INFORMATIE
BEVEILIGINGS
DIENST

HANDREIKING

RISICOMANAGEMENT DOOR LIJNMANAGERS

Hoe plaatst u als CISO de lijnmanagers in de juiste rol ten aanzien van informatiebeveiliging?

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document

Risicomanagement door lijnmanagers

Versienummer

1.00

Versiedatum

16 oktober 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	Datum	Wijziging / Actie
0.8	3-8-2018	Interne review
0.87	8-8-2018	Verwerking interne reviewresultaten
0.89	28-8-2018	Voor externe review
0.9	31-8-2018	Externe review
0.99	1-10-2018	Gereedmaken voor publicatie
1.00	16-10-2018	Publicatieversie

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

Dit document stelt de CISO in staat om de lijnmanagers te adviseren die eindverantwoordelijk zijn voor informatiebeveiliging van hun organisatieonderdeel.

Doelgroep

Dit document is van belang voor de CISO en de lijnmanagers in de organisatie.

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
- Baselinetoets
- Diepgaande risicoanalyse methode gemeenten
- Handreiking Dataclassificatie
- Factsheet Informatiebeveiliging en de lijnmanager

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Maatregel 6.1.2.1	De rollen van de CISO en het lijnmanagement zijn beschreven
Maatregel 6.1.3.1	Elke lijnmanager is verantwoordelijk voor de integrale beveiliging van zijn of haar organisatieonderdeel

Inhoudsopgave

1. Inleiding

1.1. Waarom deze handreiking?

Informatiebeveiliging is vaak voor lijnmanagers “ver van mijn bed”, iets dat ergens centraal binnen de organisatie wordt geregeld en waar je op afdelingsniveau geen omkijken naar hebt. Want informatiebeveiliging, daar hebben we toch een CISO voor benoemd? Niets is minder waar. Als CISO heeft u alleen een adviserende en coördinerende rol in relatie tot informatiebeveiliging.

Informatiebeveiliging is integraal onderdeel van de bedrijfsprocessen. Voor elk proces of systeem is een lijnmanager verantwoordelijk en die verantwoordelijkheid strekt zich dus ook uit tot de verantwoordelijkheid voor informatiebeveiliging. Hoe krijgt u als CISO de lijnmanager in de juiste stand als het om informatiebeveiliging gaat?

Als CISO wilt u dezelfde taal spreken als de lijnmanager. Een lijnmanager denkt meestal niet vanuit beveiligingsmaatregelen, maar (bewust of onbewust) vanuit dreigingen en risico's. Een lijnmanager denkt niet in termen van maatregelen om ongeautoriseerde toegang tot het systeem te voorkomen, maar hij weet wel dat misbruik van vertrouwelijke informatie een dreiging is waartegen iets moet worden gedaan. Bij de implementatie van beveiligingsmaatregelen is niet de maatregel het uitgangspunt, maar de dreiging waar de maatregel op is gericht. Het is de verantwoordelijkheid van de lijnmanager om een afweging te maken welke dreigingen een risico vormen voor het uitvoerende proces. Als CISO helpt u de lijnmanager de mogelijke beveiligingsmaatregelen te bepalen om verantwoord met deze risico's om te gaan.

Implementatie van de baseline (BIG / BIO) [1] lijkt soms een doel te zijn, dat gerealiseerd moet worden door de CISO. Dat gaat voorbij aan het feit dat de BIG / BIO niet meer is dan een instrument om beveiligingsmaatregelen gestructureerd in te voeren. Bij implementatie van beveiligingsmaatregelen is er geen sprake van 'one size fits all'. Per informatiesysteem moet gekeken worden of de beveiligingsmaatregelen passend zijn of aanvulling vereisen, of dat er ruimte is om af te wijken ('pas toe of leg uit'). Het doel van informatiebeveiliging is dat risico’s ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid van informatie worden voorkomen. De basis voor informatiebeveiliging is risicomanagement en dat is onderdeel van de taken van de lijnmanager.

Uw rol als CISO is om lijnmanagers te helpen bij het leggen van de relatie tussen dreigingen en risico's en de mogelijke beheer- en beveiligingsmaatregelen. Daarbij laat u de ruimte bij de lijnmanager om vanuit zijn integrale verantwoordelijkheid voor informatiesystemen binnen zijn organisatieonderdeel maatregelen wel of niet van toepassing te verklaren of aan te scherpen. Aan die keuze ligt een risicoafweging ten grondslag.

1.2. Doelstelling van deze handreiking

Deze handreiking legt de relatie tussen de risico’s in het uitvoerende proces en informatiebeveiliging. Wat is de rol van de lijnmanager bij het leggen van deze relatie en welke rol speelt u als CISO in dit verband? Het doel van de handreiking is om u een handvat te geven voor het gesprek met de lijnmanager over informatiebeveiliging, met het doel de lijnmanager in de juiste rol te plaatsen in de beveiligingsorganisatie. Als CISO heeft u een adviserende en coördinerende rol, maar de lijnmanager is uiteindelijk verantwoordelijk voor de keuze welke beveiligingsmaatregelen op het informatiesysteem van toepassing worden verklaard.

1.3. Aanwijzing voor gebruik

Deze handreiking is bedoeld als hulpmiddel voor de CISO om de lijnmanager in de juiste positie te plaatsen in de beveiligingsorganisatie. In het document wordt verwezen naar bestaande operationele producten (BIG-OP) van de Informatiebeveiligingsdienst. Deze zijn terug te vinden op de website van de IBD: www.informatiebeveiligingsdienst.nl. Tegelijkertijd met de publicatie van deze handreiking is een factsheet ‘Informatiebeveiliging en de lijnmanager’ uitgebracht, waarin kort wordt samengevat wat de rol van de lijnmanager is in de beveiligingsorganisatie. Deze factsheet is bedoeld om uit te reiken aan de lijnmanagers in uw organisatie die een rol vervullen als uw aanspreekpunt voor informatiebeveiliging in de gemeentelijke organisatie.

Wij raden u aan om:

- De factsheet ‘Informatiebeveiliging en de lijnmanager’ onder de aandacht te brengen van de lijnmanagers met eindverantwoordelijkheid voor informatiesystemen binnen hun organisatieonderdeel;
- De factsheet ‘Informatiebeveiliging en de lijnmanager’ te gebruiken als basis voor een gesprek over rollen in

[1] Wanneer de bestuurlijke besluitvorming rond is, wordt de eigen baseline voor gemeenten vervangen door een gezamenlijke baseline voor alle overheidslagen, de Baseline Informatiebeveiliging Overheid (BIO). Een belangrijk kenmerk van de BIO is dat deze nog meer dan de BIG zal zijn gebaseerd op risicomanagement. Voor meer informatie over de BIO, zie: https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/

de beveiligingsorganisatie (u als CISO in de controlerende rol, de lijnmanager in de beslissende rol);

- Met de lijnmanagers te bepalen of een diepgaande risicoanalyse op de informatiesystemen noodzakelijk is of dat de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) voor het informatiesysteem voldoende is;
- Bij de vaststelling dat een diepgaande risicoanalyse noodzakelijk is te adviseren welke aanvullende maatregelen mogelijk zijn.

De indeling van dit document is als volgt:

Hoofdstuk 2 : Verantwoordelijkheden van de lijnmanager
Hoofdstuk 3 : Risicomanagement
Hoofdstuk 4 : Uitvoeren risicoanalyse
Hoofdstuk 5 : Naleving en verantwoording
Bijlage : Tabel Dreigingen en maatregelen

2. Verantwoordelijkheden van de lijnmanager

2.1. Inleiding

In uw CISO-rol heeft u er een groot belang bij dat de lijnmanager zijn verantwoordelijkheid kent in het kader van informatiebeveiliging. U moet het volledige spectrum van informatiebeveiligingsmaatregelen overzien in de gemeentelijke organisatie. Maar de dreigingen en risico's die zich in relatie tot informatiebeveiliging voordoen, kunnen verschillen per informatiesysteem. Wat per informatiesysteem aan beveiligingsmaatregelen getroffen wordt, is afhankelijk van de voor dat informatiesysteem geldende betrouwbaarheidseisen, inzicht in de bedrijfsvoering en kennis van wettelijke voorschriften. De lijnmanager is de aangewezen persoon om voor de informatiesystemen binnen zijn organisatieonderdeel te bepalen welk niveau van informatiebeveiliging is vereist. Dat doet hij op basis van een expliciete risicoafweging.

