leveranciers. Gemeenten hebben er behoefte aan dat leveranciers en gemeenschappelijke regelingen over hun diensten verantwoording afleggen, de gemeente moet zich immers ook weer verantwoorden richting de gemeenteraad.

Verantwoording door leveranciers en ketenpartners kan bijvoorbeeld plaatsvinden via het uitvoeren van een right to audit, een in control verklaring, een assuranceverklaring of een certificering. Dit document richt zich op assuranceverklaringen en certificeringen die relevant zijn vanuit de optiek van informatiebeveiliging en privacy. Daarbij wordt ingegaan op de specifieke kenmerken en aandachtspunten die daarbij komen kijken.

Assurance betekent: mate van betrouwbaarheid; zekerheid; vertrouwensniveau; verzekering; zekerstelling. In relatie tot dienstverlening van een leverancier zegt het iets over de betrouwbaarheid van een product of van bepaalde processen die worden uitgevoerd.
In de praktijk komen we assuranceverklaringen tegen en certificaten. Een assuranceverklaring is een rapport van een onafhankelijke externe auditor, die een betrouwbaarheidsoordeel over de cijfers of processen van een leverancier of haar diensten geeft. Een certificaat is verklaring van een externe auditor dat de betreffende partij een kwaliteitsmanagementsysteem rond een onderwerp als informatiebeveiliging of continuïteit heeft.

In het geval van het verwerken van persoonsgegevens horen de gemeente en de leverancier afspraken vast te leggen over informatiebeveiliging en privacy. Hiervoor heeft de IBD een model verwerkersovereenkomst en een factsheet[1] opgesteld. Ook als er geen sprake is van privacygevoelige gegevens kan er behoefte zijn om afspraken vast te leggen over informatiebeveiliging of beschikbaarheid.
Aangezien het in de praktijk het vaak lastig blijkt om goed te monitoren of een leverancier aan de eisen ten aanzien van informatiebeveiliging en privacy voldoet kan een assuranceverklaring of certificering hier een rol in spelen. Aangezien gemeenten de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) gebruiken als norm voor informatiebeveiliging zal in dit document van de verschillende assuranceverklaringen en certificaten aangegeven worden hoe zij zich tot de BIG verhouden.

Doelen document

Het doel van deze factsheet is lezers meer inzicht te geven in de verschillende vormen van assurance, waardoor ze zelf beter een mening vormen over welke certificering/ verklaring het beste past bij een af te nemen dienst. Daarnaast is het doel lezers te helpen bij het kunnen inschatten of een afgegeven certificaat/ verklaring past bij het risico van de afgenomen dienst.

Kaders

Algemene verordening gegevensbescherming (AVG)
Art 32 van de AVG gaat over de verplichting om passende technische en organisatorische maatregelen te treffen om de beveiliging van persoonsgegevens te waarborgen. Deze eis geldt voor verwerkingsverantwoordelijken[2] en verwerkers[3], dus zowel voor gemeenten als leveranciers. Daar waar gemeenten verwerkingsverantwoordelijke zijn hebben zij de uiteindelijke verantwoordelijkheid dat passende beveiligingsmaatregelen getroffen zijn. De afweging wat passende beveiligingsmaatregelen zijn vindt plaats op basis van beschikbare technologie, de uitvoeringskosten en het risico van de verwerking. Daarnaast is deze afweging ook afhankelijk van de organisatie, de aard van de

1 Zie ook: https://www.informatiebeveiligingsdienst.nl/?s=verwerkersovereenkomst
2 https://www.informatiebeveiligingsdienst.nl/faq/wanneer-ben-ik-een-verwerkersverantwoordelijke/
3 https://www.informatiebeveiligingsdienst.nl/faq/wanneer-ben-ik-een-verwerker/

persoonsgegevens en de omvang van de verwerking. Uit Artikel 32 van de AVG volgt dat gemeenten afspraken maken over de mate van beveiliging bij de leverancier en afspraken over de manier waarop de leverancier daar periodiek over rapporteert. Deze afspraken worden doorgaans opgenomen in een verwerkersovereenkomst.

IBD model voor een verwerkersovereenkomst

Artikel 7 van het IBD model voor een verwerkersovereenkomst[4], bevat de eisen ten aanzien van verantwoording over informatiebeveiliging bij de verwerking. Bijlage 1 en 4 geven nadere specificaties over de specifieke beveiligingseisen waaraan de leverancier moet voldoen.

Baseline Informatiebeveiliging Nederlandse Gemeenten

Alle Nederlandse gemeenten moeten voldoen aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Deze baseline is afgeleid van de ISO27001/2 standaard. In de BIG staan eisen hoe gemeenten met informatiebeveiliging en dienstverlening vanuit derden om moeten gaan.

Hoofdstuk 10.2.1 van de BIG gaat over verantwoordelijkheid voor informatiebeveiliging en goedkeuring bij uitbesteding:
Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.

1. *De uitbestedende partij blijft verantwoordelijk voor de betrouwbaarheid van uitbestede diensten.*
2. *Uitbesteding is goedgekeurd door de voor het informatiesysteem verantwoordelijke lijnmanager.*

Hoofdstuk 10.2.2 gaat over de controle en beoordeling van dienstverlening door een derde partij:
De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.

