INFORMATIE
BEVEILIGINGS
DIENST

INFORMATION SECURITY MANAGEMENT SYSTEM

Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Information Security Management System

Versienummer
1.0.1

Versiedatum
Augustus 2016

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	Datum	Opmerkingen
1	December 2014	
1.0.1	Augustus 2016	Taskforce BID verwijderd, WBP vervangen door Wbp, GBA vervangen door BRP

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Voorwoord

De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. Aanleiding voor de oprichting van de IBD vormen enerzijds de leerpunten uit een aantal grote incidenten op informatiebeveiligingsvlak en anderzijds de visie Digitale Overheid 2017.
De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen.

De IBD heeft drie doelen:

1. Het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.
2. Het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
3. Het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen. De ondersteuning die de IBD biedt bij het ICT-Beveiligingsassessment DigiD is een voorbeeld van een dergelijk project.

Hoe realiseert de IBD haar doelen?
Om invulling te kunnen geven aan haar doelen is door de IBD op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) een vertaalslag gemaakt naar een baseline voor de gemeentelijke markt. Deze Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) betreft twee varianten, een Strategische- én een Tactische Baseline. Beide varianten van de BIG zijn beschikbaar voor alle gemeenten op de community van de IBD, zodat door iedere gemeente tot invoering van de BIG kan worden overgegaan. Bestuur en management hebben met deze baseline een instrument in handen waarmee zij in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging. Om de invoering van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD producten ontwikkeld op operationeel niveau. Dit heeft een productenportfolio opgeleverd, genaamd de Operationele Baseline Nederlandse Gemeenten. Onderhavig product is onderdeel van het productenportfolio.
Naast een productenportfolio, heeft de IBD voor gemeenten ook een dienstenportfolio ontwikkeld. Voor een volledig overzicht van het producten- en dienstenportfolio, kunt u terecht op de website van de IBD.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: BRP, SUWI, BAG, PUN en Wbp, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is in de naleving van dat kader voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Leeswijzer

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

Doel
Het doel van dit document is een handreiking te geven om een Information Security Management System (ISMS) te implementeren en te onderhouden.

Doelgroep
Dit document is van belang voor het management van de gemeente, de Chief Information Security Officer (CISO) of informatiebeveiligingsfunctionaris (IBF), de systeemeigenaren, applicatiebeheerders en de ICT-afdeling.

Relatie met overige producten
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - Strategische variant van de Baseline Informatiebeveiliging voor Gemeenten
  - Tactische variant van de Baseline Informatiebeveiliging voor Gemeenten
- Informatiebeveiligingsbeleid van de gemeente

Maatregelen strategische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
Hoofdstuk 2.5
Hoofdstuk 2.6

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Paragraaf 5.1.1	Beleidsdocumenten voor informatiebeveiliging
Hoofdstuk 6	De organisatie van informatiebeveiliging
Paragraaf 13.2.2	Leren van informatiebeveiligingsincidenten
Paragraaf 15.2	Naleving beveiligingsbeleid en normen en technische naleving

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Inhoudsopgave

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

1 Inleiding

Deze handleiding over het Information Security Management System (ISMS) van een gemeente beschrijft wat er nodig is om een ISMS te implementeren en te beheersen op basis van de Strategische en Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Het ISMS is de motor van de informatiebeveiligingsactiviteiten die een gemeente kan ondernemen. Het ISMS moet effectief zijn over de langere termijn en dient onderhouden te worden volgens de verbetercyclus zoals de Plan-Do-Check-Act (PDCA)-cyclus. Deze sluit idealiter aan bij de Planning- en Control (P&C)-cyclus van de gemeente. Het bestuurlijk en organisatorisch borgen van informatieveiligheid door aansluiten bij de bestaande P&C-cyclus is een van de punten in de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' en de toelichting hierop, zoals deze is aangenomen op de Buitengewone Algemene Ledenvergadering van de Vereniging van Nederlandse Gemeenten (VNG) van 29 november 2013. Het is aan te bevelen de borging van informatiebeveiliging vorm te geven door de invoering van een ISMS.

Het doel van het ISMS is onder andere het continue beoordelen van welke beveiligingsmaatregelen passend zijn en deze indien nodig bij te stellen. Het ISMS is een proces dat de basis legt voor passende beveiligingsmaatregelen voor de gemeente over de langere termijn. Het ISMS wordt uitgevoerd door de (virtuele) informatiebeveiligingsorganisatie met verschillende activiteiten in de PDCA-cyclus van het ISMS.

Om het ISMS als proces effectief te laten zijn dient de gemeente dat proces actief te ondersteunen. Dit houdt in dat taken en verantwoordelijkheden gekoppeld dienen te worden aan personen om zo die (virtuele) beveiligingsorganisatie vorm te geven. In de BIG wordt al gesproken over de Chief Information Security Officer (CISO) of Informatiebeveiligingsfunctionaris (IBF), waar ook een functieprofiel voor beschikbaar is gesteld door de IBD. Daarnaast hebben ook andere personen een rol. De rol van CISO/IBF is bij voorkeur buiten de ICT-afdeling belegd. Deze CISO heeft een belangrijk rol binnen het ISMS. Een grote gemeente is in staat om het ISMS vorm te geven met verschillende functionarissen op alle niveaus en binnen meerdere afdelingen. Een kleine gemeente heeft hier waarschijnlijk minder (specialistische / gespecialiseerde) personen voor beschikbaar. Samenwerking op dit vlak is voor kleinere gemeenten een realistisch optie. De inrichting van een ISMS is dus organisatie afhankelijk, waarbij een bepaalde set van taken en verantwoordelijkheden die minimaal nodig is voor het onderhouden van een ISMS noodzakelijk is.

1.1 Doelstellingen ISMS

Een ISMS helpt gemeenten om de beveiligingsdoelstellingen te ondersteunen. Bijvoorbeeld door:

- Het faciliteren van bedrijfscontinuïteit.
- Het verbeteren van de manier hoe op informatiebeveiligingsincidenten wordt gereageerd.
- Het omgaan met verantwoording en rapportage.
- Het reduceren van kosten die nodig zijn om beveiligingsmaatregelen te implementeren.
- Het bijdragen aan een juiste beveiliging van middelen van de gemeente.
- Het bijdragen aan verbeterde interne controle over beveiliging.

1.2 Structuur

De indeling van dit document is als volgt:
Hoofdstuk 2 : ISMS algemene uitleg
Hoofdstuk 3 : Het implementeren van een ISMS
Hoofdstuk 4 : ISMS-beheersing
Hoofdstuk 5 : Verwijzing naar ISMS-beleid in het voorbeeld Gemeentelijke Informatie beveiligingsbeleid

1.3 Aanwijzing voor gebruik

Deze handleiding is qua opzet geschreven om de maatregelen met betrekking tot het ISMS van de gemeente uit te werken en daarbij handreikingen te geven voor de invoering en de beheersing van het ISMS. De gemeentelijke beleidsregels met betrekking tot het ISMS staan beschreven in de Strategische en Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

2 ISMS

Een ISMS is ondersteunend aan de doelstelling om informatieveiligheid over een langere periode op een steeds hoger niveau uit te voeren. Het hebben van een ISMS is geen eenmalige activiteit cq. project. Het is een voortdurend proces dat binnen de gemeente uitgevoerd wordt.
Vaak ligt bij een ISMS de nadruk op de documentatie en administratie en wordt voor de administratie naar een tool gegrepen. Een deel van de documentatie is echter maar noodzakelijk om de doelstelling met betrekking tot informatieveiligheid te ondersteunen, de rest van de documentatie is vooral bedoeld om belanghebbenden de gelegenheid te geven controles uit te voeren. De focus dient vooral te liggen op de eerste set aan documentatie. Uiteraard kan een tool wel bijdragen aan de effectiviteit van een ISMS.

