Impactanalyse Informatiebeveiliging Publicatieversie

Provinciebrede impactanalyse voor ISO 27001 certificering

Provincie Zeeland

Impactanalyse Informatiebeveiliging Publicatieversie

Provinciebrede impactanalyse voor ISO 27001 certificering

Datum:	7 december 2017
Auteur:	Werkgroep Informatiebeveiliging
Versienummer:	1.2
Classificatie	Openbaar

Inhoudsopgave

Voorwoord

Inleiding

Informatie is één van de voornaamste bedrijfsmiddelen van de Provincie Zeeland. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan gevolgen hebben voor de bedrijfsvoering, maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met mogelijk ook politieke consequenties, economische schade of zelfs dodelijke ongevallen. De Provincie is verantwoordelijk voor de informatie die zij verwerkt en moet hier zorgvuldig en veilig mee omgaan. Stel je voor dat er informatie van en over burgers weglekt en dat dit leidt tot schending van privacy. Of dat onbevoegden toegang krijgen tot de bediening van bruggen en sluizen, waardoor ernstige ongelukken kunnen gebeuren. Dit moet ten alle tijde worden voorkomen door het treffen van passende maatregelen.

Dit document betreft een impactanalyse voor informatiebeveiliging voor de komende jaren. Doel is, in lijn met de interprovinciale afspraken, om in 2021 te voldoen aan het basisniveau informatiebeveiliging, namelijk dat we dan gereed zijn voor ISO 27001 certificering. Momenteel voldoen we daar niet aan en hier dient de Provincie naar toe te groeien gedurende de komende jaren. Dat betekent dat in 2021 alle geïnventariseerde acties gereed moeten zijn. De acties zijn terug te herleiden tot de drie pijlers van informatiebeveiliging: integriteit, beschikbaarheid en vertrouwelijkheid.

Op basis van deze impactanalyse wordt een aanbesteding gestart om externe expertise in te schakelen. Deze externe partij gaat de werkgroep Informatiebeveiliging begeleiden bij het traject om provinciebreed over vier jaar ISO 27001 gecertificeerd te zijn. De aanpak hiervoor is als volgt:

- Een eerste stap is het uitvoeren van een marktverkenning met als doel om in beeld te brengen wat de omvang van het werk betreft, een inschatting van benodigde investering en welk partijen in aanmerking komen voor de aanbesteding. *Planning: februari 2018 gereed*
- Daarna wordt conform interprovinciale afspraken een 0-meting uitgevoerd door een externe partij die dit voor alle provincies gaat doen. *Planning: april 2018 gereed*
- Vervolgens starten we een aanbesteding voor meerjarige begeleiding om eind 2021 ISO 27001 gecertificeerd te zijn. *Planning: september 2018 gereed*

1. Onderwerp en toepassingsgebied

Deze impactanalyse is gebaseerd op de internationale breed toegepaste norm voor informatiebeveiliging ISO 27001. Deze norm levert een methode voor de invoering en beheersing van informatiebeveiliging en stelt organisaties in staat zich te certificeren.

2. Normatieve verwijzingen

Om de veiligheid van informatie te kunnen waarborgen dienen we te voldoen aan een zogenaamd basisniveau informatiebeveiliging. Provincies hebben gezamenlijk in 2014 het Convenant Interprovinciale Regulering Informatieveiligheid ondertekend waarin het basisniveau informatieveiligheid is afgesproken. De Interprovinciale Baseline Informatiebeveiliging (IBI) met als basis de ISO27001/2 is hiervoor het vastgestelde normenkader. Op dit moment wordt gewerkt een opvolger hiervan, namelijk. een landelijke Baseline Informatiebeveiliging Overheid (BIO). Er is een conceptversie beschikbaar waaruit blijkt dat deze in de praktijk beter bruikbaar is dan de huidige Interprovinciale Baseline en naadloos aansluit op de ISO 27001/2 standaard.

De standaarden NEN-ISO/IEC 27001 en 27002 zijn een vertaling van de internationale normen ISO/IEC 27001 en 27002.

De NEN-ISO/IEC 27001-standaard bevat eisen waar het managementsysteem voor informatiebeveiliging aan dient te voldoen. Het is deze norm waartegen wordt geaudit bij certificering. Deze standaard specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's van een organisatie.