1. *Er worden afspraken gemaakt over de inhoud van rapportages, zoals over het melden van incidenten en autorisatiebeheer.*
2. *De in dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld middels audits of rapportages en gebeurt minimaal eens per jaar (voor ieder systeem).*
3. *Er zijn voor beide partijen eenduidige aanspreekpunten.*

ENSIA

Vanuit ENSIA (Eenduidige Normatiek Single Information Audit) vindt horizontale verantwoording plaats door het college van B&W richting de raad over de mate waarin de gemeente voldoet aan de BIG. Om hier betrouwbaar over te kunnen rapporteren zullen gemeenten ook een beeld moeten hebben over het niveau van beveiliging bij de leveranciers en gemeenschappelijke regelingen waar zij gebruik van maken. Op basis van risico van de uitbestede dienst en haar eigen informatiebehoefte bepaalt de gemeente welke zekerheid nodig is en wat voor assurance of certificaat hier het beste bij past.

Gemeenschappelijke regelingen

Ook bij gemeenschappelijke regelingen is het uitgangspunt dat gemeenten verantwoordelijk blijven voor het aantoonbaar voldoen aan de BIG (c.q. de beveiligingsafspraken) van de bij de gemeenschappelijke regeling ondergebrachte activiteiten en dat zij hierover afspraken maken en zich laten informeren over het voldoen aan deze afspraken. Afhankelijk van het type gemeenschappelijke regeling zullen deze afspraken op hun eigen wijze moeten worden geborgd[5].

4 https://www.informatiebeveiligingsdienst.nl/?s=verwerkersovereenkomst
5 zie hiervoor de notitie Verantwoordingsstelsel ENSIA definitief en het document https://vng.nl/files/vng/publicaties/2015/20150731_informatieveiligheid-en-intergemeentelijke.pdf

2 Toelichting assurance

2.1 Doel van assurance

Een assuranceverklaring of certificaat kan het toezien vergemakkelijken op afspraken met derden over onderwerpen zoals informatiebeveiliging of privacy. Afhankelijk van de afstand en de invloed die een gemeente heeft op een derde en de afgenomen dienstverlening kan een gemeente kiezen welke soort zekerheid gewenst is om sluitend te kunnen verantwoorden. Met een assuranceverklaring of certificaat wordt op een eenduidige manier verantwoording worden afgelegd. Als een assuranceverklaring of certificaat goed aansluit op de behoeften van de afnemer scheelt dit zowel de afnemer als de leverancier tijd en kosten.

2.2 Assurance i.p.v. van right to audit?

Het krijgen van een assuranceverklaring is geen vervanging voor het recht om audits uit te voeren bij een leverancier. Dus ook als er afspraken zijn gemaakt over het krijgen van een assuranceverklaring, dienen er in de (verwerkers)overeenkomst afspraken gemaakt te worden over het recht om audits uit te voeren. Een assuranceverklaring kan er wel toe leiden dat er minder behoefte is om een audit uit te laten voeren omdat uit de assuranceverklaring voldoende vertrouwen kan worden geput dat het in de hand is.

2.3 Belangrijkste verschillen tussen een assuranceverklaring en een certificering

- Scope en diepgang:
  Bij een certificaat ligt de nadruk op het toetsen of het managementsysteem functioneert. Bij een assurancerapportage ligt de focus op de uitkomsten van individuele normen/ maatregelen.
- Inhoud:
  Een assuranceverklaring is een redelijk uitgebreid document met daarin o.a. uitleg over het normenkader, de manier waarop getoetst is en eventuele bevindingen die geconstateerd zijn. Een certificaat is een stuk beperkter qua inhoud (meestal 1 a 2 pagina's) en vertelt globaal de scope van het certificaat en de norm waartegen getoetst is.
- Eisen voor afgifte:
  Een assuranceverklaring wordt afgegeven ongeacht of er afwijkingen zijn geconstateerd.
  Een certificaat wordt alleen afgegeven als de organisatie aan de eisen voor certificaat voldoet.
- Doelgroep en verspreiding:
  Certificaten en assuranceverklaringen verschillen qua doelgroep en verspreidingskring. Een certificaat bevat algemene informatie over de scope en de norm en is gericht op meerdere doelgroepen zoals (potentiële)klanten, ketenpartners en andere belanghebbenden. Daardoor zal een certificaat ruimer gedeeld worden ten opzichte van een assuranceverklaring. Een assuranceverklaring is vooral gericht op klanten en is gevoeliger qua inhoud. Dit betekent dat een assuranceverklaring in de regel alleen gedeeld wordt met klanten die hier specifieke afspraken over hebben.
- Geldigheid:
  Een assuranceverklaring zegt alleen iets over een periode in het verleden en is alleen geldig over die periode. Het geeft dus geen zekerheid over de toekomst. Een certificaat is gericht op het in control zijn rond informatiebeveiliging en is 3 jaar geldig vanaf de periode van afgifte. Een certificaat geeft dus ook enige zekerheid richting de toekomst.
- Audit tijd en kosten:
  Voor een initiële certificeringsaudit is significant minder tijd nodig (gemiddeld ongeveer 25%) dan voor een initiële assuranceverklaring. Voor tussentijdse certificeringsaudits is de benodigde tijd nog veel minder (gemiddeld ongeveer 10%) ten opzichte van een assuranceverklaring. Dit vertaalt zich ook terug in de kosten, waarbij een assurance verklaring meestal significant duurder is dan een certificering.