2.2. Verantwoordelijkheden van de lijnmanager

In de Tactische Baseline Informatiebeveiliging[2] zijn de verantwoordelijkheden van het lijnmanagement voor de beveiliging van informatiesystemen als volgt benoemd:

Het lijnmanagement:

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

De afweging van risico's en het kiezen, implementeren, controleren en evalueren van beveiligingsmaatregelen zijn dus expliciet toegewezen aan de lijnmanager. Het gaat hierbij om de eindverantwoordelijkheid. U zult in uw rol als CISO ook regelmatig de actualiteit en geschiktheid van de maatregelen controleren en adviseren over de eventueel benodigde bijstelling van maatregelen en vanuit uw rol rapporteren over de implementatie van beveiligingsmaatregelen in de organisatie als geheel. Maar de verantwoordelijkheid voor de actualiteit en geschiktheid van beveiligingsmaatregelen ten opzichte van het te beveiligen informatiesysteem ligt te allen tijde bij de lijnmanager.

2.3. Waarom is de lijnmanager verantwoordelijk?

De lijnmanager dient te zorgen voor een ongestoorde bedrijfsvoering, zodat de doelstellingen van het bedrijfsproces op een effectieve en efficiënte wijze worden gerealiseerd. Om die doelstellingen te realiseren is informatiebeveiliging een randvoorwaarde. Informatiebeveiliging wordt bereikt door een geschikte verzameling maatregelen in te zetten om met risico's op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van gegevens om te gaan, in die zin is het niet anders dan het omgaan met andere risico's voor de bedrijfsvoering waarvoor de lijnmanager verantwoordelijk is. Het primaire uitgangspunt voor het bepalen van de benodigde beveiligingsmaatregelen is risicomanagement. Het is de rol van de lijnmanager om afwegingen te maken in hoeverre risico's binnen zijn organisatieonderdeel acceptabel zijn. Hij kent het te beveiligen werkproces en de te beschermen informatie uiteindelijk het best. Na toepassing van beveiligingsmaatregelen is het restrisico idealiter tot een voor de lijnmanager acceptabel niveau teruggebracht. De keuze welke restrisico's na het toepassen van beveiligingsmaatregelen worden geaccepteerd, wordt door de lijnmanager gemaakt.

2.4. Wat is de scope van de verantwoordelijkheid?

De verantwoordelijkheid van de lijnmanager wordt begrensd door de scope van de door hem te beheren processen en de dreigingen die hierop van toepassing zijn. Daarom is het belangrijk dat deze scope duidelijk is. De scope kan bestaan uit de informatiesystemen die bij een proces of afdeling horen of om andere reden een bij elkaar behorende

2 Zie de 'Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten':
https://www.informatiebeveiligingsdienst.nl/product/tactische-baseline-informatiebeveiliging-nederlandse-gemeenten-2/

verzameling van informatiesystemen. Het helpt ook om een systeembeschrijving te hebben, aangevuld met een eenvoudig overzicht van de hoofdcomponenten van het informatiesysteem.

Binnen elke gemeente zijn informatiesystemen in gebruik die ondersteunend zijn voor bedrijfsprocessen die de grenzen van een afdeling overstijgen, bijvoorbeeld een zaaksysteem of een postregistratiesysteem. Wie is in dat geval eindverantwoordelijk voor de informatiebeveiliging van dat systeem? Het antwoord is dat ook bij dit soort systemen een lijnmanager is aan te wijzen, die de eindverantwoordelijkheid heeft voor het invullen van de betrouwbaarheidseisen voor deze systemen. Vaak is dit de manager bedrijfsvoering.

2.5. Rapportage

In de Tactische Baseline Informatiebeveiliging zijn voor de lijnmanager twee aandachtsgebieden in relatie tot informatiebeveiliging benoemd:

- De personeelsverantwoordelijkheid. De lijnmanager is verantwoordelijk voor het handhaven van de personele beveiliging met eventuele ondersteuning door Personeelszaken.
- De procesverantwoordelijkheid. De lijnmanager is verantwoordelijk voor het uitvoeren van activiteiten in processen op basis van de beschreven inrichting ervan. De verantwoordelijkheid voor de naleving van specifieke beveiligingsaspecten hangt af van het soort proces.

Personeelsverantwoordelijkheid

In elk beveiligingssysteem is de mens de zwakste schakel. Hoe zorg je ervoor dat deze (belangrijkste) schakel wordt versterkt? De inhoud van de functie bepaalt de eisen die in het kader van informatiebeveiliging aan (nieuwe) medewerkers worden gesteld. Wordt er gewerkt met geheim te houden gegevens? Is er sprake van kwetsbaarheden binnen de functie, bijvoorbeeld omgang met geld, of bestaat de mogelijkheid om toegangsrechten toe te kennen, te wijzigen of in te trekken? Gelden voor uitzendkrachten en ander tijdelijk personeel dezelfde criteria bij indiensttreding als bij vaste medewerkers? De eisen die aan medewerkers worden gesteld bepalen de maatregelen die bij de personele beveiliging worden getroffen. De lijnmanager weet welke rol de medewerker binnen de organisatie vervult en welke risico's aan die rol zijn verbonden.

Over het algemeen zal binnen een gemeente het personeelsbeleid generiek zijn beschreven en zullen algemene afspraken over maatregelen bij aanstelling, functiewijziging en vertrek van medewerkers zijn vastgelegd. De lijnmanager moet in overleg met de afdeling Personeelszaken en de CISO bepalen aan welke specifieke beveiligingseisen medewerkers eventueel aanvullend moeten voldoen.

Procesverantwoordelijkheid

Binnen elk informatiesysteem zijn beveiligingsmaatregelen noodzakelijk. De lijnmanager is verantwoordelijk voor de uitvoering van maatregelen op basis van de betrouwbaarheidseisen die voor het informatiesysteem gelden. Welke betrouwbaarheidseisen hierbij een rol spelen hangt af van het soort proces. Een mogelijk onderscheid van maatregelen in relatie tot informatiebeveiliging is het onderscheid in:

- *organisatorische* maatregelen, zoals het opstellen van informatiebeveiligingsbeleid en het benoemen van functies en verantwoordelijkheden, het inrichten van een incidentenregistratie en een meldingsprocedure, het opstellen van een calamiteitenplan en dergelijke. Organisatorische maatregelen hebben betrekking op de hele organisatie. Maatregelen op dit niveau moeten door de lijnmanager worden geaccepteerd en kunnen door hem niet buiten toepassing worden gelaten.

- *technische* maatregelen, waarbij geautomatiseerde controles worden aangebracht om de betrouwbaarheid, integriteit en vertrouwelijkheid van de gegevens conform een afgesproken beveiligingsniveau te beschermen. Daarnaast kan gedacht worden aan maatregelen om de bedrijfscontinuïteit te garanderen (back-up en uitwijkvoorzieningen). De lijnmanager bepaalt welk beschermingsniveau passend is op basis van de betrouwbaarheidseisen van het informatiesysteem. Uitvoering van deze maatregelen ligt veelal bij de ICT-afdeling of een externe dienstenaanbieder.

- *procedurele* maatregelen, die bestaan uit de inrichting van het bedrijfsproces op een zodanige manier dat de beschikbaarheid, integriteit en vertrouwelijkheid van informatie wordt gewaarborgd. De lijnmanager is onder andere verantwoordelijk voor het toepassen van een adequate functiescheiding om de betrouwbaarheidseisen te waarborgen.

- *fysieke* maatregelen, zoals de opslag van dossiers in een daartoe aangewezen bewaarplaats en niet langer dan gedurende een door de lijnmanager of op basis van regelgeving bepaalde termijn. Afspraken over het registreren en begeleiden van bezoekers naar beperkt toegankelijke ruimten zijn ook een voorbeeld van een fysieke maatregel die in overleg met de lijnmanager wordt genomen.