Binnen de Strategische Baseline is hiervoor de basis gelegd die ontleend is aan de ISO/IEC 27001:2005. Dit heeft geleid tot de volgende beleidsuitgangspunten die in het voorbeeld Informatiebeveiligingsbeleid van de IBD zijn uitgewerkt en die ook door gemeenten zo wordt gebruikt. Daarnaast staan er in de Tactische Baseline maatregelen die behoren bij het uitvoeren van het ISMS-proces.

Maatregelen uit het voorbeeld Informatiebeveiligingsbeleid, Hoofdstuk 2, verantwoordelijkheden:
Het college van Burgemeester en Wethouders (college van B&W) is integraal verantwoordelijk voor de beveiliging (beslissende rol) van informatie binnen de werkprocessen van de gemeente.[1]

- Zij stelt kaders voor informatiebeveiliging (IB) op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders.

De Directie (in sturende rol) is verantwoordelijk voor kaderstelling en sturing. De Directie:[2]

- Stuurt op concern risico's.
- Controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden.
- Evalueert periodiek beleidskaders en stelt deze waar nodig bij.

De afdelingen binnen de gemeente (in vragende rol) zijn verantwoordelijk voor de integrale beveiliging van hun organisatieonderdelen.[3] De (cluster)directie/lijnmanagement/proceseigenaar:

- Stelt op basis van een expliciete risicoafweging, betrouwbaarheidseisen voor zijn informatiesystemen vast (classificatie).
- Is verantwoordelijk voor de keuze, de invoering en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen.
- Stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn).
- Rapporteert over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de managementrapportages.

De gemeentelijke Service Organisatie of gelijkwaardig (ICT, HR, bedrijfsvoering, et cetera, in uitvoerende rol) is verantwoordelijk voor de uitvoering.[4]

[1] Zie ook: Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
[2] Met betrekking tot de i-functie geeft de CIO op dagelijkse basis namens de directie invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan.
[3] Zie ook: Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
[4] Let op, de service organisatie, stafdienst, afdeling bedrijfsvoering is tegelijk ook klant, het gaat hier echter om de uitvoerende rol.

De gemeentelijke service organisatie:

- Is verantwoordelijk voor beveiliging van de informatievoorziening en invoering van beveiligingsmaatregelen, die voortvloeien uit betrouwbaarheidseisen (classificaties).
- Is verantwoordelijk voor alle beheeraspecten van informatiebeveiliging, zoals ICT security management, incident- en problem management, facilitaire en personele zaken.
- Verzorgt logging, monitoring en rapportage.
- Levert intergemeentelijke klanten (technisch) beveiligingsadvies.

2.1 Waarom een ISMS

Het hoofddoel van een ISMS is het verbeteren van de effectiviteit van informatiebeveiliging door een procesmatige aanpak, die wordt ondersteund door het management van de gemeente. Beveiliging krijgt een duidelijke rol in de verticale sturingskolom van een gemeente. Dit door de eerder genoemde uitgangspunten op te nemen in het informatiebeveiligingsbeleid van de gemeente, te koppelen aan de P&C-cyclus van de gemeente en hierover door de organisatieonderdelen verantwoording af te laten leggen door reguliere voortgangsrapportages. Een dergelijke cyclus is veelal vastgelegd in de gemeentelijke begrotingssystematiek. Aansluiting hierbij voorkomt dat informatiebeveiliging als een eigenstandig onderwerp wordt behandeld en daardoor laag geprioriteerd wordt. Over het functioneren van de informatiebeveiliging, wordt conform de P&C-cyclus binnen de gemeente en richting het college van B&W verantwoording afgelegd door het management.
Voor het effectueren van informatiebeveiliging wordt binnen het ISMS gewerkt via een verbetercyclus, zoals de PDCA-cyclus. Zoals eerder aangegeven kan dit het beste aansluiten bij de P&C-cyclus van de gemeente. Na het vaststellen van wat nodig is, worden maatregelen getroffen en vervolgens wordt gecontroleerd of die maatregelen het gewenste effect sorteren (controle). Maatregelen kunnen in de tijd gezien veranderen (omdat bedreigingen en risico's ook veranderen). Dus de controle kan aanleiding geven tot bijsturing in de maatregelen. Daarnaast kan het totaalpakket van eisen, maatregelen en controle aan een herijking toe zijn (evaluatie). Het goed doorlopen van de stappen kan op elk moment zorgen voor een passend beveiligingsniveau.

PLAN

In de PLAN-fase wordt het ISMS ontworpen en wordt het gemeentelijk informatiebeveiligingsbeleid vastgesteld. In het voorbeeld Informatiebeveiligingsbeleid van de IBD zijn alle (noodzakelijke) elementen voor het ISMS beschreven. Indien er wordt gekozen om in het gemeentelijk beveiligingsbeleid geen elementen op te nemen voor de verankering van het ISMS, is het raadzaam om hier een apart ISMS-beleid voor op te stellen en te laten vaststellen.

DO

In de DO-fase wordt uitvoering gegeven aan het informatiebeveiligingsbeleid. Voor wat betreft de toets tegen de BIG, wordt de 0-meting en de impactanalyse uitgevoerd. Als resultaat wordt er een informatiebeveiligingsplan op- en vastgesteld door het management. Hier worden de stappen beschreven om concrete maatregelen in te voeren binnen de gemeente. Wie het informatiebeveiligingsplan dient vast te stellen hangt af van welk mandaat de CISO heeft gekregen.