De NEN-ISO/IEC 27002 (verkort ISO27002) standaard is een "best practice" van beveiligingsmaatregelen ('controls') om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. Deze standaard kan gezien worden als een nadere uitwerking van de NEN-ISO/IEC 27001, bijlage A. De ISO27002 geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiligingsmaatregelen binnen een organisatie. De ISO27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en als effectieve methode voor het bereiken van deze veiligheid.

Interprovinciaal ligt er inmiddels een afspraak dat elke provincie binnen 5 jaar ISO 27001 gecertificeerd is en blijft. Dit is een belangrijke stip op de horizon waar elke provincie naar toe werkt. Iedere provincie is en blijft zelf verantwoordelijk voor de eigen implementatie, wel biedt dit kansen om nauw samen te werken aan gezamenlijke producten.

Naast de eisen vanuit de ISO 27001 verwijzen we naar de eisen vanuit de Algemene Verordening Gegevensbescherming. Deze wetgeving is per 25 mei 2018 zodanig van toepassing dat er ook toezicht door de Autoriteit Persoonsgegevens wordt uitgeoefend.

3. Termen en definities

<Dit hoofdstuk wordt nog ingevuld in een vervolgversie van dit document>.

4. Context van de organisatie

4.1. De organisatie en haar context

Voor uitvoering van de acties rond informatiebeveiliging is het van belang om per werkproces of taak de informatievragen helder te krijgen rond integriteit, vertrouwelijkheid en beschikbaarheid. Van belang is dat de provinciale organisatie in beeld heeft wat haar doelstellingen zijn voor de komende vier jaar en welke kerntaken & werkprocessen hieraan gekoppeld zijn.

Actie:

- *Inventariseren van de doelstelling, kerntaken en werkprocessen van de Provincie Zeeland voor de komende vier jaar.*

4.2. Behoeften en verwachtingen van belanghebbenden

Van belang is om zo volledig mogelijk in kaart te brengen wat de belanghebbenden (stakeholders) zijn van de provinciale organisatie en wat de eisen zijn die zij stellen aan informatiebeveiliging van de provincie voor hetgeen zij van de organisatie afnemen. Dat is per werkproces naar alle waarschijnlijkheid verschillend. Een proces met geheime informatie vraagt meer dan werk met alleen openbare informatie. Voorbeelden van stakeholders zijn: burgers, bedrijven, andere overheden, leveranciers. Vanuit de provinciale architectuur is hiervoor reeds in het verleden een aanzet gedaan om dit schematisch in beeld te brengen.

Acties:

- *Actualiseren van het context diagram en aanvullen met datastromen en eisen vanuit stakeholders voor informatiebeveiliging*
- *Context diagram en aanvullende informatie formeel laten vaststellen door directie en GS, dit overzicht jaarlijks actualiseren*
- *Op basis van het contextdiagram per informatiestroom de classificatie & vereisten helder maken.*

4.3. Toepassingsgebied voor informatiebeveiliging

Informatiebeveiliging is enerzijds van toepassing op de interne provinciale organisatie, anderzijds op de externe rol die de Provincie Zeeland heeft in het kader van haar stakeholders. Belangrijk is dat de Provincie Zeeland in alle gevallen een aantoonbare betrouwbare organisatie is voor zowel haar medewerkers als externe belanghebbenden. Van belang is om dit toepassingsgebied te formuleren en formeel vast te laten stellen door directie.

Actie:

- *Formuleren van het toepassingsgebied en formeel laten vaststellen door directie.*

4.4. Managementsysteem voor informatiebeveiliging

Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de overheid. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Deze procesbenadering (PDCA) wordt in de ISO 27001 norm ook wel het managementsysteem voor informatiebeveiliging genoemd. Het uitgangspunt is dat we in de komende jaren langs deze lijn toewerken naar een basisniveau voor informatiebeveiliging zodat we hieraan in 2021 aantoonbaar (via certificering) kunnen voldoen. Dit betekent dat we dan het volgende geregeld dienen te hebben:

- Beleid, rollen en verantwoordelijkheden rondom informatiebeveiliging actualiseren aan de hand van de nieuwe vereisten en vaststellen;
- Inzicht in de bedrijfskritische processen, informatiesystemen en gegevens en koppelen aan eigenaarschap;
- Inzicht in de impact op beschikbaarheid, integriteit, vertrouwelijkheid en privacy binnen de werkprocessen en specifiek bij bedrijfskritische processen en beleggen van de verantwoordelijkheden hiervoor;
- Technische en organisatorische basismaatregelen genomen voor alle processen in het algemeen (net als thuis: ‘in elk geval ervoor zorgen dat de deur op slot zit’);
- Risico’s van de bedrijfskritische processen ingeschat, extra passende beheersmaatregelen hiervoor genomen (net als thuis: ‘gevoelige informatie opbergen in de kluis en ervoor zorgen dat het niet in verkeerde handen komt’) en verantwoordelijkheden belegd en gedocumenteerd;
- Plan Do Check Act cyclus (continu verbeterproces) ingeregeld voor alle noodzakelijke maatregelen;
- Bewustzijn rondom informatieveiligheid bij bestuur, management en medewerkers;
- Tijdig de impact ingeschat voor de te nemen maatregelen en hierover communiceren;
- Regelmatige interne en externe audits inregelen.

Acties:

- *In 2018 een interprovinciale 0-meting uitvoeren naar stand van zaken informatiebeveiliging op basis van ISO 27001 norm*
- *Monitoren effectiviteit maatregelen van de getroffen maatregelen en bij verminderde effectiviteit de maatregelen aanpassen of uitbreiden*
- *Implementeren managementsysteem informatiebeveiliging volgens ISO 27001 gedurende de jaren 2018 t/m 2021*
- *In 2020 een interprovinciale 1-meting uitvoeren naar stand van zaken informatiebeveiliging op basis van ISO 27001 norm*
- *Eind 2021 certificering volgens ISO 27001 norm regelen voor Provincie Zeeland*

5. Leiderschap

5.1. Leiderschap en betrokkenheid

Een ander onderwerp uit de ISO norm informatiebeveiliging is leiderschap, met ook specifieke aandachtsvelden. Belangrijk is dat directie en GS leiderschap en betrokkenheid tonen en blijven vasthouden bij de verbeteringen en het bijbehorende (verplichte)het managementsysteem voor informatiebeveiliging (PDCA cyclus en continu verbeteren). Dit betekent dat zij actief betrokken blijven bij het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van informatiebeveiliging binnen de organisatie:

a) het formulieren van de strategie bij de invoering van verbeteracties & het managementsysteem voor informatiebeveiliging om voortgang & risico's te meten;
b) het vaststellen van het informatiebeveiligingsbeleid en het jaarlijkse informatiebeveiligingsplan;
c) het vastleggen van de rollen en verantwoordelijkheden ten aanzien van informatiebeveiliging;
d) het belang van informatiebeveiliging actief uitdragen en het benadrukken van het voldoen aan de doelstellingen en het naleven van het beleid;
e) het beschikbaar stellen van voldoende middelen;
f) criteria vaststellen voor aanvaardbare risiconiveaus en risicobereidheid;
g) het laten uitvoeren van interne en externe audits.

Actie:

- *In 2018 het beleidskader actualiseren en hierin conform ISO 27001 specifiek ingaan op het onderwerp leiderschap inclusief bijhorende verantwoordelijkheden meenemen, vervolgens beleidskader formeel laten vaststellen door directie/GS.*

5.2. Beleid

In 2015 is het 'Beleidskader informatiebeveiliging Provincie Zeeland 2015-2018' vastgesteld door GS. Dit beleidskader dient in 2018 te worden herzien in verband met organisatorische ontwikkelingen, voortschrijdende inzichten en de nieuwe privacy wetgeving.

Acties:

- *In 2018 het beleidskader actualiseren op basis van ISO 27001 en koppelen aan het managementsysteem voor informatiebeveiliging (PDCA en continu verbetering).*
- *Doorvertalen naar andere beleidsvelden zoals bijv. informatiebeleid, privacybeleid , integriteitsbeleid, inkoopbeleid.*

