INFORMATIE
BEVEILIGINGS
DIENST

STRATEGISCHE BASELINE INFORMATIEBEVEILIGING NEDERLANDSE GEMEENTEN

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Meer informatie

Heeft u vragen over onderhavig document? De Informatiebeveiligingsdienst voor gemeenten beantwoordt deze graag via **info@ibdgemeenten.nl of via** 070 373 8011.

Wijzigingshistorie:

versie	**datum**	**Opmerkingen**
1.0	26 mei 2013	Eerste versie van deze BIG SNK
1.01	8 juli 2015	Opmerkingen verwerkt welke uit de gemeenten zijn ontvangen in de voorgaande periode
1.02	Juli 2016	Website NEN toegevoegd

Gerelateerde documenten

Titel	Auteur	Jaartal	Omschrijving
NEN-ISO/IEC-27001/27002	NEN	2005 / 2007	De code voor informatiebeveiliging, zie www.nen.nl
Wbp			Wet Bescherming Persoonsgegevens
SUWI			SUWI-wet en -aansluitvoorwaarden
Normenkader GeVS	BKWI	2011	Gezamenlijke elektronische Voorzieningen SUWI
BIR-familie		2012	Baseline Informatiebeveiliging Rijk
BRP1			/ Basisregistratie Personen.
BIA	ISF	2007	Business Impact Analyse
GEMMA	KING		GEMeentelijk Model Architectuur (GEMMA)
NORA		2007	De Nederlandse Overheid Referentie Architectuur
ITIL security management	Spruit, M. (HEC)	2003	www.marcelspruit.nl/papers/itilsecman.pdf
RASCI			www.kwaliteitshandvesten.nl
Best Practice Normen Informatiebeveiliging ICT-voorzieningen	Jaap van der Veen	2009	Beveiligingspatronen, versie 1.0
Diverse NCSC documenten			www.ncsc.nl
Basiskennis Informatiebeveiliging volgens NEN-ISO 2700x	J. Hintzbergen en anderen	2011	Van Haren Publishing
Provinciale Baseline Informatiebeveiliging	Diverse auteurs	2010	
Diverse informatie beveiligingsplannen gemeenten	Diverse auteurs		
Het inrichten van een beveiligingsorganisatie. Welke factoren zijn van invloed?	PvIB	2006	http://www.pvib.nl/download/?id=6259853

[1] De Basisregistratie Personen (BRP) heeft de Gemeentelijke Basisadministratie Personen (GBA) vervangen. In de BRP staan persoonsgegevens van inwoners in Nederland (de ingezetenen) en van personen in het buitenland die een relatie hebben met de Nederlandse overheid (de niet-ingezetenen).

INHOUDSOPGAVE

1 Management samenvatting

1.1 Achtergrond

Door de toenemende digitalisering is het zorgvuldig omgaan met de informatie en gegevens van burgers, bedrijven en ketenpartners voor gemeenten van groot belang. Uitval van computers of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de continuïteit van de bedrijfsvoering en het primaire proces. Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening van gemeenten. Het is niet ondenkbaar dat hieraan ook politieke consequenties verbonden zijn of dat het imago van de gemeente en daarmee van de overheid in het algemeen wordt geschaad.

De DigiNotar-crisis en Lektober in 2011 hebben aangetoond dat de ICT-infrastructuur van gemeenten kwetsbaar is. Uit de acties rondom Lektober is gebleken dat de gemeentelijke beveiliging van de ICT-infrastructuur en de opgeslagen informatie niet bij alle gemeenten even goed op orde is.

In 2012 hebben gemeenten aanzienlijke investeringen gedaan om incidenten op te lossen als gevolg van het zogenaamde Dorifel virus[2]. Onderzoek van TNO geeft aan dat cybercriminaliteit de Nederlandse economie jaarlijks ongeveer €10 miljard kost. Deze raming zou kunnen betekenen dat de schade door cybercriminaliteit voor gemeenten jaarlijks ongeveer €300 miljoen bedraagt.[3]

Maar de beveiligingsincidenten gaan over meer dan geld alleen. De overheid beheert veel persoonsgegevens. Als de overheid de beveiliging hiervan niet voldoende kan waarborgen, is het vertrouwen in de overheid in het geding. Een incident met de rioleringspompen in een gemeente liet zien dat het mogelijk is om op afstand via internet pompen, en vergelijkbare systemen als sluizen en gemalen, te hacken. In dergelijke gevallen is ook de fysieke veiligheid van burgers in het geding.