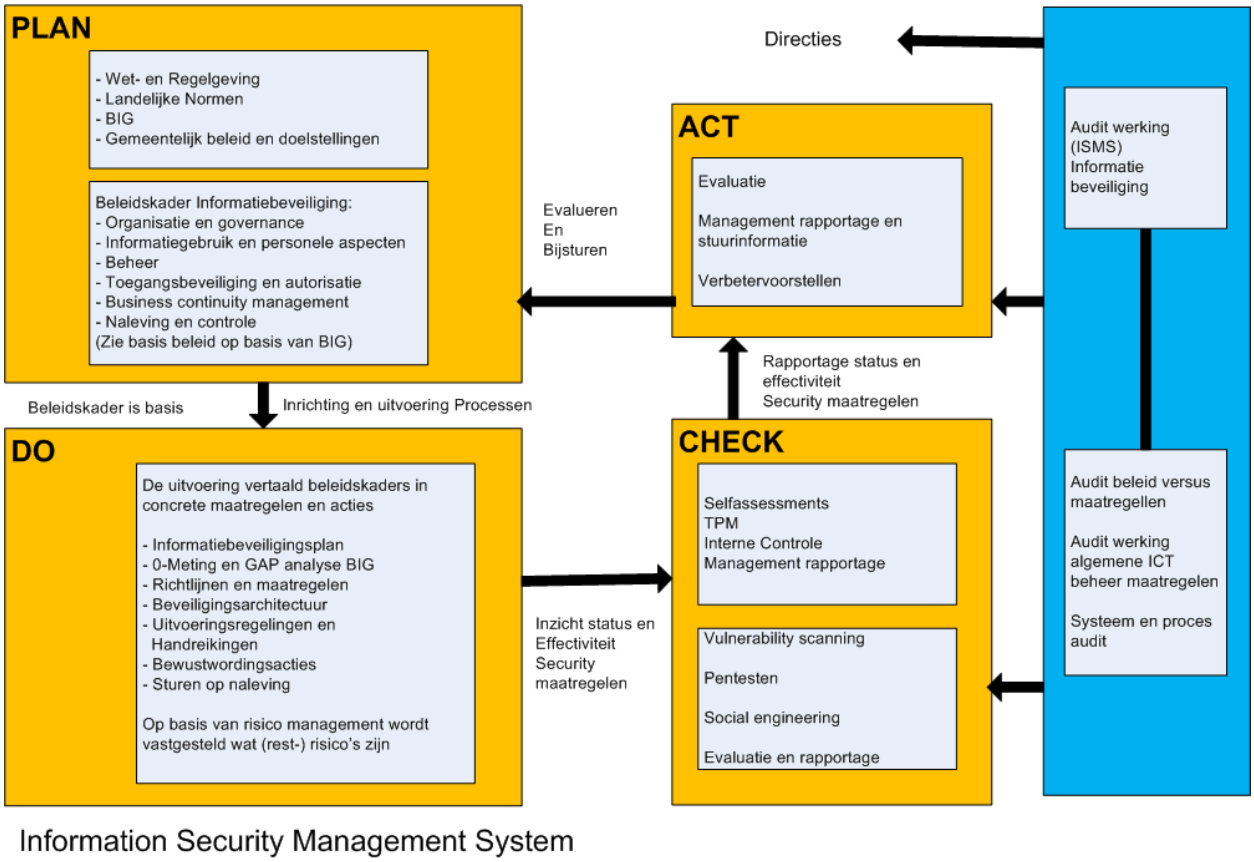
CHECK

In de CHECK-fase wordt de effectiviteit en efficiency van het ISMS beoordeeld door middel van zelfassessments, interne controle, audits en bijvoorbeeld management rapportages.

ACT

In de ACT-fase wordt geëvalueerd en bijgesteld op basis van de informatie uit de CHECK-fase.

2.2 ISMS-bereik



Figuur 1, Afbeelding uit voorbeeld Informatiebeveiligingsbeleid

Het blikveld van het ISMS binnen de gemeente omvat de bedrijfsvoeringsprocessen, de onderliggende informatiesystemen en het informatiegebruik bij de gemeente in de meest brede zin van het woord. Het ISMS heeft ook betrekking op de informatie die daarbinnen verwerkt wordt. De plaats waar informatiesystemen fysiek draaien is niet van invloed.[5]

[5] Denk aan SaaS, uitbesteding van taken et cetera.

3 Het implementeren van een ISMS

Om te beginnen met het invoeren van een ISMS moet de gemeente een aantal stappen zetten. Het beste is om de invoering van een ISMS projectmatig aan te pakken, en als het ISMS is ingevoerd wordt verder het als proces uitgevoerd. Onderstaand is een voorbeeld van stappen die doorlopen kunnen worden:

ISMS-stappenplan

Stap 1 - Vaststellen doelstellingen ISMS
Het vaststellen van doelstellingen voor het ISMS en het bepalen van prioriteiten is essentieel voor de steun van het management van de gemeente. Voor gemeenten kunnen de volgende doelstellingen van toepassing zijn:

- Verzekering aan ketenpartners met betrekking tot de status van de organisatie op het gebied van informatiebeveiliging van de gemeente.
- Verzekering aan burgers en ketenpartners over de toewijding van de gemeente tot informatiebeveiliging, privacy en informatieveiligheid.
- Hoger vertrouwen door het toepassen van de BIG voor de beveiliging voor de vertrouwelijke gegevens van de burger.
- Identificatie van bedrijfsinformatie en effectieve risicobeoordeling.
- Bescherming van de reputatie van de gemeente.
- Naleving van de BIG. Maar ook naleving van normen zoals BRP, PUN, BAG en SUWI.
- Creëren van draagkracht voor informatieveiligheid binnen de gemeente.

Stap 2—Verkrijgen van steun van het management van de gemeente
Het management van de gemeente moet achter de invoering van het ISMS staan. Hiertoe behoort het management ervoor te zorgen dat de benodigde middelen beschikbaar zijn om aan het ISMS te werken. Tevens dienen alle gemeentelijke medewerkers die te maken hebben met het ISMS te beschikken over het juiste kennisniveau en de vereiste competenties. De volgende activiteiten/initiatieven duiden op steun van het gemeentelijk management:

- Een gemeentelijk informatiebeveiligingsbeleid met daarin de opmerking dat een ISMS wordt ingericht en onderhouden, welke resources worden toegewezen en hoe verantwoording over naleving wordt ingericht.[6]
- Het hebben van een informatiebeveiligingsplan op basis van de BIG-impactanalyse.
- Er zijn conform de BIG, functies en verantwoordelijkheden vastgesteld voor informatiebeveiliging.
- Communicatie binnen de gemeente over het belang van informatieveiligheid.
- Er zijn voldoende middelen voor het ISMS beschikbaar.
- Het jaarlijks beoordelen van het ISMS.

Stap 3—Vaststellen scope van de ISMS-invoering
De Strategische Baseline bepaalt dat de invoering van het ISMS uitgevoerd dient te worden voor de gehele gemeente, zie paragraaf 2.4 van de Strategische Baseline. Het ISMS geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en het karakter van de informatie.
De volgende punten kunnen worden overwogen:

[6] Zie voorbeeld Informatiebeveiligingsbeleid Gemeenten van de IBD

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

- Welke locaties, bedrijfsmiddelen (ook data) en technologieën van de gemeente worden beheerst door het ISMS?
- Wordt van toeleveranciers en afnemers verlangd dat ze zich houden aan het ISMS en de overige regels van de gemeente?[7]
- Gekeken moet worden welke wet- en regelgeving en normen van toepassing zijn op het ISMS. Voor gemeenten is dit de BIG en tevens kan gekeken worden naar het document met opsomming van wet- en regelgeving.[8]