2.4 Algemene aandachtspunten bij assurance

Er zijn een aantal standaard aandachtspunten die voor alle typen assuranceverklaringen en certificaten gelden:

- Ten eerste de scope van de verklaring. Sluit deze aan op de dienst die afgenomen wordt? Als men bijvoorbeeld een SAAS dienst afneemt is een assuranceverklaring die enkel over de hosting gaat niet voldoende.
- Welke norm wordt gehanteerd?
- Welke controls van welke norm zijn in scope van de verklaring? Zijn die door te vertalen naar de BIG? En worden alle BIG maatregelen geraakt die je op basis van het risico van de dienst zou verwachten?
- De bevoegdheid en kwalificaties van de auditor die de audit uitvoert. Afhankelijk van benodigde expertise moet in Nederland een assuranceverklaring worden afgegeven door een Register EDP (RE) auditor of een Register Accountant (RA).
- De positie van de auditor. In veel gevallen wordt een assuranceverklaring afgegeven door een externe auditor, dit kan echter ook een interne auditor zijn. Alhoewel de assuranceverklaring aan dezelfde kwaliteitseisen moet voldoen, kiest men vaak voor een externe auditor omdat deze een schijnbaar grotere onafhankelijkheid heeft.

2.5 De manier van toetsing bij een assuranceverklaring

In alle gevallen zal de verklaring door een onafhankelijke auditor afgegeven worden. De manier van toetsen van controls kan echter verschillen. In de meeste gevallen wordt er getoetst op opzet en bestaan of op opzet, bestaan en werking.

Opzet

Betekent dat de auditor kijkt of een control beschreven is en eventueel of deze het risico (op papier) goed afdekt.

Bestaan

Dit houdt in dat een auditor gaat kijken of de controls daadwerkelijk uitgevoerd worden zoals beschreven. Belangrijk om te weten is dat het hierbij om een momentopname gaat. Bij het toetsen op bestaan wordt ook de opzet meegenomen

Werking

Als er getoetst wordt op werking wordt er ook gekeken of de control over een bepaalde periode gefunctioneerd heeft. Meestal gebeurt dit op basis van samples waarbij over bijvoorbeeld een heel jaar gekeken wordt of de control gefunctioneerd heeft. Bij het toetsen op werking worden de opzet en bestaan ook mee getest. Toetsen op de werking geeft de meeste zekerheid maar kost ook het meeste tijd.

Volwassenheidsmodel

Het is ook mogelijk dat de auditor de controlemaatregelen toetst tegen een volwassenheidsmodel. Een veel gebruikt volwassenheidsmodel is het CoBIT-raamwerk. Dit bestaat uit de volwassenheidsniveau's 0 t/m 5. Bij volwassenheidsniveau 0 is er geen enkele control aanwezig en bij niveau 5 is er een continue verbetercyclus ingericht rond die betreffende control. Globaal komt volwassenheidsniveau 3 overeen met de aantoonbaarheid van de opzet en bestaan van een control en vanaf niveau 4 is de werking over een bepaalde periode ook aantoonbaar.

3 Verschillende typen assurance en certificaten

Een assuranceverklaring is een rapport van een onafhankelijke onafhankelijke auditor, die een betrouwbaarheidsoordeel over de cijfers of processen van een leverancier of haar diensten geeft. Een certificaat is verklaring van een externe auditor dat de betreffende partij een kwaliteitsmanagementsysteem rond een onderwerp als informatiebeveiliging of continuïteit heeft. In dit hoofdstuk worden de meest gangbare assuranceverklaringen en certificaten behandeld. Dit zijn:

- ISAE3402 (SOC1)
- ISO27001
- ISO22301
- NEN7510
- DigiD (indien niet op naam van een gemeente)
- ISAE3000
- SOC2 of 3

Als term komt ook regelmatig TPM (Third Party Memorandum of Third Party Mededeling) voor. Dit is een audit verklaring van een onafhankelijke auditor. In de praktijk vallen hier de ISAE3402, ISAE3000 en SOC2 en 3 onder.

3.1 ISAE3402

ISAE3402 of SOC1 staat voor Assurance Reports on Controls at a Service Organization. Voorheen werd dit ook een SAS70 verklaring genoemd. Een ISAE3402 verklaring bevat een oordeel van een onafhankelijke auditor over de inrichting van internal controls. De focus ligt hierbij op verantwoording ten behoeve van financiële verslaglegging. Daarnaast bevat het ook een verklaring van het management over de mate waarin zij in control is.

Er zijn twee typen ISAE3402 verklaringen:

- De zogenaamd type I verklaring betreft een snapshot op een gegeven moment. De auditor heeft dus alleen de opzet en het bestaan van een control getoetst.
- De type II verklaring geeft assurance over een bepaalde periode (6mnd/ 1 jaar). De opzet, het bestaan en werking van controls zijn dus getoetst.

De reden dat soms gekozen wordt voor een type 1 verklaring is dat de audit werkzaamheden minder omvangrijk zijn. Hierdoor zijn de kosten ook lager. De type II verklaring geeft echter weer meer zekerheid.

3.1.1 Toepasbaarheid

De scope van de verklaring is gericht op controls die van direct materieel belang zijn voor de financiële verantwoording. De ISAE3402 is dus vooral bruikbaar als men zekerheid wil over de juistheid en betrouwbaarheid van een uitbesteed proces, zoals bijvoorbeeld de salarisadministratie van een gemeente. Een ISAE3402 verklaring bevat standaard een aantal IT General Controls (ITGC's). Dit vormt echter maar klein onderdeel van de verklaring en de bruikbaarheid vanuit het oogpunt van security is hiervan beperkt.