Ook als de uitvoering van maatregelen in relatie tot het informatiesysteem elders ligt, moet de lijnmanager op de hoogte zijn welke maatregelen getroffen zijn. Uiteindelijk bepaalt de lijnmanager welke restrisico's geaccepteerd worden na de implementatie van alle bovenstaande maatregelen.

2.6. Bewustwording en voorbeeldgedrag

Uit het dreigingsbeeld Nederlandse gemeenten[3] komt de factor mens als grootste risico naar voren. Mensen voeren handelingen uit, die bewust of onbewust bedreigingen veroorzaken voor de informatieveiligheid. Voorbeelden van bewust handelen zijn het opvoeren van niet bestaande gebruikers in een informatiesysteem of het uitvoeren van een verhuismutatie om een korting op een toeslag te voorkomen. Het onbewust handelen manifesteert zich bijvoorbeeld in het opschrijven van wachtwoorden om ze makkelijker te onthouden, of het onzorgvuldig omgaan met vertrouwelijke gegevens. Onbewuste en onbedoelde acties blijken een groter risico dan bewuste en gerichte aanvallen.

De lijnmanager heeft een belangrijke rol om onveilig gedrag van medewerkers te voorkomen. Dat uit zich in toezicht op naleving van regels en richtlijnen door medewerkers en het bevorderen van het beveiligingsbewustzijn van medewerkers. Maatregelen om het bewustzijn bij medewerkers te vergroten zijn bijvoorbeeld het hanteren van een gedragscode, waarin regels zijn vastgelegd voor een verantwoorde omgang met informatie en het benoemen van informatiebeveiliging als onderwerp tijdens werkoverleg en in functionerings- en beoordelingsgesprekken. Ook het hanteren van een clear desk- en clear screen-beleid is in het kader van informatiebeveiliging een belangrijk aandachtspunt.

Het toezicht op naleving van afspraken door medewerkers heeft uiteraard alleen zin wanneer de lijnmanager zelf voorbeeldgedrag vertoont en in zijn dagelijkse werkzaamheden tot uitdrukking brengt dat informatiebeveiliging serieus wordt genomen. De afspraken die voor medewerkers gelden, gelden onverkort ook voor de lijnmanager.

2.7. Wat als de lijnmanager geen verantwoordelijkheid neemt?

Maatregelen die worden getroffen in het kader van informatiebeveiliging zijn altijd een compromis tussen aan de ene kant de noodzaak een informatiesysteem te beschermen tegen dreigingen en aan de andere kant de zorg voor een ongestoorde bedrijfsvoering. Wanneer informatiebeveiliging te veel als taak van de CISO wordt beschouwd en de lijnmanager geen verantwoordelijkheid neemt voor informatiebeveiliging, kunnen beveiligingsdrempels worden opgeworpen die het werken onmogelijk maken. De lijnmanager heeft in dit opzicht de taak om het belang van een ongestoorde bedrijfsvoering in balans te brengen met de beveiligingsmaatregelen die vanuit het oogpunt van informatiebeveiliging worden voorgesteld.

Een lijnmanager die informatiebeveiliging ziet als integraal onderdeel van de bedrijfsvoering voorkomt dat het

[3] Bron: Dreigingsbeeld Nederlandse Gemeenten 2018

informatiesysteem uit de pas gaat lopen met risico's die de doelstellingen van het bedrijfsproces in gevaar brengen. Dreigingen die zich in de omgeving voordoen, moeten tijdig worden vertaald in beveiligingsmaatregelen. Het is de taak van de lijnmanager om die dreigingen te signaleren en zich bewust te zijn van de risico's die aan deze dreigingen verbonden zijn. Als CISO adviseert u de lijnmanager over beveiligingsmaatregelen voor deze risico's.

3. Risicomanagement

3.1. Inleiding

De implementatie van de BIG/BIO is een proces en geen eindpunt. De wereld staat niet stil en ook de gemeentelijke organisatie past zich aan. Het streven naar een kleinere en goedkopere overheid leidt tot een ruime toepassing van moderne technologie in de bedrijfsvoering. Het gemeentehuis is niet meer de vanzelfsprekende plek van waaruit de dienstverlening aan burgers plaatsvindt. Mobiel werken wordt meer regel dan uitzondering. De dynamiek van de ontwikkelingen in de omgeving van de gemeente is van invloed op het dreigingsbeeld waarop gemeentelijke organisaties zich moeten instellen. Deze dynamiek vereist een cyclische benadering van informatiebeveiliging (Plan, Do, Check, Act), waarin de actualiteit en volledigheid van de aanwezige beveiligingsmaatregelen regelmatig wordt vergeleken met de actuele dreigingen.

Risicomanagement is het regelmatig identificeren en beoordelen van risico's met betrekking tot de doelstellingen van het te beheren informatiesysteem. Door het regelmatig herhalen van risicoanalyses wordt een optimale aansluiting behouden tussen de dreigingen en de beveiligingsmaatregelen die voor het beheersen van de hiermee verband houdende risico's zijn getroffen.

3.2. Wanneer wordt een risicoanalyse uitgevoerd?

Een risicoanalyse is niet altijd noodzakelijk. Voor een deel van de gemeentelijke informatiesystemen is de implementatie van de baseline toereikend voor de bescherming van de in deze systemen vastgelegde informatie. Dat geldt niet voor een aantal vitale processen binnen de gemeente die aanvullende beveiligingsmaatregelen vereisen. Dat is bijvoorbeeld het geval wanneer er bijzondere of strafrechtelijke gegevens worden vastgelegd. Voor een ander deel van de informatiesystemen moet nog worden vastgesteld of de BIG/BIO toereikend is. Voor nieuwe processen en systemen is door het uitvoeren van een baselinetoets[4] op het proces te bepalen of het beveiligingsniveau van de BIG / BIO afdoende is of niet[5].

Aan het gesprek dat u als CISO voert met de lijnmanager over informatiebeveiliging gaan twee vragen vooraf, namelijk:

- Is er een baselinetoets uitgevoerd op de processen die tot de verantwoordelijkheid van de lijnmanager behoren? U moet er uiteraard wel zeker van zijn dat de BIG-maatregelen in relatie tot het informatiesysteem zijn getroffen.
- Zo ja, heeft de baselinetoets tot de conclusie geleid dat er in aanvulling op de BIG beveiligingsmaatregelen noodzakelijk zijn om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie te waarborgen?

De baselinetoets bestaat uit een aantal vragenlijsten. Deze zijn gericht op de betrouwbaarheidseisen waaraan een proces moet voldoen. De antwoorden op de vragen worden gewaardeerd met een cijfer. Op basis van het totaal van de antwoorden wordt duidelijk of de standaard beveiliging (BIG) voldoende is, of dat er een aanvullend onderzoek (diepgaande risicoanalyse) of een PIA (Privacy Impact Assessment) nodig is.

3.3. Betrouwbaarheidseisen

De betrouwbaarheidseisen waaraan een proces moet voldoen, worden uitgedrukt in niveaus voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie:

- **Beschikbaarheid**: hoeveel en wanneer data toegankelijk is en gebruikt kan worden.
- **Integriteit**: het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid).
- **Vertrouwelijkheid**: de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden.

De lijnmanager bepaalt het vereiste niveau voor deze betrouwbaarheidseisen voor de informatiesystemen waarvoor hij verantwoordelijk is. Er wordt onderscheid gemaakt in de niveaus Laag, Midden en Hoog. Daarmee wordt het

[4] In de BIO wordt gesproken van een 'Quickscan Information Security' (QIS). Hiermee wordt het basis beveiligingsniveau (BBN) vastgesteld. BBN2 is het middenniveau (qua niveau vergelijkbaar met de huidige BIG).
5 Zie BIG OP 'Baselinetoets BIG'

informatiesysteem en/of de data in het systeem geclassificeerd. Op GemmaOnline is een handreiking terug te vinden voor het classificeren van gemeentelijke gegevens.[6] Daarnaast is een overzicht beschikbaar van de beveiligingsniveaus, die aan gemeentelijke informatiesystemen zijn toegekend.[7] Aan de hand van de toegekende beveiligingsniveaus wordt duidelijk welke beveiligingseisen gelden en waar het zwaartepunt ligt binnen deze beveiligingseisen. Dat is de basis om te bepalen welke beveiligingsmaatregelen getroffen moeten worden.

De eerste stap bij het vaststellen van de betrouwbaarheidseisen is nagaan welke wet- en regelgeving mogelijk eisen stelt aan gebruik, distributie en opslag van data. De AVG bepaalt bijvoorbeeld dat er een passend niveau van technische en organisatorische maatregelen moet worden getroffen (artikel 32 AVG). Wat passend is, hangt af van de stand van de techniek, het te realiseren beveiligingsniveau en de inschatting van de lijnmanager van de risico's ten aanzien van het specifieke informatiesysteem.

De classificatie hoeft niet op elk informatiesysteem te worden uitgevoerd. Dit is alleen noodzakelijk als de verwachting bestaat dat voor een systeem de betrouwbaarheidseisen hoger zijn dan het beveiligingsniveau dat door implementatie van de BIG al aanwezig is.

Zoals hierboven aangegeven kan het beveiligingsniveau met behulp van een baselinetoets worden vastgesteld. Als u heeft vastgesteld dat voor een informatiesysteem de BIG niet toereikend is, moet een diepgaande risicoanalyse worden uitgevoerd voor dit systeem.

3.4. Diepgaande risicoanalyse

Doelstelling van de diepgaande risicoanalyse is om in kaart te brengen welke maatregelen aanvullend op de BIG moeten worden getroffen om het juiste niveau van beveiliging te realiseren. Uitgangspunt daarbij is dat de baselinetoets al volledig is uitgevoerd.

De diepgaande risicoanalyse bestaat uit drie hoofdstappen:

1. Het in kaart brengen van de onderdelen van de informatievoorziening conform het MAPGOOD model.
2. Het in kaart brengen van de dreigingen die relevant zijn voor het te onderzoeken informatiesysteem, met per dreiging de kans op optreden en de mogelijke schade.
3. Het vertalen van de meest relevante dreigingen naar maatregelen die moeten worden getroffen.

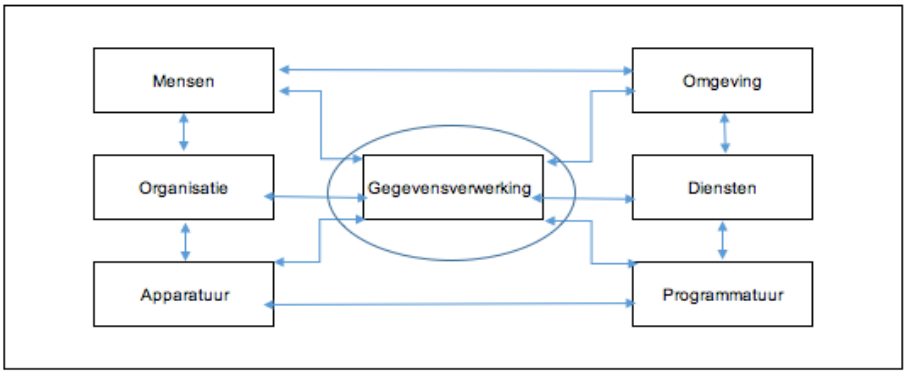
Het MAPGOOD-model

Het MAPGOOD-model gebruikt u om alle componenten van de informatievoorziening in kaart te brengen. Een informatiesysteem bestaat niet alleen uit een technische component. De afkorting MAPGOOD staat voor alle componenten waaruit een informatiesysteem bestaat, namelijk:

- **M**ensen, de mensen die nodig zijn om het informatiesysteem te beheren en te gebruiken
- **A**pparatuur, de apparatuur die nodig is om het informatiesysteem te laten functioneren
- **P**rogrammatuur, de programmatuur (applicatie) waaruit het informatiesysteem bestaat
- **G**egevens, de gegevens die door het systeem worden verwerkt
- **O**rganisatie, de organisatie die nodig is om het systeem te laten functioneren
- **O**mgeving, de omgeving waarbinnen het informatiesysteem functioneert
- **D**iensten, de externe diensten die nodig zijn om het systeem te laten functioneren

[6] https://www.gemmaonline.nl/index.php/Dataclassificatie
[7] https://www.gemmaonline.nl/index.php/Overzicht_BIV_classificaties_referentiecomponenten.

Figuur 1 Schematische weergave MAPGOOD-model



In kaart brengen van dreigingen

De lijnmanager die verantwoordelijk is voor het informatiesysteem, bepaalt ook de risico's die een ongestoorde voortgang van de werkzaamheden bedreigen.

Een dreiging is een kans op schade. Een dreiging wordt pas relevant als er sprake van is dat een kwetsbaarheid waarop de dreiging kan werken zich manifesteert in een beveiligingsincident. Een risico is de kans dat een bepaalde kwetsbaarheid of bedreiging resulteert in een daadwerkelijk incident. Bijvoorbeeld: de mogelijkheid dat een vliegtuig neerstort op het gemeentehuis is een dreiging, maar het risico dat dit daadwerkelijk gebeurt is niet groot.

Een risico is in het kader van informatiebeveiliging een ongewenste gebeurtenis die we willen voorkomen. Een risico is altijd meetbaar door de kans op het optreden van het incident in te schatten en af te zetten tegen de gevolgschade die dit incident kan veroorzaken. Deze vergelijking levert een bepaalde waarde op.

Figuur 2 Risicomatrix

		SCHADE		
		H	**M**	**L**
KANS	**H**	HH	H	M
	M	H	M	L
	L	M	L	LL

In een formule is het risico uit te drukken als: Risico = Kans x Schade.
In het voorbeeld van het vliegtuig is de kans dat het gemeentehuis getroffen wordt zeer klein, maar als het gebeurt zijn de gevolgen heel groot. Als de dreiging zeer klein wordt geacht, kan toch besloten worden om geen maatregelen te nemen. Dat besluit volgt uit de risicoanalyse.

Vertaling van dreigingen naar maatregelen

Bij de risicoanalyse wordt voor iedere bedreiging bepaald wat de kans op optreden is en welke impact daarbij hoort. Daarna wordt vastgesteld hoe met het vastgestelde risico wordt omgegaan. Elk risico kan op vier verschillende manieren tegemoet worden getreden, namelijk:

- door het risico te **accepteren**. In dat geval wordt het risico niet of slechts beperkt van invloed verklaard op het informatiesysteem. Het kan ook zijn dat de kosten die gemaakt moeten worden om het risico weg te nemen,

hoger zijn dan de mogelijke schade die ontstaat als het risico optreedt.

- door het risico te **vermijden**. Dat kan door het bedrijfsproces op een zodanige manier aan te passen dat een geïdentificeerd risico zich niet meer voordoet.
- door het risico te **verminderen**. In dit geval worden maatregelen genomen die de kans dat een bedreiging zich voordoet verminderen, of worden maatregelen genomen om de gevolgschade als het risico zich voordoet te beperken. Een voorbeeld van het verminderen van een risico is het plaatsen van een slot op de deur, wat de kans op onbevoegde toegang vermindert. Een voorbeeld van het beperken van gevolgschade is het plaatsen van een brandblusser in een opslagruimte.
- door het risico **over te dragen** aan een andere partij. Dat kan bijvoorbeeld door een verzekering af te sluiten, die de gevolgschade van het optreden van een risico dekt. Overdracht van het risico is ook mogelijk door het uitbesteden van de taak of dienst aan een externe partij.

De keuze uit deze risicostrategieën wordt per informatiesysteem gemaakt door de lijnmanager, binnen de grenzen van het gemeentelijke informatiebeveiligingsbeleid. Niet elk risico is uit te sluiten, want 100% veiligheid bestaat niet. Er zullen altijd restrisico's blijven bestaan. Het is wel van belang om de juiste keuzes te maken welke risico's wel en welke risico's niet worden geaccepteerd. Bij die keuzes speelt het belang van een ongestoorde voortgang van de bedrijfsvoering een rol. Uiteindelijk moet voor elke dreiging het restrisico door de lijnmanager geaccepteerd kunnen worden, omdat voldoende beveiligingsmaatregelen aanwezig zijn.

In het volgende hoofdstuk wordt een methodiek behandeld die u als CISO kunt gebruiken om samen met de lijnmanager op een verantwoorde wijze de risico's ten aanzien van een informatiesysteem in beeld te brengen, zodat de juiste beveiligingsmaatregelen kunnen worden genomen.

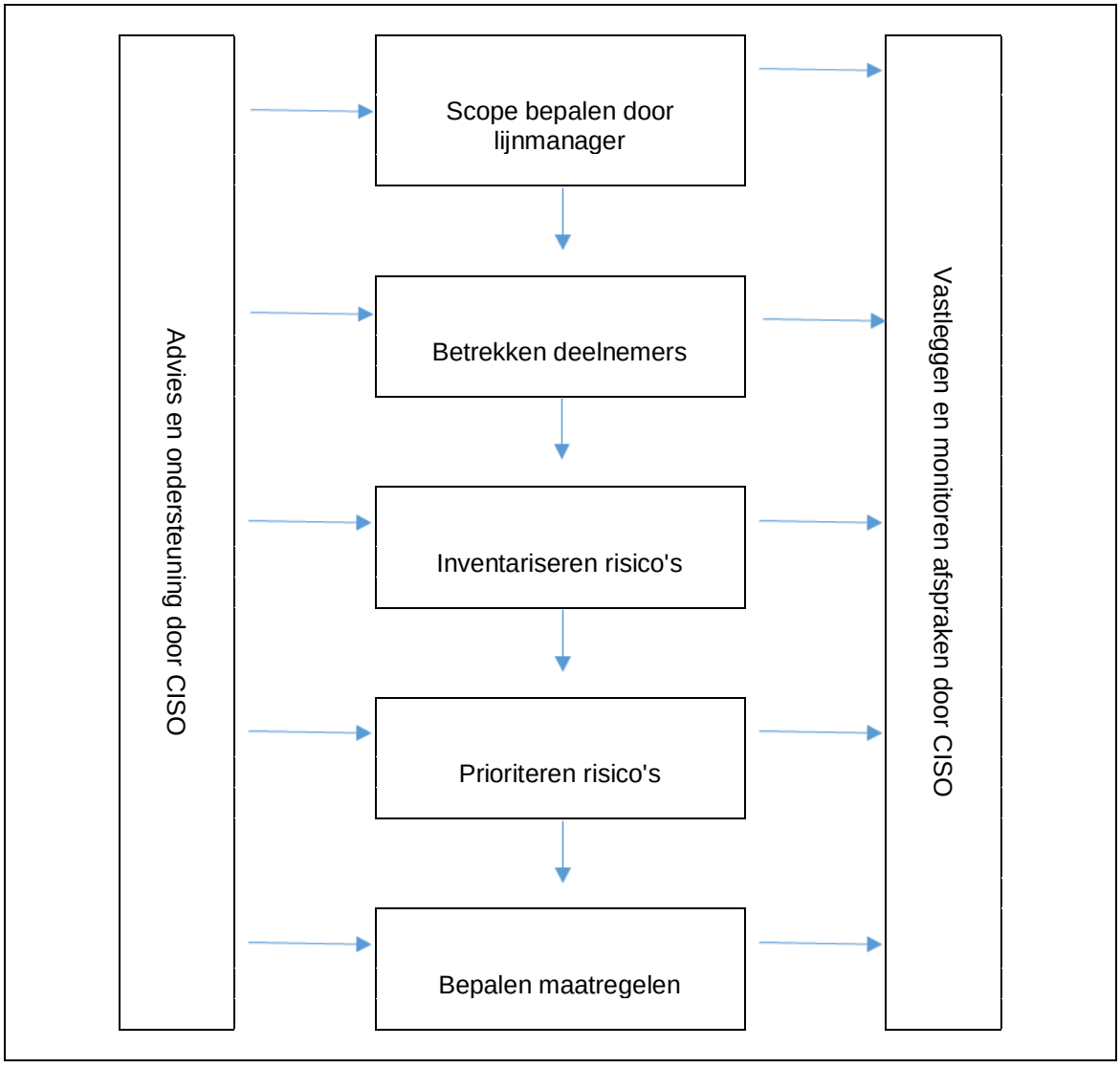
4. Uitvoeren risicoanalyse

4.1. Inleiding

Als CISO zorgt u voor de aanwezigheid van een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen uw gemeente. De lijnmanager bepaalt welke betrouwbaarheidseisen gelden voor de tot zijn verantwoordelijkheid behorende informatiesystemen. Bij een risicoanalyse wordt bepaald welke risico's van invloed zijn op de betrouwbaarheidseisen van die systemen. Doordat deze risico's per informatiesysteem kunnen verschillen, is het uitvoeren van één risicoanalyse die gericht is op de gehele organisatie niet voldoende. Een risicoanalyse zoals hier is beschreven voert u pas uit als de scores van de baselinetoets hiertoe aanleiding geven en duidelijk is dat de betrouwbaarheidseisen buiten de baseline vallen. De baselinetoets gaat dus altijd vooraf aan een meer diepgaande risicoanalyse.

Om de risico's van een specifiek informatiesysteem in beeld te brengen, moet een aantal stappen worden uitgevoerd. In dit proces heeft u als CISO een adviserende en ondersteunende rol. De uitkomsten van het proces legt u vast in het systeem dat u gebruikt om de beveiligingsmaatregelen binnen de gemeentelijke organisatie te monitoren.

Figuur 3 Stappen in de risicoanalyse



4.2. Scopebepaling

Het doel van de scopebepaling is om vast te stellen welke informatiesystemen worden meegenomen in de risicoanalyse. De lijnmanager is verantwoordelijk voor de uitvoering van een risicoanalyse binnen de scope van zijn verantwoordelijkheid. Hoe bepaalt de lijnmanager de scope van deze verantwoordelijkheid? Een mogelijkheid tot afbakening is de risicoanalyse te baseren op de referentiecomponenten in de GEMMA-architectuur.[8] Dan wordt bijvoorbeeld als scope voor de risicoanalyse het gemeentelijke gegevensmagazijn gekozen, of het Document Management Systeem (DMS). Een andere mogelijkheid is om een proces, een product of een dienst als uitgangspunt te nemen voor de scopebepaling. Als een product, dienst of proces als scope wordt gehanteerd, moet de risicoanalyse worden uitgevoerd op de daarbij behorende informatiesystemen. Uiteindelijk is het doel van de risicoanalyse om risico's in het kader van informatie vast te stellen.

Als CISO moet u op de hoogte zijn van de scope. U moet weten wie verantwoordelijk is voor het uitvoeren van de binnen de scope te treffen beveiligingsmaatregelen. Binnen de scope worden de risico's bepaald en de keuze van beveiligingsmaatregelen om met deze risico's om te gaan. Als CISO adviseert u en bewaakt u de afstemming van maatregelen binnen de hele gemeentelijke organisatie en ziet u toe op de afspraken die in relatie tot informatiebeveiliging zijn gemaakt. Generieke maatregelen worden doorgaans voor de hele organisatie genomen. Specifieke maatregelen zijn doorgaans van belang voor een bepaald informatiesysteem. De lijnmanager is binnen de scope van de specifieke maatregelen verantwoordelijk voor het accepteren van het restrisico, nadat afdoende maatregelen zijn getroffen. Pas nadat de scope van het informatiesysteem is bepaald, kijkt u naar de risico's voor dit systeem.

4.3. Wie nemen deel aan de risicoanalyse?

Voor het uitvoeren van een risicoanalyse is het belangrijk dat de juiste mensen hierbij betrokken worden. Dat zijn mensen die zicht hebben op de doelstellingen van het informatiesysteem en het belang van het systeem voor de organisatie. Daarnaast moet kennis vertegenwoordigd zijn over de uitvoering van het bedrijfsproces dat met het systeem wordt ondersteund. Proces- en systeemkennis is essentieel, maar betrek daarnaast ook mensen die direct de nadelen ondervinden als de betrouwbaarheidseisen onvoldoende gewaarborgd zijn. Bij de uitvoering van een risicoanalyse is het inschatten van de kans op een incident even belangrijk als de inschatting welke gevolgschade het incident veroorzaakt. In elk geval moet de voor de scope verantwoordelijke lijnmanager aanwezig zijn. Hij bepaalt uiteindelijk op basis van de uitkomst van de risicoanalyse welk restrisico wordt geaccepteerd.

Het uitvoeren van een risicoanalyse dient ondersteund te worden door een medewerker met ervaring bij het uitvoeren van risicoanalyses. Als u deze ervaring zelf niet heeft, is het aan te bevelen dat de gemeente hiervoor een medewerker aanstelt die deze risicoanalyses uitvoert en zo ervaring opbouwt. De nadruk ligt dan op procesbewaking. Maar ook op het stellen van controlevragen om de verschillende inschattingen tussen de deelnemers van de risicoanalyse te toetsen. Zoek hiervoor eventueel iemand bij een buurgemeente in de regio of huur expertise in.

4.4. Inventarisatie van risico's

Voor het inventariseren van risico's moet u eerst de dreigingen in beeld brengen. Per informatiesysteem kijkt u naar het belang van dit systeem voor de gemeentelijke organisatie en bepaalt u wat de impact is voor de organisatie als er een probleem ontstaat met de beschikbaarheid, integriteit en/of vertrouwelijkheid van het systeem en de daarin opgeslagen informatie. De dreigingen bespreekt u los van reeds genomen maatregelen. U gaat dus uit van een onbeveiligde situatie. Daarmee voorkomt u dat risico's verkeerd worden gewogen vanuit de veronderstelling dat de dreiging door tegenmaatregelen al is weggenomen.

8 Zie verder www.gemmaonline.nl

4.5. Prioriteren van risico's

U bepaalt per dreiging wat de kans is dat deze dreiging tot een incident leidt en wat de impact is die het incident op het informatiesysteem heeft. In de bijlage is een (niet uitputtend) overzicht9 opgenomen van de dreigingen per MAPGOOD-component. Met dit overzicht is prioriteit aan te brengen in de gesignaleerde risico's.

Hoewel de lijnmanager verantwoordelijk is voor de risico's binnen de vastgestelde scope van de risicoanalyse, kan een risico impact hebben op andere delen van de organisatie. Het is dus belangrijk om afspraken te maken over wie risico's mag accepteren en onder welke voorwaarden. Hiervoor kan de volgende beslisboom worden gehanteerd:

- Het risico raakt alleen het informatiesysteem binnen de scope: de lijnmanager mag de afweging maken om het risico te accepteren;
- Het risico raakt organisatiedelen buiten de scope: de directie moet de afweging maken of het risico acceptabel is;
- Het risico kan tot grote schade leiden: het accepteren van het risico is niet toegestaan.

Als CISO adviseert u de lijnmanager in de afweging om het risico te accepteren. Over het accepteren van risico's wordt jaarlijks verantwoording afgelegd richting de directie en het college. Bij het accepteren van een risico moet u altijd vaststellen voor welke termijn het risico geaccepteerd wordt.

4.6. Bepalen van maatregelen

De uitvoering van de risicoanalyse resulteert in een lijst van uit te voeren maatregelen. Deze maatregelen zijn te onderscheiden in generieke maatregelen, die voor de hele organisatie gelden, en maatregelen die specifiek voor het informatiesysteem van belang zijn en dus de expliciete verantwoordelijkheid zijn van de lijnmanager. De verantwoordelijkheid voor de uitvoering van de generieke maatregelen ligt meestal elders in de organisatie, maar bij de risicoanalyse moet u wel vaststellen of deze maatregelen ook inderdaad aanwezig zijn. In de tabel in de bijlage worden mogelijke dreigingen gekoppeld aan de beveiligingsmaatregelen van de BIG.

9 Je weet niet wat je niet weet, vandaar dat een overzicht nooit volledig kan zijn.

5. Naleving en verantwoording

5.1. Naleving

Maatregel 15.2.1.1 van de BIG legt de verantwoordelijkheid voor het naleven van beveiligingsprocedures expliciet bij de lijnmanager:

Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.

Als CISO ziet u toe op de naleving van afspraken die in het kader van informatiebeveiliging met de lijnmanager zijn gemaakt. U verantwoordt jaarlijks hierover richting het gemeentebestuur. Maar het is niet alleen voor u van belang dat de lijnmanager in de juiste positie komt te staan binnen de beveiligingsorganisatie van de gemeente. De lijnmanager is ook verantwoordelijk voor het borgen van privacy in de gegevensverwerkende processen en het naleven van de in de Algemene Verordening Gegevensbescherming (AVG) vastgelegde voorschriften. De Functionaris Gegevensbescherming (FG) speelt namens de Autoriteit Persoonsgegevens (AP) een toezichthoudende rol in de gemeentelijke organisatie.

Het is aan te raden dat u als CISO afspraken met de FG maakt hoe u inzicht krijgt in opzet, bestaan en werking van beveiligingsmaatregelen. Verantwoording van maatregelen vereist zowel binnen de scope van de AVG als in relatie tot de BIG een Plan-Do-Check-Act-cyclus, die ervoor zorgt dat de gemeente blijft voldoen aan de AVG en de BIG.

Veel maatregelen die nodig zijn voor het voldoen aan de AVG vallen samen met de beveiligingsmaatregelen die in het kader van de BIG zijn geïmplementeerd. Uitbesteding van gegevensverwerkingen aan derden vereist bijvoorbeeld zowel in het kader van de AVG als in het kader van de BIG dat verwerkersovereenkomsten worden gesloten met verwerkers. Voor een lijnmanager is het vervelend als hij dezelfde maatregel tegenover twee verschillende functionarissen moet verantwoorden. Probeer daarom afspraken te maken met de FG van uw gemeente om gezamenlijke controlemomenten in te bouwen in de planning- en control-cyclus van de gemeente. Zorg dat u ook afstemming zoekt met de Security Officer Suwinet en de Beveiligingsfunctionaris Reisdocumenten binnen uw organisatie. Zij hebben vanuit hun rol binnen specifieke domeinen ook een belangrijke taak in het toezicht op beveiligingsmaatregelen.

5.2. Verantwoording

Jaarlijks moet verantwoording worden afgelegd over de beveiligingsmaatregelen in het kader van ENSIA[10], waarmee informatiebeveiliging aandacht krijgt van het gemeentebestuur en de rijksoverheid.
ENSIA staat voor de Eenduidige Normatiek Single Information Audit. Het doel van ENSIA is het ontwikkelen en implementeren van een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid. De focus van ENSIA ligt op de horizontale verantwoording: binnen de gemeente, met een belangrijke rol voor de gemeenteraad. ENSIA helpt gemeenten in één keer verantwoording af te leggen over informatieveiligheid gebaseerd op de BIG. Met ENSIA sluit de verantwoording over informatieveiligheid aan op de planning en control-cyclus van de gemeente. Hierdoor heeft het gemeentebestuur meer overzicht over de informatieveiligheid van hun gemeente en kan het beter sturen en verantwoording afleggen aan de gemeenteraad. ENSIA structureert ook de verticale verantwoording richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI).

Uitgangspunt voor de verantwoording is het horizontale verantwoordingsproces aan de gemeenteraad. Dit vormt de basis voor het verticale verantwoordingsproces aan nationale partijen die een rol hebben in het toezicht op informatieveiligheid. Bij het afleggen van verantwoording wordt het principe van single information single audit toegepast; alle informatie die noodzakelijk is voor verticale verantwoording is ook onderdeel van het horizontale verantwoordingsproces.

[10] www.ensia.nl

In ENSIA zijn beveiligingsmaatregelen die voortkomen uit de BIG en aanvullende eisen, die voortkomen uit sectorale regelgeving (de zogenaamde domeinspecifieke vragen), samengevoegd in een vragenlijst. Elke gemeente heeft een ENSIA-coördinator benoemd, die zorg draagt voor het invullen en aanleveren van de ENSIA-vragenlijst en het opstellen van de collegeverklaring Informatiebeveiliging en Assurance.

De beantwoording van de vragen is een primaire verantwoordelijkheid van het lijnmanagement. Met name de domeinspecifieke vragen vereisen kennis van het uitvoerende proces die in de regel niet aanwezig is bij de ENSIA-coördinator.

Bijlage: MAPGOOD-risico's

Toelichting op de tabel

In de eerste twee kolommen worden dreigingen en de mogelijke incidenten die hieruit voortkomen weergegeven. In de volgende kolom wordt aangegeven of de dreiging zich voordoet op het niveau van de organisatie (G = generiek), op het niveau van het informatiesysteem (S = specifiek), of op beide niveaus (G/S = zowel generiek als specifiek). Dit niveau bepaalt waar de verantwoordelijkheid voor het restrisico ligt:

G = directieniveau
S = lijnmanager
G/S = gedeelde verantwoordelijkheid. Het probleem dat personeel kan uitvallen doet zich bijvoorbeeld binnen de hele organisatie voor en vraagt om generieke maatregelen, die vastgelegd zijn in het gemeentelijke personeelsbeleid (inhuur van uitzendkrachten, gebruik van een flexibele schil e.d.). Daarnaast is er een specifieke verantwoordelijkheid van de lijnmanager om de continuïteit van de bedrijfsvoering binnen zijn organisatieonderdeel te waarborgen door voldoende medewerkers met het juiste functieniveau aan te stellen. De dreiging van personeelsuitval vraagt dus om zowel generieke maatregelen als specifieke maatregelen. Voorafgaand aan het gesprek met de lijnmanager moet u eerst een beeld hebben van de generieke maatregelen die binnen de organisatie getroffen zijn, waarna u met de lijnmanager de aanvullende maatregelen bepaalt om het restrisico te kunnen accepteren.

De impact van een beveiligingsincident op het informatiesysteem wordt berekend door de kans op het optreden van dit incident (binnen een periode van een jaar) te vermenigvuldigen met de schade die het incident mogelijk veroorzaakt. De impact bepaalt de prioriteit bij het treffen van beveiligingsmaatregelen. In de volgende kolom is aangegeven waar in de BIG de specifieke maatregelen zijn beschreven. Tenslotte geeft u in de laatste kolom aan of er aanvullende maatregelen noodzakelijk zijn. U kunt gebruik maken van de vragenlijsten, die aan de handreiking dataclassificatie zijn toegevoegd, om het antwoord op deze vraag voor de betrouwbaarheidsaspecten integriteit en vertrouwelijkheid te bepalen.

Bedreigingen per groep		Niveau	KANS	SCHADE	IMPACT	specifieke BIG maatregel nummer	aanvullende maatregelen noodzakelijk?
Mensen	**Incident**		**L/M/H**	**L/M/H**	**Kans* Schade**		**Ja/Nee**
Uitvallen	Voorzienbaar (ontslag, vakantie)	G/S				H8, H14.1.1	
	Onvoorzienbaar (ziekten, overlijden, ongeval, staking)	G/S				H8, H14.1.1	
Onopzettelijke foutief handelen	Onkunde, slordigheid	G/S				H8.2.2, H8.2.3	
	Foutieve procedures	G/S				H5.1.1, H6.1, H15.2.1	
	Complexe foutgevoelige bediening	G/S				H10.1	
	Onzorgvuldige omgang met wachtwoorden	G/S				H11.3.1, H7.1.3, H8.2.2, H8.2.3	
	Onvoldoende kennis/training	G/S				H8.2.2	
Opzettelijke foutief handelen	Niet werken volgens voorschriften/procedures	G/S				H8.2.2, H8.2.3, H10.1.1	
	Fraude/diefstal/lekken van informatie	G/S				H8.1.1, H8.1.2, H8.2.2, H8.2.3, H13	
	Ongeautoriseerde toegang met account van medewerker met hogere autorisaties	G/S				H7.1.3, H8.2.2, H8.2.3, H10.10.2, H11.1.1, H11.3.1	

Apparatuur	Incident		L	H	Ja/Nee		
Spontaan technisch falen	Veroudering/slijtage	G/S				H7.1.1, H9.2.4, H14.1.2	
	Storing	G/S				H7.1.1, H9.2.4, H13, H14.1.2	
	Ontwerp/fabricage/installatie-onderhouds fouten	G/S				H9.2.4, H10.1.2, H12.1.1, H12.5.1, H12.5.2	
Technisch falen door externe invloeden	Stroomuitval	G				H9.1.4, H9.2.1 t/m 5, H14.1.2	
	Slechte klimaatbeheersing, thermische straling	G				H9.1.4, H14.1.2	
	Nalatig onderhoud door schoonmaak	G				H9.1.4, H14.1.2	
	Elektromagnetische straling	G				H9.1.4, H14.1.2	
	Elektrostatische lading	G				H9.1.4, H14.1.2	
	Diefstal/schade	G				H9.1.1 & 2	
	stof, corrosie	G				H9.1.4 & 5, H9.2.1, H9.2.4, H14.1.2	
Menselijk handelen/falen	Bedieningsfouten	G				10.1.1	
	Opzettelijke aanpassingen/sabotage	G/S				H9.1.1 t/m 3	
	Beschadiging/vernieling	G/S				H9.1.1 t/m 3	
	Verlies/diefstal (onder andere van USB-sticks)	G/S				H9.1.1 t/m 3, H10.7, H10.8.3, H11.7.1	
	Verwijdering van onderdelen waardoor storingen ontstaan	G/S				H9.1.1 t/m 3	

Programmatuur	Incident		L	H	Ja/Nee		
Nalatig menselijk handelen	Ontwerp-, programmeer-, invoering, beheer / onderhoudsfouten	G				H10.1.1 & 2, H12.5.1 &2	
	Introductie van virus en dergelijke door gebruik van niet gescreende programma's	G/S				H7.1.3, H8.2.2, H10.4, H11.2.2, H12.6.1	
	Gebruik van de verkeerde versie van programmatuur	G/S				H10.1.1 & 2, H12.5.1 &2	
	Slechte documentatie	G/S				H10.1.1	
Opzettelijk menselijk handelen	Manipulatie voor of na ingebruikname	G/S				H12.5.3	
	(Ongeautoriseerde) functieverandering en/of toevoeging	G/S				H12.5.3	
	Installatie van virussen, Trojaanse paarden en dergelijke	G/S				H10.4, H11.2.2, H12.6.1	
	Gebruiken van autorisaties van collega's	S				H10.10, H11.1.1, H11.2.3, H11.3.1	
	Illegaal kopiëren van programmatuur	G/S				H7.1.3, H8.2.3, H15.1.2	
	Oneigenlijk gebruik of privé gebruik van bedrijfs programmatuur	S				H7.1.3, H8.2.3, H15.1.2, H15.1.5	
Onopzettelijk menselijk handelen	Fouten door niet juist volgen van procedures	S				H8.2.2, H10.1.1	
	Installatie van malware en virussen door gebruik van hoge autorisaties bijvoorbeeld door gebruik van admin-account tijdens het browsen van websites.	G/S				H10.4, H11.2.2, H12.6.1	
Technische fouten/mankementen	Fouten in code programmatuur die de werking verstoren	G				H12.4.1, H12.5.1 & 2	
	Achterdeuren in programmatuur voor (onbevoegde) toegang	G				H11.4.4, H12.6.1	
	Bugs/fouten in code die tot exploits kunnen leiden	G				H12.6.1	

Gegevens/data	Incident		L	H	Ja/Nee		
Via gegevensdragers (CD/DVD/ USB-ticks/ Harddisk/ Back-ups	Diefstal/zoekraken/lekken	G/S				H9.1.1 t/m 3, H10.7, H10.8.3, H11.7.1	
	Beschadiging door verkeerde behandeling	G/S				H10.1.1, H10.5.1	
	Niet overeenkomende bestandformaten	G/S				H10.1.1, H10.8	
	Foutieve of geen versleuteling	G/S				H7.2, H12.3.1	
	Foutieve of vervalste identificatie van ontvangers om aan gegevens te komen	G				H8.2.2, H10.1.1, H10.8.2	
	onvoldoende storage, buffer overflow	G				H10.3.1, H10.5.1	
Via Cloud voorzieningen	Ongeautoriseerde toegang door onbevoegden (hackers/hosters)	G				H8.2.2, H10.4, H10.10, H12.3.1, H13	
	Ongeautoriseerde wijziging of verwijdering van gegevens (hacking)	G				H8.2.2, H10.4, H10.10, H12.3.1, H13	
via Netwerk voorzieningen	onbeveiligd netwerkverkeer	G				H10.6, H11.4.5, H12.3.1	
	ontbreken / onvoldoende logging en audit trails	G				H10.10	
	falende identificatie en authenticatie procedures en mechanismen	G				H11.1 T/M 4, H11.5	
	falend wachtwoordbeleid en management	G				H11.3.1, H11.5	
	onvoldoende verificatie ontvangst en verzenden berichten verkeer	G				H10.8.1, 2 & 4, H12.2.2	
Via apparatuur	Fysieke schrijf- of leesfouten	G				H10.1.2, H10.5, H10.10.1, H12.2	
	Onvoldoende toegangsbeperking tot apparatuur	G				H9.2.1, H10.6, H10.10, H11.4, H12.6.1	
	Fouten in interne geheugens	G				H10.5.1, H10.10	
	Aftappen van gegevens	G				H9.2.4, H10.6, H10.8.4, H10.10, H11.4, H12.3	
	retrieval of recycled or discarded media	G				H9.2.6, H10.7.2	