Stap 4—Het definiëren van een methode voor risicobeoordeling.
In principe dient de gemeente te voldoen aan de maatregelen van de Tactische Baseline, waarbij ruimte is voor een afweging op basis van 'pas toe of leg uit'. De Tactische Baseline is zo opgebouwd dat er, zonder de voor het basisniveau getroffen maatregelen aan te tasten, een verdieping bovenop gebouwd kan worden, om te voldoen aan hogere of specialistische eisen. Specialistische maatregelen voor afwijkende situaties of hogere beveiligingsniveaus dan het basisniveau, zijn *niet* in de Strategische Baseline opgenomen. Voor dit soort bijzondere omstandigheden moet teruggegrepen worden naar een gerichte risicoafweging. De middelen hiervoor zijn

- De baselinetoets BIG, om vast te stellen of een informatiesysteem door de maatregelen in de BIG voldoende beschermd wordt. De baselinetoets BIG doet een uitspraak over de impactniveaus voor vertrouwelijkheid, integriteit, beschikbaarheid en tevens de privacy.
- Als er meer maatregelen nodig zijn: het hanteren van een vaste risicobeoordelingsaanpak, de diepgaande risicoanalyse. Deze risicoanalyseaanpak geeft ruimte voor het vaststellen van welke risico's onaanvaardbaar zijn en daarom moeten worden beperkt. Als de diepgaande risicoanalyse goed wordt uitgevoerd is de uitkomst de maatregelen die nodig zijn bovenop de BIG.
- De Privacy Impact Assessment (PIA).
- Het overblijvende risico dient beheerd te worden door middel van zorgvuldig opgestelde bedrijfsregels, procedures en controlemechanismen.

Het kiezen van een standaard risicobeoordelingsmethode voor alle gemeenten is een van de belangrijkste onderdelen van het opzetten van het ISMS. Daarnaast kan de volgende documentatie hierbij van pas komen:

- Het document voor classificering van bedrijfsmiddelen en gegevens[9].

Door de producten die geleverd worden door de IBD voor de operationele baseline, waaronder de baselinetoets BIG, de diepgaande risicoanalyse, de GAP- en impactanalyse is voor de gemeenten aan dit punt voldaan, indien deze producten als uitgangspunt gekozen worden.

Stap 5—Uitvoeren GAP- en impactanalyse
De gemeente dient inzicht te hebben in de te beschermen bedrijfsinformatiesystemen en hun status ten opzichte van de Tactische Baseline. Door het uitvoeren van de GAP- en impactanalyse wordt inzicht verkregen in ontbrekende maatregelen, gemeente breed of per informatiesysteem. De impactanalyse geeft daarnaast input aan het op te stellen informatiebeveiligingsplan.

[7] Denk hier het melden van incidenten, volgen van aanwijzigingen en herziening van beveiligingseisen van de gemeente naar de leverancier.
[8] https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/20101126_Conceptlijst-aanvullende-inhoud-Informatiebeveiliging-v040.pdf
[9] https://community.ibdgemeenten.nl/wp-content/uploads/2014/06/13-1018-handreiking-dataclassificatie-1.0.docx

De GAP- en impactanalyse bieden de ruimte om, mits goed toegepast, gestructureerd, bewust en objectief, informatiebeveiligingsmaatregelen te kiezen voor de behandeling van de risico's. Of de ruimte om maatregelen niet te kiezen en daarmee risico's te aanvaarden. Dit moet dan wel expliciet worden gemaakt. Deze keuzes dienen door het management te worden gemaakt, waarbij de CISO een adviserende rol heeft.

Stap 6—Opstellen informatiebeveiligingsplan

Indien bekend is welke maatregelen uit de impactanalyse en een eventuele aanvullende diepgaande risicoanalyse nog niet zijn geïmplementeerd, dienen deze maatregelen in een informatiebeveiligingsplan te worden opgenomen. In dit plan worden aan maatregelen actiehouders toegewezen welke verantwoordelijk zijn voor de invoering van de maatregelen. De benodigde middelen dienen tijdig in de P&C-cyclus te worden meegenomen, om de vereiste maatregelen om risico's af te dekken ook het jaar erop in te kunnen voeren.

Stap 7—Het opstellen van aanvullend beleid en procedures voor het beheersen van risico's

Een informatiebeveiligingsmaatregel heeft vaak meerdere verschijningsvormen; een organisatorische, een procedurele en een technische. Bijvoorbeeld,
het af te dekken risico is: Niet geautoriseerde toegang tot informatie.
In de Tactische Baseline staat de maatregel 11.2.3 'Gebruik van gebruikerswachtwoorden'. Dit leidt tot een onderwerp in het gemeentelijk informatiebeveiligingsbeleid[10], zie daarvoor 7.1 'Authenticatie en autorisatie' in het beleid voorbeeld document. Het gebruik van wachtwoorden is zo belangrijk dat het een plaats krijgt in het overkoepelend gemeentelijk informatiebeveiligingsbeleid.
In het BIG OP-document 'Wachtwoordbeleid gemeenten' is een verdere verdieping aangebracht op de BIG-eisen en het voorbeeld informatiebeveiligingsbeleid voor de gemeente. Dit leidt onder andere tot een document 'Aanvullend wachtwoordbeleid gemeenten'. Hier komen ook uitvoeringseisen aan bod die iets betekenen voor systeemeigenaren, ICT en de eindgebruiker, bijvoorbeeld in specifieke systeemdocumentatie en rapportages over de uitvoering van wachtwoord processen. Concreet komt op basis van de BIG-maatregel iets terug in het gemeentelijk informatiebeveiligingsbeleid en het aanvullend wachtwoord beleid van de gemeente. Dit levert binnen de ICT-afdeling één of meerdere procedures op. Bijvoorbeeld een wachtwoord verstrekking procedure of een wachtwoord reset procedure. Maar mogelijk ook een werkinstructie om handmatig of geautomatiseerd te controleren of de gebruikte wachtwoorden wel aan het beleid voldoen. Tevens dienen de systeeminstellingen van verschillende systemen, om het wachtwoordbeleid effectief af te dwingen in die systemen, te worden opgeschreven in beheer documentatie waar de specifieke systeem instellingen worden beschreven.
Uiteindelijk zal aan de CISO periodiek gerapporteerd dienen te worden hoe het staat met de uitwerking van het wachtwoordbeleid. Dit kan ICT-breed worden gedaan maar ook per systeemeigenaar en per systeem. Tevens kan de controle van het wachtwoordbeleid onderdeel zijn van een audit. Afwijkingen leiden dan weer tot aanpassingen in de uitwerking van het beleid in de volgende cyclus.
Het is van belang dat voor alle maatregelen, die meerdere verschijningsvormen hebben, een goede organisatorische, procedurele en technische invoering beschreven is. Bedenk dat er aan het uitvoeren van procedures ook een bewijskant zit, het vastleggen van resultaten en het rapporteren erover.

[10] Wachtwoordbeleid bestaatl binnen de gemeente al voor SUWI en BRP. Het gaat er in dit voorbeeld om dit gemeentebreed te trekken en uit te gaan van een gemeentebreed informatiebeveiligingsbeleid.

Stap 8—Het toewijzen van middelen, opleiding en training
Een van de belangrijkste taken van het management is het beschikbaar stellen van voldoende middelen voor het ontwikkelen, onderhouden en implementeren van het ISMS. Hierbij dient ook aandacht te zijn voor opleidingen van ISMS-deelnemers. Bijvoorbeeld door specifieke beveiligingscursussen, maar ook een aangepaste bewustwordingspresentatie kan hiervoor worden gebruikt. Voor het toewijzen van de middelen is het van belang om een goed invoeringsplan te hebben dat aansluit bij het gemeentelijk informatiebeveiligingsbeleid.