Typische IT General Controls zijn:

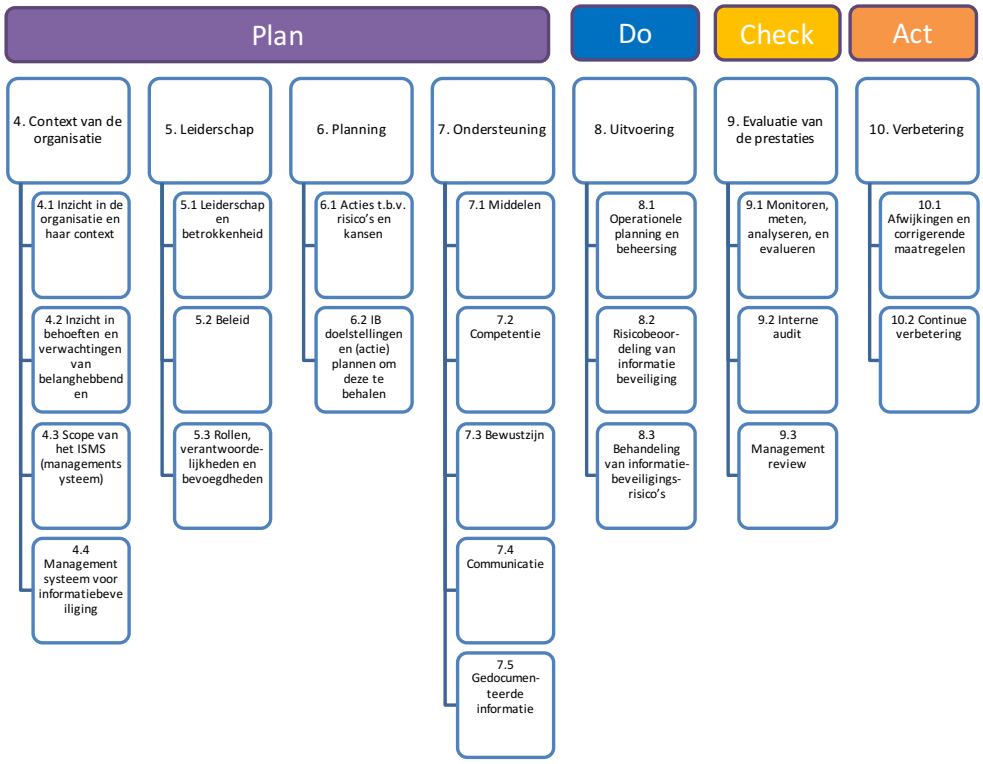
- Changemanagement
- Autorisatiemanagement
- Availability en continuity management

3.1.2 Specifieke aandachtspunten:

- Bij een type II verklaring wordt soms niet over het gehele jaar gerapporteerd, maar bijvoorbeeld over de periode januari t/m oktober. Dit is omdat in die twee laatste maanden de auditor bezig is met de audit. Om te voorkomen dat er een soort gat ontstaat waarover geen zekerheid gegeven wordt, geeft het management dan vaak een zogenaamde bridging letter af. In deze bridging letter verklaart het management dat er in de periode die buiten de ISAE3402 verklaring valt zich geen materiele afwijkingen hebben voorgedaan.
- Er is een landelijk ISAE register (www.isae3402.nl). Dit is een niet verplicht register waarop bedrijven zich kunnen inschrijven en klanten kunnen inzien welke leveranciers een ISAE3402 verklaring hebben.
- Een ISAE3402 verklaring mag alleen afgegeven worden door een register auditor (RE) of -accountant (RA)

3.2 ISO27001

Het ISO27001 certificaat is een door een certificeerde instelling afgegeven kwaliteitskeurmerk over de kwaliteit van het managen van informatiebeveiliging. Hiervoor wordt de werking van het Information Security Management System (ISMS) getoetst. Het ISMS bestaat uit een serie van activiteiten rond de beheersing van informatiebeveiliging en heeft als doel het continue verbeteren van de effectiviteit van informatiebeveiliging door een procesmatige aanpak. Onderstaande afbeelding geeft een overzicht van de hoofdstukken uit de ISO27001 norm en de activiteiten die het ISMS vormen. De activiteiten uit deze hoofdstukken vormen samen de stappen Plan, Do, Check en Act (kwaliteitscirkel van Deming). Vergeleken met een ISAE3402 geeft een ISO27001 certificaat weinig detail over de inhoud van de werkzaamheden. Toch zit er een hele wereld aan activiteiten achter, die nodig zijn om aan de certificeringseisen te voldoen. Er wordt onder andere ieder jaar intern en extern geaudit, riskassessments uitgevoerd en gemonitord op de Annex A controls en gestuurd op continue verbetering. Een belangrijk onderdeel van de certificering is ook de betrokkenheid vanuit het management. De verplichte management review houdt ook in dat de directie zich een oordeel moet vormen over de effectiviteit van haar informatiebeveiligingsbeleid en kansen ter verbetering.



Naast de hoofdstukken die het ISMS vormen bevat de ISO27001 norm een Annex A. Deze Annex A bevat 114 controls die best practices vormen op het gebied van informatiebeveiliging. De ISO27001 norm stelt het hebben van een ISMS verplicht en geeft duidelijk aan welke eisen hiervoor gelden. De controls uit de Annex A zijn daar tegenover niet verplicht. Wel moet de gecertificeerde instantie aangeven welke controls in scope zijn, wat de rechtvaardiging voor het in scope nemen is, of ze zijn geïmplementeerd en de rechtvaardiging om controls van bijlage A uit te sluiten. De gecertificeerde instantie dient dit aan te geven in een Verklaring van Toepasselijkheid (VVT)[6]. De ISO27002 norm bevat een leidraad voor de implementatie van de Annex A controls. Implementatie conform de ISO27002 is niet verplicht voor het behalen van een ISO27001 certificaat. Het is ook niet mogelijk om je op de ISO27002 norm te laten certificeren. Eventueel is het wel mogelijk om een ISAE3000 verklaring te hebben op basis van de ISO27002 norm (Zie uitleg bij ISAE3000).