De belangrijkste les uit de incidenten is dan ook dat er behoefte is aan een fundamentele oplossing van het informatieveiligheidsprobleem bij gemeenten. De Rijksoverheid gaat eveneens nadere eisen stellen aan de beveiliging van de gemeentelijke informatiehuishouding, bijvoorbeeld als voorwaarde om aangesloten te zijn en te blijven op DigiD. Ook in het onderzoek van de Onderzoeksraad voor Veiligheid naar het DigiNotar-incident is een dergelijk aanbeveling opgenomen. De eerste stap op dit pad is het ontwikkelen van een integrale Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten. Deze ligt nu voor u.

[2] http://webwereld.nl/nieuws/111490/dorifel-kost-gemeenten-tienduizenden-euro-s.html
[3] http://www.nu.nl/internet/2783983/cybercrime-kost-nederland-10-miljard-per-jaar--.html

1.2 Opdracht

Doel

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft opdracht gegeven voor het ontwikkelen van een Baseline Informatiebeveiliging Nederlandse Gemeenten. De Baseline Informatiebeveiliging Nederlandse Gemeenten is bedoeld om:

1. Gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging.
2. Gemeenten een hulpmiddel te geven om aan alle eisen op het gebied van Informatiebeveiliging te kunnen voldoen.
3. De auditlast bij gemeenten te verminderen.
4. Gemeenten een aantoonbaar betrouwbare partner te laten zijn.

Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de processen bij gemeenten. Informatiebeveiliging is het proces dat deze betrouwbare informatievoorziening borgt. Het opnemen van informatiebeveiliging als kwaliteitscriterium voor een gezonde bedrijfsvoering is tegenwoordig niet langer een keuze, het is bittere noodzaak geworden.

De integrale Baseline Informatiebeveiliging Nederlandse Gemeenten bestaat uit drie delen:

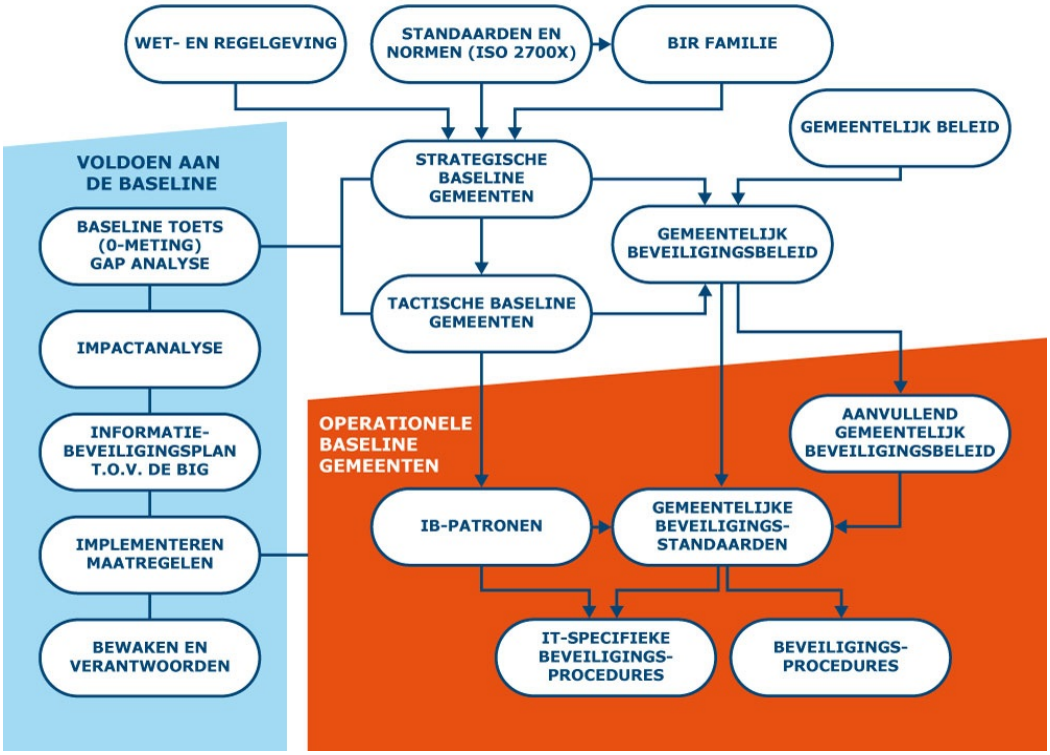
1. BIG – Strategische Baseline

   De Strategische Baseline kan gezien worden als de ’kapstok’ waaraan de elementen van informatiebeveiliging opgehangen kunnen worden. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente. De Strategisch Baseline omvat onderhavig document.

2. BIG – Tactische Baseline
   De Tactische Baseline beschrijft de normen en maatregelen ten behoeve van controle en risicomanagement. De Tactische Baseline beschrijft aan de hand van dezelfde indeling als de internationale beveiligingsnorm ISO/IEC 27002:2007, de controls/maatregelen die als baseline gelden voor de gemeenten. De Tactische Baseline is een separaat document.

3. BIG – Operationele baseline

Om de invoering van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD producten ontwikkeld op operationeel niveau. Deze producten zijn samen met een groot aantal betrokken gemeenten vervaardigd, vertegenwoordigers van deze gemeenten hebben de producten gereviewd.



Figuur 1: Structuur van de BIG-documenten

2 De Strategische Baseline

Onderhavige Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten (hierna: Strategische Baseline) bevat een hiërarchie in de beschrijving van de informatiebeveiligingseisen. Binnen dit hoofdstuk zijn de beleidsuitgangspunten als Strategische Baseline van de informatiebeveiliging binnen de gemeente weergegeven.

Deze Strategisch Baseline sluit aan bij de organisatie van informatiebeveiliging binnen de Rijksdienst. De Baseline Informatiebeveiliging Rijksdienst is overeenkomstig beschreven. Dit omdat processen en ondersteunende informatiesystemen overheidsbreed gebruikt worden en daarmee de verankering en verantwoording (SISA) ook op eenzelfde manier dient plaats te vinden.

2.1 Scope

De scope van deze Strategische Baseline omvat de bedrijfsvoeringsprocessen, onderliggende informatiesystemen en informatie van de gemeente in de meest brede zin van het woord. Deze Strategische Baseline is van toepassing op alle ruimten van een gemeentehuis en aanverwante gebouwen. Alsmede op de apparatuur die door gemeente ambtenaren gebruikt worden bij de uitoefening van hun taak op diverse locaties. Deze Strategische Baseline heeft betrekking op de informatie die daarbinnen verwerkt wordt. Als informatiesystemen niet fysiek binnen de gemeente draaien is deze Strategische Baseline ook van toepassing.[4]

Binnen de scope van deze Strategische Baseline vallen alle op dit moment geldende normen en regels op het gebied van informatiebeveiliging die door derden aan de gemeente opgelegd zijn. Deze Strategische Baseline bevat minimaal al deze maatregelen en brengt ze met elkaar in verband.

Binnen de scope is ook rekening gehouden met de verregaande digitalisering van de overheid en met de in de toekomst nog volgende basisregistraties of aanvullingen op bestaande basisregistraties.

2.2 Uitgangspunten

- Binnen de gemeenten is het College van Burgemeester en Wethouders integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente. Informatiebeveiliging gaat niet over ICT alleen, het gaat over informatie in alle verschijningvormen binnen de organisatie.

[4] Denk aan SAAS, uitbesteding van taken etc.

- Er is gekozen voor een optimale aansluiting bij de wereld van geaccepteerde standaarden, ISO 27001:2005 en ISO 27002:2007 en de daarvan afgeleide overheidsstandaarden zoals de VIR/BIR. Indien een organisatieonderdeel of een toeleverancier haar zaken op orde heeft volgens ISO 27001:2005, rekening houdend met de implementatiemaatregelen uit ISO 27002:2007, dan hoeft deze gemeente slechts te controleren op de aanvullende bepalingen voor bijvoorbeeld aansluitvoorwaarden voor een specifiek register.

- Het basisvertrouwelijkheidniveau is vastgesteld als 'Departementaal Vertrouwelijk'[5], zoals gedefinieerd in het Besluit Voorschrift Informatiebeveiliging Rijksdienst-Bijzondere Informatie (VIRBI:2012). Voor wat betreft de bescherming van privacygevoelige informatie is uitgegaan van verwerking van persoonsgegevens zoals bedoeld in artikel 16 van de Wbp. De combinatie van beide niveaus komt veelvuldig voor bij de decentrale overheid. Voor gemeenten praten we hier over 'Vertrouwelijk'. Het gaat dan bijvoorbeeld om persoonsvertrouwelijke informatie, commercieel vertrouwelijke informatie of gevoelige informatie in het kader van beleidsvorming, zogenaamde beleidsintimiteit.

- Als overheden hun informatievoorziening en ICT inrichten volgens deze Strategische Baseline in opzet, bestaan en werking, dan is dat afdoende garantie dat gemeenten hun eigen informatie en die van andere overheidsinstellingen zowel centraal als decentraal veilig behandelen. Onder veilig wordt verstaan: betrouwbaar, beschikbaar en correct. Overheden moeten elkaar hierop kunnen aanspreken. Bij de implementatie geldt voor de tactische normen en eisen een 'comply or explain beleid'. Het toetsen vindt plaats aan de hand van de 'in control' verklaring.

- Deze Strategische Baseline is opgesteld op basis van de huidige situatie: gelaagde beveiliging is gebruikt.

- Voor deze Strategische Baseline wordt het 'Schengen'-principe gehanteerd. Dit houdt in, dat organisatie-onderdelen van de overheid elkaar beschouwen als vertrouwd partner en niet als onvertrouwde buitenwereld. Het gevolg hiervan is dat iedere overheidsorganisatie afzonderlijk zijn omgeving beveiligt en 'schoon' houdt en dat de andere omgevingen hierop kunnen vertrouwen. Hierbij moet controle de basis van het vertrouwen zijn (governance).

- Het beveiligingsniveau is in lagen uitbreidbaar. Bij de opbouw van deze Strategische Baseline wordt het principe van gelaagde opbouw gehanteerd. Er is een basisbeveiligingsniveau overeenkomend met departementaal of gemeente Vertrouwelijk. Daar waar bepaalde toepassingen, werkomgevingen of specifieke dreigingen een hogere beveiligingsgraad of specialistische maatregelen vereisen, kunnen extra maatregelen getroffen worden bovenop het

[5] Gemeenten zouden dit ook 'gemeentelijk Vertrouwelijk' kunnen noemen.

basisbeveiligingsniveau. Deze Strategische 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 deze Strategische Baseline opgenomen. Voor dit soort bijzondere omstandigheden moet teruggegrepen worden naar een gerichte risicoafweging.

- Het gekozen Strategische Baseline niveau is zodanig, dat er in een overgrote meerderheid van de gevallen geen aanleiding bestaat om tot extra maatregelen over te gaan.

Deze Strategische Baseline gaat niet uit van één voorgeschreven methodiek, zoals een standaard risicoanalysemethode. De kern is niet zozeer het hanteren van een methodiek, maar het bewust komen tot betrouwbaarheidseisen en -maatregelen. Gemeenten kunnen op deze wijze kiezen voor een methode of systematiek die past bij de interne risicoanalyse methodiek en daarmee dus aansluit op het risico-denken binnen de gemeente. Daarmee is het element 'comply or explain' toegevoegd aan deze Strategische Baseline. In feite wordt hiermee aan het management een managementverantwoording wat betreft de informatiebeveiliging gevraagd.

Doordat deze Strategische Baseline integraal onderdeel is van de bedrijfsvoering sluit het aan bij de planning- en controlcyclus (P&C-cyclus).

2.3 Randvoorwaarden

In deze Strategische Baseline zijn, voor zover mogelijk gegeven de stand van de techniek, de volgende randvoorwaarden op de beveiliging van de gemeenten verwerkt:

1. Informatiebeveiliging is en blijft een verantwoordelijkheid van het lijnmanagement.
2. Het primaire uitgangspunt voor informatiebeveiliging is en blijft risicomanagement[6].
3. De klassieke informatiebeveiligingsaanpak waarbij inperking van mogelijkheden de boventoon voert maakt plaats voor veilig faciliteren.
4. Methoden voor rubricering en continue evaluatie hiervan zijn hanteerbaar om onder- en overrubricering te voorkomen. Onderhavige Strategische Baseline geeft geen aanpak voor rubriceren van informatie.
5. De focus verschuift van netwerkbeveiliging naar gegevensbeveiliging.
6. Verantwoord en bewust gedrag van mensen is essentieel voor een goede informatiebeveiliging.

[6] Hiermee wordt niet bedoeld dat daarmee deze Strategische Baseline niet van toepassing is, de Strategische Baseline bevat het basis beveiligingsniveau en er dient voor informatiesystemen te worden vastgesteld of deze Strategische Baseline wel voldoende afdekt.

7. Deze Strategische Baseline wordt gemeentebreed afgesproken en overheidsbrede kaders en -maatregelen worden ook overheidsbreed afgesproken. Waarbij de overheidsbrede kaders en -maatregelen geënt worden op deze Strategische Baseline. In uitzonderingsgevallen wordt, in overleg, afgeweken.
8. Kennis en expertise zijn essentieel voor een toekomstvaste informatiebeveiliging en moeten geborgd worden.
9. Informatiebeveiliging vereist een integrale aanpak, zowel binnen de gemeenten als voor overheidsbrede gemeenschappelijke voorzieningen.

2.4 Plaatsbepaling en Reikwijdte

Deze Strategische Baseline geldt voor Nederlandse gemeenten waartoe gerekend worden de gemeenten met de daaronder vallende diensten, bedrijven en instellingen zoals werkpleinen.

Deze Strategische Baseline geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.

Informatiebeveiliging is een lijnverantwoordelijkheid en onderdeel van de kwaliteitszorg voor organisatie- en bestuursprocessen en de ondersteunende informatiesystemen.

2.5 Beleid

Het College van Burgemeester en Wethouders van een gemeente stelt het informatiebeveiligingsbeleid vast en draagt dit uit. Het beleid omvat ten minste:

1. De strategische uitgangspunten en randvoorwaarden die de gemeente hanteert ten aanzien van informatiebeveiliging, waaronder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid.
2. Het doel van het informatiebeveiligingsbeleid.
3. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden.
4. De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers.
5. De gemeenschappelijke betrouwbaarheidseisen en normen die voor de gemeente van toepassing zijn.
6. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd.
7. De bevordering van het beveiligingsbewustzijn.

2.6 Verantwoordelijkheden

Het lijnmanagement is verantwoordelijk voor de beveiliging van informatiesystemen.

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.

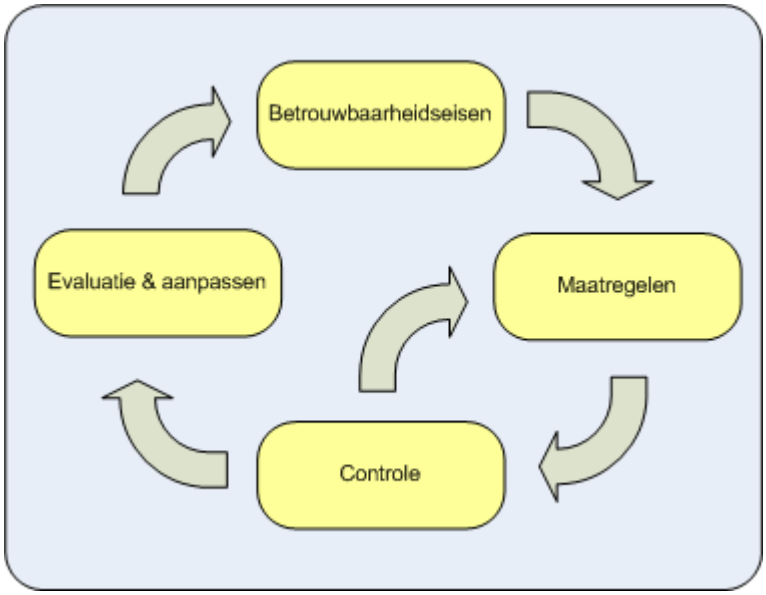
Het lijnmanagement:

1. stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast.
2. is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen.
3. controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze maatregelen worden nageleefd.
4. evalueert periodiek de betrouwbaarheidseisen en stelt deze waar nodig bij.
5. rapporteert over de implementatie van de maatregelen in de management rapportages.

Het lijnmanagement kan besluiten om (delen van) de ontwikkeling, exploitatie of het onderhoud van systemen uit te besteden. Ook in deze gevallen blijft het lijnmanagement verantwoordelijk voor de beveiliging van het individuele systeem. Het lijnmanagement communiceert de betrouwbaarheidseisen van het systeem aan de derde partij. Via een schriftelijke overeenkomst, bijvoorbeeld een bewerkersovereenkomst of een Service Level Agreement wordt vastgelegd hoe de derde partij aan deze eisen gaat voldoen en tevens worden er consequenties verbonden aan het niet naleven van deze afspraken. Vanuit zijn hoedanigheid als verantwoordelijke partij, controleert het lijnmanagement of de werkzaamheden van de derde partij het vereiste betrouwbaarheidsniveau realiseren.

Door het beveiligingsbeleid op te nemen in de P&C-cyclus van de gemeente en hierover door de organisatieonderdelen verantwoording af te laten leggen door reguliere voortgangsrapportages, heeft beveiliging een duidelijke rol in de verticale sturingskolom van een gemeente. 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, de kwaliteitscirkel, wordt conform de P&C-cyclus binnen de gemeente en richting B&W verantwoording afgelegd door het management.

Voor het effectueren van informatiebeveiliging wordt gewerkt via de Plan Do Check Act cyclus (PDCA-cyclus) (zie figuur 2). Na het vaststellen wat nodig is, worden maatregelen getroffen en gecontroleerd of die maatregelen het gewenste effect sorteren (controle). Deze controle kan direct aanleiding geven tot bijsturing in de maatregelen. Ook kan het totaal van eisen, maatregelen en controle aan revisie toe zijn (evaluatie). Het goed doorlopen van deze kwaliteitscirkel zorgt op elk moment voor het adequate beveiligingsniveau.



Figuur 2: PDCA Cyclus

2.7 Opzet, beheer en onderhoud van de Baseline

VNG/KING is eigenaar van dit document en daarmee verantwoordelijk voor het beheer en onderhoud van de totale Baseline Informatiebeveiliging Nederlandse Gemeenten. Deze totale Baseline is gemaakt door de Informatiebeveiligingsdienst voor gemeenten (IBD) en bevat de basisset aan minimale beveiligingsmaatregelen die nodig zijn als stabiele, veilige basis binnen de gemeente.

Dit document en de daarin opgenomen maatregelen worden periodiek op inhoud, uitvoerbaarheid, invoering en werking beoordeeld en, indien nodig, aangepast om te voorkomen dat deze Strategische Baseline veroudert.

De inhoudelijke toetsing en bijstelling van deze Strategische Baseline vinden plaats door de Informatiebeveiligingsdienst voor gemeenten vanuit het nog te starten IB-overleg.

Herziening is mede afhankelijk van de wijzigingen in wetgeving, de onderliggende normen, het beleid en de beheerorganisatie. Beveiligingsincidenten vormen aanwijzingen waar voor de gemeentelijke overheid specifieke kwetsbaarheden liggen. Voor de aanpassing van het minimumniveau wordt dan ook gebruik gemaakt van een analyse van incidenten uit de periode voorafgaand aan het vaststellen van het minimumniveau.

Daarom wordt van de verantwoordelijke functionarissen bij de gemeenten verwacht dat zij zorg dragen voor een juiste en volledige registratie van security incidenten en het melden daarvan aan de Informatiebeveiligingsdienst, als onderdeel van de minimum set van maatregelen.

2.8 Informatiebeveiligingsdienst voor gemeenten (IBD)

Door VNG/KING is op 1 januari 2013 de Informatiebeveiligingsdienst voor gemeenten (IBD) opgericht. De Informatiebeveiligingsdienst voor gemeenten is ingesteld met als missie om IT & informatie gerelateerde veiligheidsincidenten die kunnen optreden bij haar gemeenten in samenwerking met haar gemeenten, partners en leveranciers te bestrijden en waar mogelijk te voorkomen. Zowel als de gemeente(n) doelwit is (zijn) van zulke incidenten of als de gemeente(n) word(t)(en) gebruikt als bron of springplank voor incidenten elders. Hiermee versterkt de Informatiebeveiligingsdienst voor gemeenten de weerbaarheid van de gemeenten tegen ICT-verstoringen en dreigingen' *(Propositie Informatiebeveiligingsdienst 2012).*

De Informatiebeveiligingsdienst voor gemeenten richt zich op het coördineren van de aanpak van informatiebeveiligingsincidenten. De kernactiviteiten zijn het voorkomen (preventie), van incidenten, het signaleren en coördineren van het afhandelen (detectie & coördinatie) daarvan, en het delen, verdiepen en vertalen van kennis (kennisdeling) over informatiebeveiliging.

Binnen elke gemeente is een functionaris nodig die de verantwoordelijkheid heeft om beveiligingsincidenten te melden vanuit de gemeenten aan de Informatiebeveiligingsdienst voor gemeenten en de coördinatie van waarschuwingen vanuit de Informatiebeveiligingsdienst voor gemeenten naar de gemeente te stroomlijnen. Deze functionaris is er nu vaak niet, of het is niet expliciet benoemd als rol. Wil een gemeente aansluiten bij de Informatiebeveiligingsdienst voor gemeenten dan dient hier aandacht voor te zijn, daarnaast is deze functionaris ook nodig om invulling te geven aan deze Strategische Baseline.

Er worden verschillende rollen onderscheiden in relatie tot de IBD en de BIG, deze zijn:

ACIB	Algemeen Contactpersoon Informatiebeveiliging (ACIB) De ACIB krijgt algemene waarschuwingen en informatie met een niet vertrouwelijk karakter over algemene bedreigingen en incidenten.
VCIB	Vertrouwde Contactpersoon Informatiebeveiliging (VCIB) De VCIB krijgt waarschuwingen en informatie met een vertrouwelijk karakter over mogelijke bedreigingen en incidenten die niet met anderen gedeeld

	mogen worden.
CISO	Chief Information Security Officer (CISO) De CISO bevordert en adviseert gevraagd en ongevraagd over de beveiliging van de gemeente, verzorgt rapportages over de status, controleert of met betrekking tot de beveiliging van de gemeente de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de informatiebeveiliging van de gemeente.

2.9 Totstandkoming

Deze Strategische Baseline is tot stand gekomen door samenwerking met een expertgroep Informatiebeveiliging, deze bevat deelnemers uit diverse gemeenten. Daarnaast is er afstemming geweest met BZK en collega's bij decentrale overheden zoals de waterschappen en provincies, maar ook met SUWINET, BAG, RvIG, PUN, NORA en GEMMA.

Het aansluiten bij de Informatiebeveiligingsdienst voor gemeenten vereist uitvoeren van maatregelen die in deze Strategische Baseline opgenomen zijn. Zoals het managen van informatiebeveiliging, het hebben van een informatiebeveiligingsincidentproces en het melden van beveiligingsincidenten aan de Informatiebeveiligingsdienst. Tevens vereist het aansluiten bij de Informatiebeveiligingsdienst voor gemeenten de invoering van deze Strategische Baseline.

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