Stap 9—Bewaken van de invoering van het ISMS
Het is noodzakelijk om binnen de gemeente door de interne auditdienst de invoering van het ISMS periodiek te laten toetsen. De geconstateerde afwijkingen of tekortkomingen dienen te worden opgelost door het uitvoeren van correctieve maatregelen. Het gemeentelijke ISMS kan alleen goed werken als het management het ISMS periodiek evalueert. Tijdens deze evaluatie dient te worden gekeken naar noodzakelijke wijzigingen op en verbeteringen aan gemeentelijke beleidsregels, procedures en bemensing. De uitvoering van het ISMS-invoeringsplan dient ook goed te worden bekeken. Alle besluiten en wijzigingen dienen te worden gedocumenteerd.
Als een gemeente wil certificeren tegen de NEN/ISO 27001:2013 dan zijn er nog meer stappen nodig. Voor de BIG zijn deze stappen buiten bereik.

3.1 Succesfactoren
De kritieke succesfactoren bij de invoering van een ISMS zijn:

- Zichtbare ondersteuning en inspanning van de bestuurder en het management van de gemeente. Onder andere door het definiëren en vaststellen van een informatiebeveiligingsbeleid en eventueel een aanvullend ISMS-beleid, waarbij taken en bevoegdheden expliciet zijn belegd.
- Er dient centraal gemanaged te worden op basis van uitgangspunten in het gemeentelijk informatiebeveiligingsbeleid (zie hoofdstuk 5), dat gekoppeld is aan de gemeentelijke doelstellingen.
- Een integraal onderdeel zijn van het managen van de gemeente gerelateerd aan de gemeentelijke doelstellingen rekening houdend met de BIG-uitgangspunten[11].
- Ruimte geven aan en aandacht hebben voor goede opleiding van direct betrokkenen en bewustwordingstrainingen aan gemeentelijk personeel.

3.2 Faalfactoren
De belangrijkste faalfactoren bij de invoering van een ISMS zijn:

- Het niet hebben van een vastgesteld gemeentelijk beveiligingsbeleid waar het ISMS-beleid in is opgenomen of het niet hebben van ISMS-beleid.
- Gebrek aan management ondersteuning. Zonder management ondersteuning is het invoeren van een ISMS gedoemd te mislukken.
- Denken dat het een 'ICT-feestje' is. Informatiebeveiliging dient organisatie breed te worden aangepakt en is niet alleen een ICT-verantwoordelijkheid.
- Gebrek aan prioriteit. Het prioriteren van taken en mijlpalen is voor ieder project belangrijk en dus ook voor een ISMS- invoeringsproject. Tevens dient er aandacht zijn voor quick wins.

[11] Zie paragraaf 2.2 van de Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

- Geen goede meetpunten. Het vaststellen van de ISMS-invoering en het bewaken van de voortgang en effectiviteit, vereist een goed gedefinieerde set aan stuurvragen (zie hoofdstuk 4.7) welke regelmatig dienen te worden vastgesteld.
- Geen methodische aanpak van het ISMS-project. Het is verstandig om het project om het ISMS in te voeren met een goede projectmanagement aanpak.
- Niet aansluiten bij bedrijfsprocessen. Een ISMS moet iets bijdragen aan bedrijfsprocessen en beter nog, aansluiten op bestaande bedrijfsprocessen zoals de P&C-cyclus van de gemeente.

3.3 Het ISMS implementeren en uitvoeren voor kleine gemeenten.

Voor grote gemeenten waar veel specialisatie mogelijk is bestaat een ISMS waarschijnlijk uit meer organisatorische lagen. Dat wil zeggen: er kan een ISMS-overleg bestaan op concern niveau maar ook decentraal binnen directies of afdelingen. Rapportage zal dan ook over meer lijnen gaan.

Kleine gemeenten hebben een plattere / smallere organisatorische structuur. Het ISMS wordt met minder mensen uitgevoerd en bestaat uit één overlegniveau.

Het implementeren van het ISMS kan het beste geleidelijk worden aangepakt. Zie hiervoor het stappenplan, zoals in hoofdstuk 2 is beschreven. Hoe de organisatie ook is, het belangrijkste is dat er een situatie ontstaat waar de PDCA-cyclus tot zijn recht komt.

Wat is minimaal nodig:

- Zorgen voor draagvlak en middelen van het ISMS.
- Verankering in het gemeentelijk informatiebeveiligingsbeleid.
- Toewijzen van rollen en verantwoordelijkheden.
- Starten met de GAP-analyse en maatregelen implementeren, door middel van een informatiebeveiligingsplan. Over die invoering laten rapporteren en bijsturen waar nodig.
- Een ISMS -overleg starten, bijvoorbeeld per kwartaal. De CISO is de voorzitter en deelnemers zijn bijvoorbeeld actiehouders die beveiligingsmaatregelen moeten implementeren, maar ook de ACIB en/of VCIB kunnen een rol hebben.
- Ervoor zorgen dat beveiligingsincidenten worden herkend, gemeld en gecorrigeerd.
- Uitzonderingen op beheersmaatregelen herkennen en indien nodig actie ondernemen.
- Het op orde hebben van de beheerprocessen zoals configuratiebeheer, incidentmanagement, patchmanagement, wijzigingsbeheer en gebruikersbeheer.
- Interne ISMS-audits (laten) uitvoeren en de uitzonderingen en tekortkomingen in het ISMS-overleg bespreken. Verbetermaatregelen vaststellen en uitvoeren om het ISMS te verbeteren.
- Opzetten en uitvoeren van trainingen en bewustwording.
- Rapportage aan het management.