[6] De Engelse benaming voor VVT wordt ook vaak gebruikt: Statement of Applicability (SOA).

3.2.1 Bruikbaarheid vanuit Informatiebeveiligings- en privacy perspectief

De ISO27001 norm is specifiek geschreven vanuit het oogpunt van informatiebeveiliging. De BIG is van deze norm afgeleid en daardoor goed te matchen. Een ISO27001 certificaat sluit daarom ook goed aan op de informatiebeveiligingseisen uit de verwerkersovereenkomst. Vanuit privacy optiek is ISO27001 is vooral bruikbaar ten aanzien van de verplichting dat verantwoordelijken en verwerkers passende beveiligingsmaatregelen moeten nemen (art. 32 AVG). De concepten privacy by design en default zijn echter niet specifiek onderdeel van de Annex A. Het kan dus zijn dat vanuit privacy optiek in bepaalde gevallen aanvullende beveiligingsmaatregelen genomen moeten worden aanvullend op de Annex A.

3.2.2 Specifieke aandachtspunten:

- Versie van de norm: Periodiek wordt de norm geactualiseerd. De huidige versie is in 2013 vastgesteld. De versie van de norm waartegen gecertificeerd is hoort op het certificaat te staan (momenteel ISO27001:2013). Alle instanties die eerst volgens de vorige versie van de norm (27001:2005) gecertificeerd waren, hebben uiterlijk in 2015 moeten her-certificeren. Certificaten die tegen de ISO27001:2005 norm zijn afgegeven zijn niet meer geldig[7].
- Transparantie: Het certificaat is niet transparant over de status van afzonderlijke beveiligingsmaatregelen en eventuele bevindingen ten aanzien van het ISMS. Na de initiële certificering vindt jaarlijks vindt een externe onderhoudsaudit plaats en moeten interne audits en monitoring plaatsvinden. De resultaten van deze audits worden niet standaard gedeeld. Een certificaat kan wel binnen de geldigheidsperiode worden ingetrokken als zware afwijkingen ten aanzien van het ISMS niet tijdig worden opgelost.
- Scope: op het certificaat staat een scope waarover het certificaat is uitgegeven. Uiteraard moet deze passen bij de dienst die bij de betreffende leverancier wordt afgenomen.
- VVT: de verklaring van toepasselijkheid bevat een overzicht van de controls die in scope genomen zijn. Deze VVT moet passen bij de dienst die wordt afgenomen en de risico's die daarbij gemoeid zijn. Voor controls uit de Annex A die niet in van toepassing verklaard zijn moet in de VVT een duidelijke argumentatie opgenomen zijn. Officieel is een leverancier niet verplicht om de VVT te tonen. Dit is echter wel gebruikelijk, aangezien de VVT meer inzicht geeft over reikwijdte van het certificaat.
- Geldigheid en authenticiteit: Een ISO27001 certificaat wordt voor 3 jaar afgegeven. De geldigheidsdatums staan op het certificaat. Daarnaast bevat het certificaat een certificaatnummer en de naam van de certificeringsinstantie. De geldigheid van het certificaat is aan de hand van het certificaatnummer en de naam van het betreffende bedrijf is op de site van de certificerende instantie de geldigheid te controleren
- Accreditatie certificeringsinstantie: op de site[8] van de Raad van Accreditatie (RVA) is na te gaan of een certificeringsinstantie bevoegd is een bepaalde certificering af te geven. De auditor moet daarnaast een speciaal gecertificeerde lead auditor zijn.
- Er zijn concrete voorbeelden waarbij certificaten zijn uitgegeven door niet geaccrediteerde partijen. Vaak heeft een certificaat dan niet de vereiste scope, nummering en logo's van de accreditatie. Een dergelijk certificaat geeft niet dezelfde zekerheid als die van een geaccrediteerde instantie.

3.3 ISO22301

De ISO22301 standaard bevat een managementsysteem voor Business Continuity (BCMS). Met een werkend BCMS heeft een bedrijf de processen en systemen ingericht naar de gewenste continuïteit en beschikbaarheid. Net als de ISO27001 behelst de ISO22301 een risico gebaseerde aanpak. Dat betekent dat bepaald wordt wat de beschikbaarheids- en continuïteitseisen zijn en dat de processen en systemen hierop aangepast worden. Een belangrijk onderdeel is het hebben van een Business Continuity Plan (BCP) waarin verschillende scenario's beschreven staan om met een grote verstoring om te gaan. Dit plan dient periodiek getest te worden.

[7] De BIG is nog gebaseerd op de ISO27001:2005 norm. Een nieuwe uitgave van de BIG op basis van de 2013 versie is onderhanden.
[8] https://www.rva.nl/geaccrediteerde-organisaties

3.3.1 Bruikbaarheid vanuit informatiebeveiligings- en privacy perspectief

Continuïteit en beschikbaarheid zijn zowel vanuit informatiebeveiliging en privacy relevant. Continuïteit is een onderdeel van de BIG (hoofdstuk 14.1) evenals beschikbaarheid (in de vorm van back-up procedures, hoofdstuk 10.5). Onder de Wbp en AVG wordt het verlies van data door een beschikbaarheidsincident ook als een datalek gezien. Omdat de scope van de ISO22301 beperkt is, zal je vanuit informatiebeveiligings- en privacyperspectief vaak nog wel aanvullende assurance of certificering willen hebben om ook de andere aspecten af te dekken.

3.3.2 Specifieke aandachtspunten:

- Het certificaat garandeert geen 100% beschikbaarheid en continuïteit. Het is dus altijd belangrijk om de houder van het certificaat te vragen naar welke garanties zij geven over beschikbaarheid en continuïteit.
- Binnen Business Continuity Management (BCM) zijn de termen RPO en RTO belangrijk:
    - RPO staat voor Recovery Point Objective. Dit is een maat voor de periode waarin data verloren mag gaan. Aangezien back-ups meestal op gezette tijden gemaakt worden betekent dit dat de data die in de periode na de laatste back-up toegevoegd of gewijzigd is, verloren kan gaan als er zich een incident met de opslag van data voordoet. De RPO moet dus overeenkomen met de eisen die de gemeente aan de beschikbaarheid van data stelt.
    - RTO staat voor Recovery Time Objective. Dat is de tijd die een dienst maximaal uit de lucht mag zijn. Ook deze moet passen bij de eisen vanuit de gemeenten. In sommige gevallen is er een work around mogelijk die de continuïteit van de dienstverlening waarborgt.

3.4 NEN7510

Het NEN7510 certificaat is een specifieke invulling van de ISO27001 norm voor de zorg. Op bepaalde punten is deze echter explicieter/ strenger dan ISO27001 norm (meer rule based dan risk based). De ISO27001 norm geeft bij de implementatie van de beheersmaatregelen uit de Annex A redelijk veel vrijheid van interpretatie hoe dit moet gebeuren. In de NEN7510 zijn beheersmaatregelen explicieter omschreven en aangepast naar het risiconiveau dat hoort bij het werken met gevoelige persoonsgegevens (o.a. medische gegevens).

3.4.1 Bruikbaarheid vanuit informatiebeveiligings- en privacy perspectief

De bruikbaarheid van de NEN 7510 voor assurance vanuit de verwerkersovereenkomst is vergelijkbaar met de ISO27001 norm. Net als de ISO27001 norm is de NEN7510 specifiek geschreven vanuit het oogpunt van informatiebeveiliging. Aangezien de NEN7510 te zien is als een soort zusje van de BIG zijn beide goed te matchen.

3.4.2 Specifieke aandachtspunten:

- Er is maar een beperkt aantal certificerende instanties (CI's) dat daadwerkelijk geaccrediteerd is door de RVA om op de NEN7510 norm te mogen certificeren.
- Er zijn ook NEN7510 certificaten in omloop die door niet geaccrediteerde CI's uitgegeven zijn. Officieel heten deze dan niet certificaat maar wordt door de auditor een soort TPM[9] afgegeven op basis van de NEN7510 norm of een ISO27001 certificaat i.c.m. een verklaring dat de invulling van de Annex A heeft plaatsgevonden op basis van de beheersmaatregelen uit NEN7510 norm.
- In 2017 is een nieuwe versie van de NEN7510 gepubliceerd. Deze nieuwe versie is aangepast naar de structuur zoals die bij de ISO27001 gehanteerd wordt. Ten opzichte van de oude versie is de NEN7510 opgesplitst in een deel dat de zogenaamde highlevel structure bevat (vergelijkbaar met ISO27001) en een deel waarin de beheersmaatregelen uit de Annex A verder staan toegelicht (vergelijkbaar met ISO27002). Daarbij is zijn de beheermaatregelen ook minder dwingend omschreven waardoor meer ruimte ontstaat voor risico inschatting.

3.4 DigiD audit

De DigiD audit is een verplichting die vanuit Logius gesteld wordt voor instanties die in hun systemen gebruik maken van DigiD. De scope van de audit blijft beperkt tot de websites, systeemkoppelingen of infrastructuur die gebruik maken van DigiD en richt zich op een aantal beheerprocessen en technische beveiligingsmaatregelen. De audit bestaat uit een penetratietest en een audit op de beheersmaatregelen uit het normenkader.

[9] TPM op basis van de ISAE3000 norm

Voor gemeenten geldt een nuancering op bovenstaande. Nieuwe DigiD aansluitingen op naam van de gemeente vallen binnen bovenstaande DigiD audit. Bestaande DigiD aansluitingen worden via ENSIA (Eenduidig Normatiek Single Information Audit) verantwoord naar Logius. Hiertoe voert de gemeente een zelfevaluatie uit (toetst zelf de normen), geeft over de resultaten van de zelfevaluatie een collegeverklaring af, waarna een geregistreerde EDP-auditor assurance op de collegeverklaring afgeeft. Voor deze aansluitingen geldt sinds verantwoordingsjaar 2017 geen DigiD audit meer: het auditobject is verschoven naar de Collegeverklaring waarover assurance wordt gegeven. Dit is een jaarlijks terugkerend verantwoordingsproces.

3.4.1 Bruikbaarheid vanuit informatiebeveiligings- en privacy perspectief

Vanuit de eisen uit de model verwerkersovereenkomst is een DigiD audit slechts beperkt bruikbaar. Dit komt door de beperkte scope die de DigiD audit heeft. De DigiD audit kan echter wel een specifieke eis zijn als de leverancier voor de gemeente een DigiD dienst ondersteunt. Afhankelijk van het risico zullen dus ook andere afspraken m.b.t. informatiebeveiligings- en privacymaatregelen en assurance gemaakt moeten worden.

3.4.2 Specifieke aandachtspunten:

- De audit moet altijd worden uitgevoerd door een Register EDP-auditor (RE).

3.5 ISAE3000

ISAE3000 is een “open” standaard voor het geven van een assuranceverklaring over niet financiële informatie. De norm waartegen getoetst wordt is zelf te kiezen (bijv Cobit5 of ISO27001/2). De ISAE3000 wordt ook wel SOC 1 genoemd.

3.5.1 Bruikbaarheid vanuit informatiebeveiligings- en privacy perspectief

De mate van bruikbaarheid voor de verwerkersovereenkomst is afhankelijk van de scope van de audit en de gekozen beheersmaatregelen.

3.5.2 Specifieke aandachtspunten:

- Een ISAE3400 verklaring mag alleen afgegeven worden door een Register EDP (RE) auditor of een Registeraccountant (RA).
- Net als bij de ISAE3402 zijn er twee typen:
  Type I : snapshot op een gegeven moment
  Type II: assurance over een bepaalde periode (6mnd/ 1 jaar)
  Bij een ISAE3000 verklaring geldt ook hetzelfde aandachtspunt als voor ISAE3402 m.b.t. de periode waarover verklaard wordt.
- Omdat de norm waartegen getoetst wordt zelf gekozen kan worden is het belangrijk om na te gaan of deze scope van de verklaring en de controlemaatregelen passen bij de afgenomen dienst.
- Het wil in sommige gevallen voorkomen dat er op een andere manier gerapporteerd wordt over de controlemaatregelen in scope, bijvoorbeeld over volwassenheid van controls i.p.v. over opzet en bestaan of opzet, bestaan en werking.

3.6 SOC2 en SOC3

De SOC 2 en 3 verklaringen zijn een specifieke invulling van ISAE3000. Hierbij is de scope van de assuranceverklaring gericht op de infrastructuur, software, procedures, mensen en data die nodig zijn voor het leveren van een bepaalde dienst. Er wordt getoetst op zogenaamde Trust Service Principles: Security, Beschikbaarheid, Vertrouwelijkheid, Integriteit van verwerking en Privacy. Daarnaast bevat het rapport een verklaring van het management over de mate waarin zij in controls is.

3.6.1 Verschil SOC 2 en SOC 3

Zowel SOC 2 als SOC 3 geven assurance over een bepaalde periode (bijv. 6 maanden of 1 jaar). SOC2 geeft daarbij inzicht in de resultaten van het testen op bestaan en werking. Bij SOC3 wordt alleen assurance gegeven over een bepaalde periode (6mnd/ 1 jaar) zonder inhoudelijke testresultaten.

3.6.2 Bruikbaarheid vanuit informatiebeveiligings- en privacy perspectief

SOC 2 en 3 zijn goed bruikbaar voor het geven van assurance ten behoeve van de verwerkersovereenkomst. Wel moet er goed opgelet worden of de scope van de audit en de gekozen beheersmaatregelen goed passen bij de afgenomen dienst. Privacy is één van de Trust Service Principles binnen SOC 2 en 3. Hiervoor geldt echter ook dat dit onderdeel optioneel is en er dus altijd gekeken moet worden of het in scope is. Daarnaast is er niet een standaard lijst van maatregelen ter ondersteuning van de trust principles en moeten deze nader bepaald worden. Dit betekent dat je als afnemer van een dienst altijd moet kijken naar de scope van de maatregelen en welke zekerheden deze bieden.

3.6.3 Specifieke aandachtspunten:

- Een SOC 2 of 3 verklaring mag alleen afgegeven worden door een Register EDP (RE) auditor of een Registeraccountant (RA).
- Zowel SOC 2 als 3 geven assurance over een bepaalde periode (6mnd/ 1 jaar). Bij een SOC 3 wordt echter geen detailinformatie gegeven over de werking van controls, enkel een overal audit opinie.

4 Samenvatting

Onderstaande tabel geeft een globale vergelijking van de verschillende assurance vormen en certificaten weer.

	scope	diepgang van controle	mgt systeem	Risico gebaseerd vs control gericht	rapportage	geldig in de toekomst	kan steunen op interne audits	kosten
BIG	informatiebeveiliging bij gemeenten	nvt	beperkt	control	nvt	nvt	nvt	nvt
ISAE3402 Type I	financiele verslaglegging	opzet en bestaan van controles (momentopname)	beperkt	control	assurance verklaring	nee	ja mits interne aditor voldoet aan eisen	gemiddeld
ISAE3402 Type II	financiele verslaglegging	opzet, bestaan en werking van controles over een gedefinieerde periode	beperkt	control	assurance verklaring	nee	ja mits interne aditor voldoet aan eisen	hoog
ISAE3000/ SOC 1 Type I of II	zelf te bepalen	type I opzet en bestaan en type II opzet, bestaan en werking over periode	nee	control	assurance verklaring	nee	ja mits interne aditor voldoet aan eisen	hoog
SOC 2	verslaglegging over de infrastructuur, software, procedures, mensen en data die nodig zijn voor het leveren van een bepaalde dienst	opzet, bestaan en werking van controles over een gedefinieerde periode	nee	control	assurance verklaring	nee	ja mits interne aditor voldoet aan eisen	hoog
SOC 3	verslaglegging over de infrastructuur, software, procedures, mensen en data die nodig zijn voor het leveren van een bepaalde dienst	opzet, bestaan en werking van controles over een gedefinieerde periode	nee	control	assurance verklaring zonder inhoudelijke uitleg over bevindingen	nee	ja mits interne aditor voldoet aan eisen	hoog
ISO27001	certificering van het managen van informatie beveiling	opzet, bestaan en werking van het management systeem rond informatie beveiliging. Werkig van de onderligende controles (Annex A) wordt minder expliciet meegenomen.	ja	risico	certificaat	ja	ja	laag
ISO22301	certificering van het managen van Business Continuity	opzet, bestaan en werking van het management systeem rond business Continuity. Werkig van de business continuity plan wordt minder expliciet meegenomen.	ja	risico	certificaat	ja	ja	laag
NEN7510	certificering van het managen van informatie beveiling gericht op de zorg	opzet, bestaan en werking van het management systeem rond informatie beveiliging. Werkig van de onderligende controles (Annex A) wordt minder expliciet meegenomen.	ja	risico	certificaat	ja	ja	laag
DigiD	verklaring tbv het gebruik maken van DigiD op websites	pentest icm toetsing van opzet en bestaan van een beperkte set controlemaatregelen	nee	control	rapportage	ja	nee	laag

5 Conclusie

Over het algemeen kan zowel middels een ISO27001 certificaat als via een ISAE3000-, SOC2- of SOC 3-verklaring verantwoording gegeven worden over de afspraken die in de verwerkersovereenkomst zijn gemaakt ten aanzien van informatiebeveiliging. Afhankelijk van de zekerheid die men wil hebben en de kosten die men wil maken, kan gekozen worden voor een ISO27001 certificaat of een ISAE3000 of SOC 2/ 3. Een SOC 2 verklaring geeft in het algemeen meer zekerheid over de werking van controls en de ISO27001 over het managementsysteem van informatiebeveiliging. Een ISO27001 certificaat is meestal voor de leverancier de goedkoopste oplossing.

De concepten privacy by design en default worden echter niet standaard door een van deze assurancevormen afgedekt. Het kan dus soms nodig zijn dat vanuit privacy optiek aanvullende maatregelen genomen moeten worden aanvullend op de Annex A of de controlemaatregelen voor de ISAE3000 en SOC 2 en 3.

Begrippenlijst

Begrip	uitleg
Assurance	Het geven van een bepaalde zekerheid over de dienstverlening van een leverancier middels een verklaring of certificaat. Het zegt het iets over de betrouwbaarheid van een product of van bepaalde processen die worden uitgevoerd.
Beheersmaatregel	Detailbeschrijving onder een control overeenkomend met het niveau van implementatierichtlijn in de ISO27002 standaard. NB in de BIG worden iets afwijkende definities gehanteerd ten opzichte van de ISO27002. In de BIG wordt onderscheid gemaakt tussen controls en beheersmaatregelen. Beheersmaatregelen zijn een verdere verdieping van een control. In de ISO27001 wordt hier de term implementatierichtlijn voor gebruikt.
Control	Generieke beschrijving van een maatregel. In de ISO27001 en 2 wordt dit een beheersmaatregel genoemd.
Cobit	Control Objectives for Information and Related Technologies is een framework voor IT management en governance. Cobit bevat een uitgebreide set controls op het gebied van informatiebeveiliging.
In control statement	Een verklaring van de verantwoordelijken over de beheersing van bepaalde processen. Bij gemeenten moet het college van B&W een control statement afgeven over de BIG als onderdeel van de gebruikelijke Planning en Control cyclus. De in control statement geeft inzicht aan welke BIG normen wordt voldaan en voor welke BIG normen een explain is gedefinieerd. Een dergelijke verklaring kan ook door een leverancier of een gemeenschappelijke regeling worden afgegeven.
ICV	In Control Verklaring. Zie In Control statement.
ITGC	IT General Control. Dit zijn IT beheer procedures die vaak een onderdeel zijn van een ISAE3402 verklaring. De meest voorkomende ITGC's zijn wijzigingen beheer, autorisatiemanagement, continuïteitsmanagement en beschikbaarheid.
Kwaliteitscirkel van Demming	De cirkel van Demming beschrijft vier activiteiten (Plan, Do, Check en Act) die op verbeteren van organisaties en processen van toepassing zijn. Het cyclische karakter garandeert dat de kwaliteitsverbetering continu onder de aandacht is.
Norm	Standaard set aan controls en doelstellingen waaraan een dienst of organisatie moet voldoen.
Right to audit	Betreft het echt om audit te laten uitvoeren bij een leverancier. Het is gebruikelijk dat deze audit door een onafhankelijke (externe) auditor wordt uitgevoerd. Het recht op audit betreft één of meerdere aspecten van de afgenomen dienstverlening. In het kader van dit document wordt hier als scope informatiebeveiliging en privacy bedoeld. Het right to audit wordt meestal contractueel vastgelegd. Op basis van artikel 28 h van de AVG heeft een leverancier de verplichting om mee te werken aan audits
TPM	Third Party Mededeling (of Memorandum). Hiermee wordt een assuranceverklaring bedoeld van een onafhankelijke auditor. TPM is geen officiële standaard. In de praktijk wordt er vaak een ISAE3000 of ISEA3402 mee bedoeld.

Kijk voor meer informatie op: www.informatiebeveiligingsdienst.nl

Nassaulaan 12
2514 JS Den Haag
CERT: 070 373 80 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl

VNG Realisatie