Via programmatuur	Foutieve of gemanipuleerde programmatuur	G				H10.4, H12.5, H12.6, H13	
	Doorwerking van virussen/malware	G				H10.4, H12.5, H12.6, H13	
	Afbreken van verwerking (w.o. DDOS)	G				H14	
Via personen	(On)opzettelijke foutieve gegevensinvoer, -verandering of –verwijdering van data	S				H10.1.1, H10.10, H10.5, H12.2.1	
	Onbevoegde toegang door onbevoegden (hackers en dergelijke via malware)	G				H8.2.2, H10.4, H10.10, H12.3.1, H13	
	Onbevoegd kopiëren van gegevens	S				H8.2.2, H10.10, H11.6.2, H12.3.1, H13	
	Meekijken over de schouder door onbevoegden	G/S				H8.2.2, H11.3.1, H11.5.1, H11.5.2, H11.5.5 & 6	
	Onzorgvuldige vernietiging (laten liggen op printer)	S				H8.2.2, H11.3.3	
	Niet toepassen clear screen/clear desk	S				H8.2.2, H11.3.3	
	Aftappen (draadloos) netwerk door onbevoegden (telewerk situaties)	S				H7.1.3, H8.2.2, H11.7	
	Oneigenlijk gebruik van autorisaties	S				X	
	Toegang verschaffen door middel van identiteitsfraude of social engineering	S				H8.2.2, H11.4.2	
	Data afkomstig uit onbetrouwbare bronnen	G				H12.2.1	
	Onzorgvuldig vernietigen van gegevens	G/S				H8.2.2, H9.2.6, H10.7.2, H13	

Organisatie	Incident		L	H	Ja/Nee		
Gebruikers-organisatie	Mismanagement	G/S				H5, H6.1, H8.2	
	Gebrekkige toedeling taken, bevoegdheden, verantwoordelijkheden	G/S				H5, H6.1, H8.2	
	Onduidelijke of ontbrekende gedragscodes	G/S				H5.1, H7.1.3, H8.2, H10.1.1 t/m 3	
	Afwezige, verouderde of onduidelijke handboeken	G/S				H10.1.1	
	Systeemdocumentatie / werkprocedures/ gebruiksinstructies	G/S				H10.1.1	
	Onvoldoende interne controle	G/S				H15.2	
	Onvoldoende toetsing op richtlijnen	G/S				H15.2	
	Onvoldoende of geen contractbeheer	G/S				H6.2.2, H10.2	
	Ontbrekende dienstverleningsovereenkomsten	G/S				H6.2.2, H10.2	
	Gebrekkige doel/middelen beheersing	G/S				H61.1 t/m 3, H8.2.1	
Beheerorganisatie	Gebrekkig beleid betreffende beheer	G				H1O.1.1	
	Onvoldoende kennis of capaciteit	G/S				H8.2.2, H10.1.1	
	Onvoldoende kwaliteitsborging	G/S				H10.1.1	
	Onvoldoende beheer van systemen en middelen (ICT-Atlas)	G				H7.1.1 & 2	
Ontwikkelings-organisatie	Slecht projectmanagement	G				H12..1, H12.4.1, H12.5	
	Niet volgen van projectenkalender of PPM	G				H12.1.1	
	Geen ontwikkelrichtlijnen en/of – procedures	G				H12..1, H12.4.1, H12.5	
	Er worden geen methoden/technieken gebruikt	G				H12..1, H12.4.1, H12.5	
	Gebrek aan planmatig werken	G				H12.1.1	

Omgeving	Incident		L	H	Ja/Nee		
Buitengebeuren	Natuurgeweld (overstroming, blikseminslag, storm, aardbeving et cetera)	G				H9.1.4, H10.5.1, H13, H14	
	Overig geweld (oorlog, terrorisme, brandstichting, inbraak, neerstortend vliegtuig, galactische oorlogsvoering)	G				H9.1.4, H10.5.1, H13, H14	
	Blokkade/staking	G					
	Onveilige, geblokkeerde, vluchtwegen bij brand	G				H9.1.3, H13, H14	
Nutsvoorzieningen	Uitval van elektriciteit, water, telefoon, dataverbindingen (w.o. SPOF's)	G				H9.2.2 & 3, H10.5.1, H13, H14	
	Wateroverlast door lekkage, bluswater	G				H9.1.4, H10.5.1, H13, H14	
	Uitval van licht-, klimaat- en/of sprinklerinstallatie	G				H9.2.2, H10.5.1, H13, H14	
Huisvesting	Ongeautoriseerde toegang tot gebouw(en)	G/S				H9.1	
	Diefstal op werkplekken	G/S				H9.1.1 t/m 3	
	Gebreken in ruimtes, waardoor kans op insluiping/inbraak	G				H9.1.1 t/m 3	
	Onvoldoende fysieke voorzieningen om te vluchten of in te grijpen tijdens geweldsdreigingen/conflicten met klanten	G				H9.1.3	
	brand, verontreiniging					H9.1.3	

Diensten	Incident		L	H	Ja/Nee		
Diensten dienstverlener definitief niet meer te leveren	Een dienstverlener gaat failliet	G/S				H6.2.1 & 3, H10.2	
	Opzegging diensten door dienstverlener	G/S				H6.2.1 & 3, H10.2	
Diensten dienstverlener tijdelijk niet beschikbaar	Levert diensten niet conform overeenkomst	G/S				H6.2.1 & 3, H10.2	
	Onderbreking dienstverlening door overname dienstverlener	G/S				H6.2.1 & 3, H10.2	
	Kan diensten tijdelijk niet uitvoeren door zaken buiten de eigen controle (stakingen en dergelijke.)	G/S				H6.2.1 & 3, H10.2	
	Past verkeerde prioriteiten toe in klantbejegening	G/S				H6.2.1 & 3, H10.2	
	Levert onvoldoende capaciteit voor een goede dienstverlening	G/S				H6.2.1 & 3, H10.2	
Diensten worden niet conform afspraak geleverd	Slecht opgeleid personeel	G/S				H6.2.1 & 3, H10.2	
	Groot personeelsverloop	G/S				H6.2.1 & 3, H10.2	
	Onvoldoende capaciteit in personeel	G/S				H6.2.1 & 3, H10.2	
	Valse verklaringen over certificeringen	G/S				H6.2.1 & 3, H10.2	
	Onvoldoende of geen kwaliteitsborging	G/S				H6.2.1 & 3, H10.2	
	Personeel voldoet niet aan eisen zoals geldig VOG en geheimhoudingsverklaringen	G/S				H6.2.1 & 3, H10.2	
	Voert wanbeheer, slordigheden in beheersactiviteiten,	G/S				H6.2.1 & 3, H10.2	
	Werkt niet conform ITIL of BiSL-principes	G/S				H6.2.1 & 3, H10.2	
	Maakt misbruik van toevertrouwde gegevens, applicaties en documentatie	G/S				H6.2.1 & 3, H10.2	
	Houdt zich niet aan functiescheiding	G/S				H6.2.1 & 3, H10.2	
	Maakt gebruik van te zware autorisatie, niet functie gebonden	G/S				H6.2.1 & 3, H10.2	

INFORMATIE
BEVEILIGINGS
DIENST

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