4 ISMS-beheersing

4.1 Taken en rollen binnen het ISMS

- Het college van B&W stelt formeel het informatiebeveiligingsbeleid vast. De uitvoering van het beleid moet gecontroleerd worden, zowel het college van B&W als de gemeenteraad (controle functie) kunnen hiervoor opdracht geven om dit te (laten) controleren. De gemeentedirectie adviseert het college van B&W formeel over het vast te stellen beleid.
- De Chief Information Officer (CIO) of vergelijkbare rol geeft namens de gemeentedirectie op dagelijkse basis invulling aan de sturende rol. Dit door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan. De informatiebeveiligingstaken die hieruit voortvloeien zijn belegd bij de Chief Information Security Officer (CISO). De CISO bevordert en adviseert gevraagd en ongevraagd over informatiebeveiliging en rapporteert eens per kwartaal structureel gemeentebreed aan de directie over de stand van zaken.
- Bij grote gemeenten kan de coördinatie van informatiebeveiliging belegd zijn bij een strategische beveiligingsadviesfunctie binnen alle afdelingen. Daarbij zijn dan uitvoerende taken zoveel mogelijk belegd bij (decentrale) informatiebeveiligingsfunctionarissen. De afdelingen rapporteren aan de CISO. Over het functioneren van informatiebeveiliging wordt jaarlijks gerapporteerd conform de P&C-cyclus. Bij kleine gemeenten is de beveiligingsfunctie vaak platter van aard. Er is een (soms in deeltijd) CISO die rechtstreeks coördineert met het ICT-hoofd of een ICT-beveiligingsfunctionaris en managers.
- De gemeentelijke service organisatie (in het bijzonder ICT) heeft een informatiebeveiligingsfunctionaris aangesteld voor dagelijks beheer van technische informatiebeveiligingsaspecten. De veiligheidsfunctionaris rapporteert aan de CISO. Informatiebeveiliging is onderdeel van de service managementrapportage.
- Het lijnmanagement is verantwoordelijk voor de kwaliteit van de bedrijfsvoering. Die verantwoordelijkheid wordt verticaal in de lijn verdeeld, van organisatietop tot teamleider. Informatiebeveiliging geldt als een integraal onderdeel van de bedrijfsvoering. Zo is het lijnmanagement ook verantwoordelijk voor informatiebeveiliging. Het begrip lijnmanagement wordt hierbij ruim opgevat. In voorkomende gevallen kan ook een afdelingshoofd of een manager van een stafafdeling onder het lijnmanagement worden verstaan.

Overleg

De CISO of gemeentelijke informatiebeveiligingsfunctionaris stelt een organisatie voor van security gerelateerde functionarissen binnen de gemeenten en de CISO organiseert tenminste eenmaal per kwartaal een ISMS-overleg met dit gremium. De CISO / informatiebeveiligingsfunctionaris is voorzitter. Het overleg heeft binnen de gemeente een adviesfunctie richting de CIO of gelijkwaardig en richt zich voornamelijk op beleid en adviseert over tactisch/strategische informatiebeveiligingskwesties. Input voor dit overleg zijn bijvoorbeeld opgetreden beveiligingsincidenten met het doel om te komen tot een aanbeveling of hier structureel iets aan moet gebeuren. Ook wordt hier gesproken over inrichting en voortgang van de informatiebeveiligingsfunctie binnen de gemeente en de invoering van de BIG.
Het onderwerp informatiebeveiliging dient verder een vast onderdeel te zijn op de agenda van het lijnoverleg zodat er sturing plaatsvindt op de uitgevoerde activiteiten.
Van de overleggen moet een verslag worden bijgehouden waarin ook de actiepunten, voortgang en besluiten staan.

4.2 ISMS-documentatie

Voor een goed gedocumenteerd ISMS moet er een minimale set aan documentatie zijn binnen de gemeente. Er kunnen verschillen zijn in de hoeveelheid documentatie, afhankelijk van de grootte van de gemeente en de hoeveelheid informatiesystemen.
De basis voor het ISMS is dat er beleidsuitgangspunten zijn waarin het volgende aan bod komt:

- Dat verantwoordelijkheid genomen wordt door het college van B&W van de gemeente voor het hebben van een ISMS.
- De reikwijdte van het ISMS.
- De beheersing van het ISMS door maatregelen en procedures.
- De manier waarop risicobeoordeling wordt vormgegeven binnen de gemeente.
- Rapportage van risicobeoordeling.
- Een informatiebeveiligingsplan, dus hoe maatregelen worden geïmplementeerd om risico's tegen te gaan (op basis van de GAP- en impactanalyse) en wie hiervoor binnen de gemeente verantwoordelijk is.
- Gedocumenteerde en formeel goedgekeurde procedures.
- Vaststellen hoe de effectiviteit van het ISMS wordt gemeten.

4.3 Beheersing van de ISMS-documentatie

ISMS documentatie heeft vele verschijningsvormen, zoals beleid, procedures, rapportages en verslagen. Deze documenten dienen te worden beheerst en beschermd. Binnen de gemeente dienen een aantal zaken geregeld te worden met betrekking tot de beheersing van ISMS-documenten.

- Goedkeuringsprocedure: Documenten dienen te worden goedgekeurd.
- Wijzigingsprocedure ISMS-documenten: naast de wijzigingsprocedure zelf, ook het opnemen van een wijzigingenblad voor het vastleggen van wijzigingen in documenten.
- Verspreiding en beheersingsprocedure van documentatie: Verspreiding van documenten zodat ze voor medewerkers beschikbaar zijn, intrekken verouderde documenten en bekend stellen nieuwe documenten, denk na over communicatie.

4.4 Beheersing van ISMS-registraties

Ten behoeve van de werking van het ISMS worden registraties bijgehouden. Denk hierbij aan auditrapporten, incidentoverzichten en dergelijke. Ook registraties die de werking aantonen van beveiligingsmaatregelen vallen hier onder. Denk hierbij aan bezoekersregistraties maar ook (systeem) autorisaties. Op alle registraties kan ook een wettelijke bewaarplicht van toepassing zijn.

Binnen de gemeente dient te worden vastgesteld welke registraties ten behoeve van het ISMS worden bijgehouden en waar en hoe lang deze worden bewaard.

4.5 Het auditen van het ISMS

Het is aan te bevelen om de werking en effectiviteit van het ISMS te laten controleren om vast te stellen of voldaan wordt aan de relevante BIG-eisen en het daarvan afgeleide gemeentelijk informatiebeveiligingsbeleid.

Zoals de afdelingshoofden / proceseigenaren dienen te rapporteren over de invoering van de beveiligingseisen, dient de CISO of vergelijkbare functionaris er voor zorg te dragen dat gerapporteerd wordt over de effectiviteit van het ISMS binnen de gemeente. Het ISMS is immers de basis voor risicomanagement en verbetering in beveiligingsmaatregelen op basis van

bijvoorbeeld incidenten. De audits dienen periodiek gepland en uitgevoerd te worden waarbij rekening gehouden wordt met de processen en gebieden die deze audit moeten ondergaan (bereik), evenals met de resultaten van vorige audits. De CISO bepaald in overleg met het management de auditcriteria, de reikwijdte, de auditfrequentie ten behoeve van het ISMS, en legt deze keuzes vast in een auditprocedure. Het ISMS zou minimaal eens per jaar dienen te worden beoordeeld.
Leidinggevenden/proceseigenaren bepalen voor hun eigen processen en essentiële systemen de auditcriteria, de reikwijdte en de auditfrequentie en leggen dit vast in een auditprocedure.

De resultaten van de audits (geconstateerde afwijkingen en oorzaken) dienen te worden geprioriteerd en uitgevoerd op basis van een risicoafweging. Daarnaast zijn de resultaten van de audits weer input voor het ISMS-overleg en managementrapportages.