5.3. Rollen, verantwoordelijkheden en bevoegdheden

In het 'Beleidskader informatiebeveiliging Provincie Zeeland 2015-2018' zijn de rollen en verantwoordelijkheden belegd en is er een werkgroep ingesteld die opgebouwd is uit tot nu toe relevante vertegenwoordiging uit de organisatie. Echter vanuit privacywetgeving hebben we geconstateerd dat in de huidige opzet van de werkgroep een aantal noodzakelijke disciplines ontbreken. Om de informatiebeveiliging en privacy provinciebreed te kunnen blijven waarborgen, is het van belang om het sturingsmodel en de verschillende rollen in de werkgroep te herzien en aan te passen naar de actuele situatie. Verder is het van groot belang om te borgen dat ieder bedrijfsproces, bedrijfsmiddel en beveiligingsproces een eigenaar en beheerder heeft. Een externe consultant wordt ingeschakeld om het ISO 27001 certificeringstraject te begeleiden en

deze zal ook gevraagd worden om de benodigde taken, rollen en sturing (governance) in beeld te brengen. Deze taken en rollen zijn een basisvoorwaarde voor uitvoering van het projectplan & ambities.

Acties:

- *Sturingsmodel 'Informatiebeveiliging en privacy' herzien en volgens deze principes werken aan het te actualiseren beleidskader in 2018. Verder hierin laten zien dat ieder bedrijfsproces, bedrijfsmiddel en beveiligingsproces een eigenaar en beheerder heeft.*
- *Het herziene sturingsmodel vast laten stellen.*

6. Planning

6.1. Maatregelen om risico's te beperken en kansen te benutten

6.1.1. Algemeen

Het is van belang dat de Provincie Zeeland haar risico's en kansen vaststelt die moeten worden aangepakt om enerzijds ervoor te zorgen dat de ambitie voor informatiebeveiliging en privacy voor de komende vier jaar worden behaald en anderzijds dat ongewenste effecten (datalekken, cyberaanvallen, et-cetera) worden voorkomen.
In het 'beleidskader Informatiebeveiliging Provincie Zeeland 2015 – 2018' is een top 10 bestuurlijke risico's opgenomen, zie bijlage voor een overzicht. Bij actualisatie van het beleidskader in 2018 dienen ook deze risico's herzien te worden.

Actie:

- *Herzien van de bestuurlijke risico's bij actualisatie van het beleidskader informatiebeveiliging in 2018.*

6.1.2. Risicobeoordeling van informatiebeveiliging en privacy

De Provincie dient een methode te ontwikkelen voor impact- en risicoanalyses op het gebied van informatiebeveiliging en privacy die aansluit bij de landelijke standaardmethoden (onder andere ontwikkeld in IPO verband). Hiervoor zijn al een aantal middelen beschikbaar die we op dit op dit moment ad-hoc toepassen, zoals een methode om per bedrijfskritisch proces vast te stellen wat de impact op informatiebeveiliging en privacy is. Aansluitend hierop dient een methode voor meer diepgaande risicoanalyse te worden uitgewerkt. Verder wordt er landelijk gewerkt aan de Baseline Informatiebeveiliging voor alle Overheden. In de conceptversie hiervan zijn drie beschermingsniveaus voor informatiebeveiliging uitgewerkt waar we mogelijk op kunnen aansluiten.
De bedoeling is dat we op basis van de reeds aanwezige informatie een toekomstbestendige methode ontwikkelen die we structureel kunnen toepassen voor onze bedrijfskritische processen.

Acties:

- *Ontwikkelen van een toekomstbestendige methode voor impact- en risicoanalyses bij de Provincie Zeeland. Onderzoeken of we de beschermingsniveaus uit de concept Baseline Informatiebeveiliging Overheden kunnen meenemen.*
- *Inventariseren van alle informatiestromen binnen de Provincie inclusief daarmee samenhangende processen, informatiesystemen, informatieobjecten, doel, eigenaar- en beheerrollen.*
- *Op basis van het overzicht identificeren van de bedrijfskritische processen via een impactanalyse op informatieveiligheid en privacy*

- *Per bedrijfskritisch proces een dreigingenanalyse uitvoeren en passende maatregelen definiëren*

6.1.3. Behandeling van risico's van informatiebeveiliging en privacy

De Provincie dient een proces uit te werken voor het behandelen van de geconstateerde risico's uit de risicoanalyse en hiervoor op basis van bijlage A uit de ISO 27001 passende beheersmaatregelen treffen. In de conceptversie van de landelijke baseline informatiebeveiliging zijn per beschermingsniveau de relevante maatregelen benoemd. Mogelijk kunnen we hier op aansluiten.

Actie:

- *Ontwikkelen van een toekomstbestendige procedure voor selectie van passende maatregelen op basis van een impact- en dreigingenanalyse bij de Provincie Zeeland. Onderzoeken of we hierin selectie van maatregelen op basis van beschermingsniveaus uit de concept Baseline Informatiebeveiliging Overheden kunnen meenemen. Dit is onderdeel van het voldoen aan ISO 27001: concreet invulling geven aan de beheersmaatregelen uit bijlage A van de ISO 27001 norm op basis van risico.*

6.2. Informatiebeveiligingsdoelstellingen prioriteren op basis van risico's en planning

Doelstelling is dat we als Provincie een betrouwbare partner willen zijn en dat de genoemde bestuurlijke risico's worden beperkt door het nemen van passende beheersmaatregelen. Verder willen we incidenten zoals bijvoorbeeld onbewust en onbekwaam handelen, datalekken, cyberaanvallen (met als gevolg dat bijvoorbeeld systemen plat gaan) en willen we bijvoorbeeld ook insluiping in gebouwen voorkomen. Op korte termijn heeft het implementeren van de 'Algemene Verordening Gegevensbescherming' die per 25 mei 2018 in werking treedt de hoogste prioriteit. Op middellange termijn willen we informatiebeveiliging continu verbeteren. Dit houdt in dat we de 'Plan, Do, Check, Act' cyclus adequaat moeten inregelen en aantoonbaar voldoen aan de interprovinciale ISO 27001 norm voor informatiebeveiliging.

Actie:

- *Op basis van deze impactanalyse een aanbesteding starten om externe expertise in te schakelen. Deze externe partij gaat de werkgroep Informatiebeveiliging begeleiden bij het traject om provinciebreed over vier jaar ISO 27001 gecertificeerd te zijn. Onderdeel hiervan is het in kaart te brengen hoe we de acties het beste kunnen prioriteren en per actie welke capaciteit (intern en/of externe) en financiële middelen hiervoor nodig zijn.*

7. Ondersteuning

7.1. Middelen

Op basis van deze impactanalyse zal samen met een extern onafhankelijke partij een inschatting worden gemaakt van de benodigde middelen (tijd en geld) om de acties de komende jaren uit te voeren. De benoemde acties zullen worden gebundeld in werkpakketten en per werkpakket zal een inschatting worden gemaakt van de capaciteit en benodigde kennis in geval van zelf doen, volledig uitbesteden aan externe partij of deels uitbesteden aan externe partij onder regie van de Provincie.

Actie:

- De impactanalyse voorleggen aan externe onafhankelijke partij en opdracht geven om meerjarige inschatting te maken van de benodigde middelen, inclusief het uitwerken van een aantal scenario's.

7.2. Competentie

Van belang is dat de Provincie de rollen, bevoegdheden en noodzakelijke competentie vaststelt voor personen die werkzaamheden verrichten waarmee de prestatie van de organisatie op het gebied van informatiebeveiliging en privacy wordt beïnvloed.

Acties:

- Vaststellen van de rollen, bevoegdheden en bijbehorende competenties voor de werkzaamheden die zich primaire richten op het verbeteren van de informatiebeveiliging en privacy (bijv. functieprofielen voor Functionaris Gegevensbescherming, de CISO en de privacy officer)
- Aanstellen Functionaris Gegevensbescherming, de CISO en de privacy officer
- Inventariseren welke personen werkzaamheden verrichten in het kader van informatiebeveiliging en toetsen of ze de juiste scholing, opleiding en ervaring hiervoor hebben. Deze informatie documenteren en jaarlijks actueel houden.

7.3. Bewustzijn

Er dient aandacht te worden besteed aan het gedrag van medewerkers. Het informatieveiligheidsbeleid staat of valt met bewustwording. Informatiebeveiliging kan alleen slagen wanneer alle betrokkenen in de organisatie (bestuur, management, ICT-functionarissen en medewerkers) bewust worden gemaakt van het belang hiervan.
Hiervoor dient een gestructureerde aanpak te worden ontwikkeld om bewustwording te borgen. Het is van belang dat de lijnorganisatie informatieveiligheid gaat dragen en het belang onderkent van haar verantwoordelijkheden en bevoegdheden. Daarom richt de stap "ontwikkeling bewustwording " zich voornamelijk op de volgende doelgroepen:

- *Bestuur en topmanagement (voorbeeldfunctie en rolinvulling);*
- *Lijnmanagement (schakelfunctie tussen top en werkvloer);*
- *Medewerkers (moeten weten hoe zij hun verantwoordelijkheid moeten invullen).*

Actie:

- *Jaarlijks plan van aanpak bewustwording maken en uitvoeren.*

7.4. Communicatie

In de huidige maatschappij verspreidt informatie zich bijzonder snel. Een incident (of een gerucht daaromtrent) bij de provincie kan snel leiden tot imagoschade. Juist (transparant, integer, tijdig) communiceren over incidenten met de stakeholders vereist vastgelegde verantwoordelijkheden en communicatielijnen. Daarnaast is het van belang om met de stakeholders intern en extern regelmatig transparant te communiceren over de wijze waarop hun informatie beschermd wordt. Dit vereist communiceren over informatiebeveiliging via de geschikte kanalen binnen de provincie zoals bijvoorbeeld via de provinciale website.

Actie:

- *Jaarlijks communicatieplan maken en uitvoeren.*

7.5. Gedocumenteerde informatie

In het beheerssysteem voor informatiebeveiliging speelt (en gaan spelen) een aantal documenten een belangrijke rol. Denk aan het informatiebeveiligingsbeleid, de gedocumenteerde uitkomsten van de risicoanalyse, verslagen van audits maar ook werkinstructies, formulieren e.d.

Het is van belang dat deze documenten op de juiste wijze beheerst worden. ISO27001 bevat hiervoor handvaten. Getoetst moet worden of de eisen die ISO27001 stelt aan de beheersing nog leiden tot extra te nemen maatregelen.

Actie:

- *Inventariseren of ISO27001 extra eisen stelt aan het beheer van documentatie anders dan de huidige beheersing door de Provincie. Eventuele extra maatregelen implementeren.*

8. Uitvoering

8.1. Operationele planning en beheersing

Vanaf 2014 is de werkgroep aan de slag om de informatieveiligheid provinciebreed te borgen en een veiligheidsniveau te hanteren om ongewenste verspreiding van vertrouwelijke informatie en ongewenste toegang tot de Provincie te voorkomen.

In 2015 is het beleidskader informatiebeveiliging geactualiseerd en vastgesteld. In dit jaar heeft de focus vooral gelegen op de technische beveiliging en in beeld brengen van de architectuur. Er zijn ook een aantal processen en beleidsrichtlijnen uitgewerkt en geïmplementeerd, bijvoorbeeld beleid voor ICT toegang, cloud- en webapplicaties en beheerprocessen I&A.

In 2016 is bij Provincie Zeeland gewerkt aan het optimaliseren, toetsen en verder uitwerken van het informatiebeveiligingsbeleid. De belangrijkste aspecten daarbij zijn: het implementeren van diverse technische beheersmaatregelen, bewustwording bij de medewerkers en het opstellen van beleidsrichtlijnen. Ook is in dit kader een proces ingeregeld met betrekking tot de Wet Bescherming Persoonsgegevens (“Wet Meldplicht Datalekken”). In de tweede helft van 2016 is een 1-meting uitgevoerd door interne medewerkers van Provincie Zeeland. Eind 2016 heeft een interne training plaatsgevonden voor de implementatie van de algemene ISO27001/2 norm.

Begin 2017 is gestart met de implementatie van diverse beveiligingsrichtlijnen voor wijzigingsbeheer, logische toegangsbeveiligingsbeleid en wachtwoordbeleid en het verder aanscherpen van de IT beveiliging. Verder zijn diverse acties ondernomen voor bewustwording en implementatie van de Europese privacywetgeving (AVG). In september 2017 zijn er een aantal bijeenkomsten georganiseerd om de bewustwording rondom informatiebeveiliging te vergroten bij GS, Directie, PS en medewerkers.

Verder is een impactanalyse uitgevoerd voor wat betreft de implementatie van de Algemene Verordening Gegevensbescherming (AVG).

Actie:

- *Inrichten van een operationeel beheerssysteem voor informatiebeveiliging bestaande uit regelmatige toetsing van de effectiviteit van de getroffen maatregelen via een operationele planning, monitoren van de operatie en bijstelling/rapportage.*

8.2. Risicobeoordeling van informatiebeveiliging

Eerst moeten alle processen zijn geïnventariseerd. Daarna dient per proces de impact op beschikbaarheid, integriteit en vertrouwelijkheid en de risico's in beeld te worden gebracht.

Actie:

- *Conform benoemde criteria per bedrijfskritisch proces een risicoanalyse uitvoeren.*

8.3. Informatiebeveiligingsrisico's behandelen

Per proces dienen vervolgens passende beheersmaatregelen te worden gedefinieerd en geïmplementeerd.

Actie:

- *Per bedrijfskritisch proces na uitvoering van de risicoanalyse maatregelen uit Annex A of uit eventuele andere bron implementeren, verbeteren of aanpassen.*

9. Evaluatie van de prestaties

De directie ontvangt halfjaarlijks een rapport van de stand van zaken rondom informatiebeveiliging.
Op basis van dit rapport maar ook op basis van haar eigen waarneming, controleprocessen, feedback van stakeholders, toezichthouders etc. dient de directie de effectiviteit van de beheersing van informatiebeveiliging bij de Provincie te beoordelen en conform de vereisten uit ISO27001 uitspraken te doen over eventuele kansen voor verbetering, noodzakelijke aanpassingen e.d.

Acties:

- De werkgroep informatiebeveiliging legt halfjaarlijks verantwoording af aan de directie over de status van de informatiebeveiligingsprestaties in het afgelopen halfjaar, de resultaten van de risicobeoordeling(en) en de kansen voor continue verbetering;
- De organisatie moet gedocumenteerde informatie bewaren als bewijsmateriaal voor de halfjaarlijkse verantwoording door de directie.

10. Verbetering

10.1. Afwijking en corrigerende maatregelen

Wanneer zich een afwijking voordoet dient hierop vanuit de werkgroep informatiebeveiliging adequaat te worden gereageerd. Indien van toepassing worden maatregelen getroffen om de afwijking te beheersen en te corrigeren en de consequenties aan te pakken.

Acties:

- *Werkafspraken maken dat vanuit de werkgroep Informatiebeveiliging actie wordt ondernomen indien zich afwijkingen voordoen;*
- *De organisatie moet gedocumenteerde informatie bewaren als bewijsmateriaal van de aard van de afwijkingen en de vervolgens genomen maatregelen en de resultaten van de corrigerende maatregelen.*

10.2. Continue verbetering

Vanuit de werkgroep informatiebeveiliging moet continu de geschiktheid, adequaatheid en doeltreffendheid van de informatiebeveiligingsprocessen worden verbeterd.

Actie

- *Inregelen dat verbeterpunten die worden gesignaleerd voor wat betreft de processen rondom informatiebeveiliging door de werkgroep informatiebeveiliging tijdig en adequaat worden opgepakt*

BIJLAGE A Overzicht bestuurlijke risico’s

In het ‘Beleidskader informatiebeveiliging 2015-2018’ zijn de top-10 bestuurlijke risico’s benoemd. In deze bijlage worden deze benoemd. De top 10 bestuurlijke risico's / issues zijn:

1. Onbewust en/of onbekwaam handelen van medewerkers;
2. Belangrijke informatie van de Provincie is niet beschikbaar (bijvoorbeeld ondersteuning GS en PS, bediening infrastructuur, vergunningverlening, verantwoording);
3. Waardevolle vertrouwelijke informatie komt op straat te liggen of wordt gemanipuleerd (zoals bedrijfsinformatie, grondaankopen, personeelsdossiers, burgemeestersbenoemingen, aanbestedingsinformatie);
4. De fysieke toegang is onvoldoende;
5. De verantwoordelijkheden in het kader van informatiebeveiliging zijn onvoldoende belegd;
6. Het management heeft nog geen voldoende beeld bij de risico's;
7. Informatiebeveiliging is niet geïntegreerd in de bedrijfsprocessen;
8. Door implementatie van web/cloud toepassingen raakt informatiebeveiliging buiten het zicht;
9. Het beleid is op onderdelen onvoldoende uitgewerkt. Dit verhindert het structureel uitvoeren en borgen van de beheersmaatregelen;
10. Escalatieproces onvoldoende geborgd. Grote kans op ad hoc maatregelen en verstoringen in de communicatie indien een calamiteit zich voordoet.