De CISO maakt in ieder geval van de ISMS-audit een verslag dat dient ter rapportage aan de directie van de gemeente. Dit verslag bevat:

1) Het resultaat van de ISMS audit.
2) Verbeterpunten/afwijkingen en ondernomen acties.
3) Status van de invoering van maatregelen.
4) Resultaten van eerdere audits en de voortgang.
5) Aanbevelingen voor aanpassing/verbetering van het ISMS.
6) De benodigde middelen om verbeteringen door te voeren.
7) Zaken die het ISMS kunnen beïnvloeden, zoals:
    - Eisen van de bedrijfsvoering
    - Beveiligingseisen
    - Bedrijfsprocessen die van invloed zijn op bestaande bedrijfseisen
    - Eisen uit wet- of regelgeving
    - Contractuele verplichtingen
    - Risiconiveaus en/of criteria voor risicoaanvaarding

4.6 ISMS-documentatiesoorten

Alles wat nodig is om informatiebeveiliging als proces te laten werken is ISMS-documentatie te noemen. Voorbeelden van deze documenten zijn:

Normenkaders

De strategische- en tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Gemeentelijk informatiebeveiligingsbeleid

Hierin staan de beleidsuitspraken met betrekking tot informatiebeveiliging binnen de gemeente.

Gemeentelijk informatiebeveiligingsplan

Dit plan bevat de operationalisering van het informatiebeveiligingsbeleid. Dus wie moet wat doen in relatie tot de beleidsuitgangspunten. Daarnaast bevat het plan de resultaten van de impactanalyse, de geplande activiteiten om informatiebeveiligingsmaatregelen te implementeren en hun actiehouders.

Aanvullend gemeentelijk informatiebeveiligingsbeleid en (operationele) procedures

Het gemeentelijk informatiebeveiligingsbeleid bevat vele punten die in een specifiek beleid verder kunnen worden uitgewerkt. Bijvoorbeeld wachtwoordbeleid.

Audit rapporten

De resultaten van interne en externe ISMS- en beveiligingsaudits horen bij de documentatie, maar ook wat er met het resultaat van die audits is gedaan.

Rapportages

Rapportages over de werking van beveiligingsmaatregelen, controles en systeemlogboeken die belangrijk zijn om bij te sturen en de effectiviteit van het ISMS te beoordelen. Hier hoort ook de rapportage over de werking van het ISMS zelf bij.

Resultaten van risicoanalyses / risicologs

Risicoanalyses dienen nog steeds te worden uitgevoerd. De resultaten (risico's en maatregelen) zijn belangrijk, om achteraf vast te kunnen stellen of de gekozen maatregelen wel voldoende waren geweest bij een opgetreden incident.

Analyserapporten van beveiligingsincidenten die optreden binnen de gemeente moeten worden geanalyseerd om vast te stellen of er verbeteringen mogelijk is om risico's te voorkomen. Kortom het verbeteren van de risicoaanpak.

ISMS-vergaderverslagen

Deze verslagen geven weer wat er met de input van het ISMS-overleg gedaan is en maken het ISMS-overleg wat minder vrijblijvend. Tevens toont het ook achteraf aan dat er overleg is geweest, wie daar bij aanwezig waren en wat het resultaat was.

Het resultaat van de GAP- en de impactanalyses.

In de ISO 27001 wordt gesproken over een Statement Of Applicability (SOA). De GAP- en impactanalyse van de BIG vervult die rol ten opzichte van de BIG, als normenkader voor de gemeente. Het moet duidelijk zijn wat de status van maatregelen is, maar ook welke maatregelen buiten bereik (out of scope) zijn verklaard. De GAP- en impactanalyse kan gemeentebreed uitgevoerd zijn maar ook per informatiesysteem, in dat geval zijn er meer.

Aandachtspunten

Houdt aanvullend informatiebeveiligingsbeleid en procedures die binnen de gemeente opgesteld dienen te worden zo kort en bondig mogelijk. Dit heeft een aantal voordelen, zoals:

- Deze zijn eenvoudige te schrijven.
- De review gaat sneller.
- De goedkeuring is eenvoudiger.
- De kleinere stukken zijn eenvoudiger te implementeren, lezen en te begrijpen.
- Ze zijn makkelijker te onderhouden. Indien je meerdere onderwerpen per beleid / policy opneemt moet je mogelijk vaker wijzigen.

Denk na over de ISMS-documentatiestructuur binnen de gemeente. Knip het op in kleine stukken die te plannen en uitvoerbaar zijn. Een groot allesomvattend handboek met beleid en procedures is minder makkelijk leesbaar en wordt niet begrepen. Tenslotte is het nooit af, houdt het daarom klein en overzichtelijk.

4.7 ISMS-stuurvragen 'meten is weten'

Het meten van de effectiviteit van het ISMS en de effectiviteit van de informatiebeveiliging kan gedaan worden door het vaststellen van normen, hierover te laten rapporteren en het uitvoeren van controle over die rapportages. De invoering van de BIG vereist transparantie en verantwoording, zowel intern als extern. Maar er zijn ook gemeentelijke interne factoren die de behoefte hebben om investeringen in informatiebeveiliging te rechtvaardigen en te prioriteren. Daarnaast dient er een goede afstemming te zijn tussen informatiebeveiliging en de algemene gemeentelijke missie, doelen en doelstellingen. Het meten dient ook het fine-tunen van de effectiviteit en efficiëntie van het informatiebeveiligingsprogramma. Tenslotte is het belangrijk om vast te stellen of er ISMS-activiteiten zijn, die verbeterd dienen te worden omdat ze niet het beoogde effect hebben.

'In control' zijn

Deze term is onlosmakelijk verbonden met het aantonen dat de gemeente informatieveiligheid beheerst op een niveau die past bij de BIG. In dit verband wordt ook de verklaring genoemd die hoort bij verantwoording, de 'in control statement'. Er zijn gemeenten die dit toepassen bij de verklaring van afdelingen of directies dat informatiebeveiliging beheerst wordt. Dat wil zeggen: het is bekend wat de status van beveiligingsmaatregelen is, bijvoorbeeld:

- De aantallen ingevoerde maatregelen.
- De aantallen nog te implementeren maatregelen.
- Welke maatregelen bewust niet geïmplementeerd worden (geaccepteerd risico's).
- De aantallen systemen waar nog beveiligingsmaatregelen voor geïmplementeerd dienen te worden.

Bij het uiteindelijk vaststellen van Kritieke Prestatie Indicatoren (KPI's) is het van belang het volgende af te vragen:

- Wat wordt er gemeten?
- Wat is het doel van de meting?
- Hoe wordt er gemeten en met welke frequentie?
- Wie voert de meting uit?
- Wie documenteert dat de meting is uitgevoerd en gerapporteerd?
- Zijn er wijzigingen die er voor zorgen dat de KPI dient te worden aangepast?

Welke KPI's zijn er bijvoorbeeld in relatie tot de BIG voor de gemeente:

Beleid

- Is het gemeentelijk informatiebeveiligingsbeleid geaccordeerd door het college van B&W?.
- Hoe recent is het informatiebeveiligingsbeleid?
- Is de gemeente bij de IBD ingeschreven en zijn alle stappen uitgevoerd?
- Wanneer was de laatste update van de gemeentelijke 'ICT-foto' die naar de IBD is gezonden?
- Wat is de frequentie van het ISMS-overleg binnen de gemeente?

GAP- en impactanalyse, baselinetoets en risicoanalyses

- Zijn de kritieke (bedrijfs)processen en bijbehorende informatiesystemen benoemd?
- Voor hoeveel systemen is de GAP- en impactanalyse uitgevoerd versus de aantallen systemen waarvoor dit gedaan zou moeten worden?
- Voor hoeveel systemen is er een baselinetoets en risicoanalyse uitgevoerd versus de aantallen systemen waarvoor dit gedaan zou moeten worden?

Bewustwording

- Hoeveel mensen hebben deelgenomen aan het informatieveiligheidsbewustwordingsprogramma versus de aantallen die deel hadden moeten nemen?
- Wat zijn de technische aspecten van de aantallen ingevoerde maatregelen?
- Wat is het aantal verwerkte patches versus het aantal beveiligingsincidenten in relatie tot die patches?
- Wat is het aantal gemelde patches versus de doorgevoerde patches?
- Wat is de doorlooptijd van de patches in werkdagen?

Incidenten en continuïteit

- Wat is de hoeveelheid beveiligingsincidenten?
- Wat is de gemiddelde tijdsduur tussen een geconstateerd incident en de opvolging?
- Wat is de gemiddelde tijdsduur tussen een geconstateerd incident en de melding naar de IBD?
- Wat is de (geschatte) schade van de informatiebeveiligingsincidenten geweest sinds de laatste rapportage?

Verantwoording

- Hoeveel audits zijn er uitgevoerd?
- Hoeveel audit aanbevelingen dienen er te worden opgevolgd?
- Hoeveel audit aanbevelingen zijn er opgevolgd?

Evalueren en leren

- Wanneer is de laatste test calamiteitenplannen geweest?
- Is de informatieveiligheidscyclus bijgesteld op basis van incidenten, ontwikkelingen, audits en / of reviews?

4.8 ISMS-tooling

Gemeenten die met de BIG aan de slag gaan merken al gauw dat enkele systemen en processen bijhouden met de GAP-analyse spreadsheet nog wel gaat. Het is dan het toevoegen van kolommen en/of bijhouden van een GAP-analyse per systeem. Echter als men voor heel veel gemeentelijke processen en informatiesystemen de GAP-analyse wil bijhouden wordt het mogelijk een behoorlijke administratieve kluif.
Daarnaast wil men binnen de gemeente de voortgang van de invoering en de status van de maatregelen makkelijk kunnen bijhouden. Idealiter worden deze bijgehouden door de persoon die de maatregel toepast of implementeert. Als meerdere personen dit op één plaats bijhouden is met één druk op de knop het overzicht te maken waar de gemeente staat ten opzichte van de BIG als geheel.

Voor dit probleem bestaat er 'tooling' die gemeenten helpt om een eigen normenkader bij te houden of een organisatie brede baseline te onderhouden. Mits goed ingericht, bijgehouden en gebruikt kan met één druk op de knop het overzicht verkregen worden van de status per actiehouder, informatiesysteem, maatregel, afdeling of voor de hele organisatie.
De tooling die hiervoor wordt gebruikt heet GRC-tooling. GRC staat voor Governance, Risk and Compliance.

- Governance: beleid, procedures en maatregelen om een organisatie, in dit geval de gemeente, te kunnen laten functioneren in overeenstemming met haar doelstellingen.
- Riskmanagement: procedures en maatregelen gericht op het identificeren van risico's, het nemen van mitigerende maatregelen en het rapporteren aan de leiding over het functioneren van riskmanagement. Vanuit de BIG gaat het hier om de baselinetoets BIG, de diepgaande risicoanalyse en de Privacy Impact Assessment (PIA).
- Compliance: hiermee wordt aangeduid dat een persoon of organisatie werkt in overeenstemming met de geldende wet- en regelgeving. Het gaat over het nakomen van normen of het zich er naar schikken. Dit is voor de BIG een belangrijk onderwerp omdat hier de verantwoording over BIG-maatregelen maar ook verantwoording over andere maatregelen mee wordt bedoeld. Denk hier dan ook aan verantwoording over wetgeving zoals de Wet Bescherming Persoonsgegevens (Wbp) en bijvoorbeeld Basis Registratie Personen (BRP).

De voordelen van een tool zijn:

- Als er voor meerdere systemen een GAP-analyse wordt uitgevoerd, neemt de hoeveelheid kolommen in de GAP-analyse toe of er worden verschillende spreadsheets bijgehouden. Dat kan veel werk kosten. De hoeveelheid regels, actiehouders en informatiesystemen zijn niet meer beperkt door het gebruik van MS Excel.
- Deelname van veel verschillende personen voor het bijhouden van de status van BIG-maatregelen kan door de personen zelf worden gedaan en vereist niet het heen en weer zenden van MS Excelsheets.
- Met één druk op de knop wordt de status van de maatregelen weergegeven. Dit vereenvoudigt de rapportage mogelijkheden, ook gemeentebreed. Horizontale en verticale verantwoording worden ondersteund.

Welke eisen kunnen worden gesteld aan GRC-tooling voor ondersteuning bij de invoering van de BIG.

- Multigemeente: de mogelijkheid om met meerdere gemeenten samen te werken (samenwerkingsverbanden, Gemeenschappelijke Regelingen (GR)).
- Multiuser: aan kunnen maken van alle benodigde gebruikers die een rol hebben in maatregel invoering en verantwoording.
- Authenticatie mogelijkheden: minimaal gebruikersnaam en wachtwoord.
- Autorisatiemogelijkheden: kunnen aanmaken van groepen, maar ook functiescheiding tot op informatiesysteem en maatregelniveau.
- Workflow ondersteuning en signaleringsfunctie.
- Rapportage: uitvoer naar verschillende formaten, organisatie breed, per afdeling, per verantwoordelijke, per proces, per systeem, per maatregel, per control, per groep van maatregelen et cetera.
- En ten slotte niet onbelangrijk, er moeten normenkaders kunnen worden toegevoegd, zoals de BIG, of nog beter, de BIG is al opgenomen bij de normen in de tool.
- Eenvoudig in gebruik: ook als iemand na bepaalde tijd invoering of status van maatregelen wil bijwerken moet het eenvoudig zijn om dit te doen.
- Denk na over eigenaarschap en beheer: wie gaat er over en hoe makkelijk is het om het systeem te beheren.

5 Bijlage: ISMS-beleid gemeente

Zie gemeentelijk informatiebeveiligingsbeleid op basis van de BIG voor de ISMS verankering binnen de gemeente.

Hoofdstuk 2: Verantwoordelijkheden
Hoofdstuk 8: Beveiligingsincidenten
Hoofdstuk 10: Naleving

Indien het voorbeeld Informatiebeveiligingsbeleid niet wordt gebruikt kunnen deze hoofdstukken uit dat voorbeeld Informatiebeveiligingsbeleid gebruikt worden om ISMS-beleid vorm te geven.

INFORMATIE BEVEILIGINGS DIENST

**INFORMATIEBEVEILIGINGSDIENST
V00R GEMEENTEN (IBD)**

**NASSAULAAN 12
2514 JS DEN HAAG**

**POSTBUS 30435
2500 GK DEN HAAG**

**HELPDESK 070 373 80 11
ALGEMEEN 070 373 80 08
FAX 070 363 56 82**

**INFO@IBDGEMEENTEN.NL
WWW.IBDGEMEENTEN.NL**

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN