



CBR - Algemeen Beveiligingsbeleid

Gepubliceerd door
CBR Informatiebeveiliging

Titel	Versie	Doelgroep
Algemeen Beveiligingsbeleid	1.8	Geheel CBR (intern en extern)

Auteur	Goedgekeurd door	Geldig tot
Esthelle Lindenburg	Jan Jurgen Huizing	31-03-2020

Status en laatste revisie	Definitief	Locatie van het document
Finaal 14 Maart 2019	definitief	Intranet – Security en Privacy

Samenvatting

Dit Algemeen Beveiligingsbeleid is het centrale raamwerk waarin het beveiligingsbeleid van het CBR wordt vastgesteld.

Versie controle

Versie	Laatste revisie	Editor	Veranderingen/ Commentaar
1.0		TvG	Initiële versie goedgekeurd door Jan Boll
1.1		JvdV	Review en toetsing
1.2		JvdV	Toevoeging medische normenkader
1.3		JvdV	Toevoeging leidraad gegevensverwerking persoonsgegevens
1.4		JvdV	ISO-27002 toegevoegd aanbeveling B. Lanza met mapping.
1.5		JvdV	Nieuw normenkader BIR2017+nen7510:2017 verwijdering Wbp door AVG/opgenomen responsible disclosure en aangesloten bij het NCSC.
1.6		MvdH, ELK	Resp. review en ISMS en PDCA toegevoegd
1.7		PD(ad interim CISO)	Review commentaar verwerkt, H8 t/m 11 verwijderd.
1.8	14-03-2109	ELK	Review verwerkt en 'Melden en registreren van informatiebeveiligingsincidenten' toegevoegd. Wordt ter review aangeboden bij MT ICT.

NB:

Een papieren kopie van dit document is mogelijk niet de laatste versie. Controleer of dit de juiste versie is op de plek waar deze digitaal staat opgeslagen.

Inhoud

1	Inleiding.....	4
1.1	Doel van dit beleidsdocument.....	4
1.2	Wijziging van context.....	4
1.3	Bereik van het beleid	4
1.4	CBR besturing	4
1.5	Doelstelling van het beleid(ISMS)	5
1.6	Risicodragende organisatie	5
2	CBR Beveiligingsregels	6
3	Beveiligingsobjecten	8
3.1	Bescherming van de mens	8
3.2	Bescherming van kennis, informatie en data	8
3.3	Bescherming van netwerk en ICT-infrastructuur	8
3.4	Bescherming van gebouwen, locaties en ruimtes	8
3.5	Bescherming van bedrijfsmiddelen.....	8
3.6	Zeker stellen van de continuïteit van de business proces	9
4	Documentatie hiërarchie.....	10
5	Verantwoordelijkheden.....	11
6	Overlegstructuren.....	13
7	Information Security Management System(ISMS).....	14
7.1	Plan	14
7.2	Do	15
7.3	Check.....	15
7.4	Act.....	15
8	Melden en registreren informatiebeveiligingsincidenten	16

1 Inleiding

CBR vindt het belangrijk dat de klanten, medewerkers en overige belanghebbenden op ons kunnen rekenen als een betrouwbare organisatie. CBR gaat met alle bedrijfsmiddelen met zorg om waarbij informatievoorziening van cruciaal belang zijn voor de organisatie en voortdurend op een passende manier beveiligd dient te zijn.

Het geïntegreerde beveiligingsbeleid richt zich met name op :

- Het beschermen van personen, panden, processen en werkzaamheden op de CBR terreinen.
- Het beschermen van de toevertrouwde data en informatie tegen een breed scala aan bedreigingen. (zoals het voorkomen van datalekken)
- De continuïteit van de bedrijfsvoering te waarborgen.
- De directe schade, maar ook de imagoschade voor de organisatie te beperken.

1.1 Doel van dit beleidsdocument

Het Algemeen Beveiligingsbeleid de vaststelling van het beveiligingsbeleid binnen het CBR. Dit beleid verbindt en ondersteunt alle onderliggende procedures en werkvoorschriften op het gebied van fysieke en informatiebeveiliging.

1.2 Wijziging van context

Het CBR is een publiekrechtelijk zelfstandig bestuursorgaan (ZBO) en moet voldoen aan het voorschrift informatiebeveiliging rijksdienst, verder in dit beleid te noemen 'VIR'. De basis voor de informatiebeveiliging binnen het CBR is gebaseerd op het VIR en op de baseline Informatiebeveiliging Rijksdienst (BIR). Deze 'code van informatiebeveiliging', de NEN-ISO/BIR2017, biedt een uitgebreide verzameling maatregelen waaruit op basis van de risico gebaseerde aanpak een selectie wordt gemaakt van deze ('best practices') van informatiebeveiliging en is bedoeld als referentiepunt voor het vaststellen van een set beveiligingsmaatregelen die nodig zijn om de grootste risico's van het CBR af te dekken. Aanvullend op de BIR2017 zijn voor specifieke medische gegevens 10 maatregelen van toepassing op basis van de NEN 7510:2017.

1.3 Bereik van het beleid

Dit beleidsdocument is van toepassing op alle medewerkers en externen (inhuurkrachten) van CBR. Daarnaast is het beleid van toepassing op klanten en leveranciers die op de locaties van CBR aanwezig zijn.

1.4 CBR besturing

De cyclus voor verbetering van informatiebeveiliging (Plan-Do-Check-Act; PDCA) wordt gekoppeld aan de Planning & Control (P&C) cyclus van het CBR. Hiermee wordt informatiebeveiliging ingebed in de bedrijfsvoering en worden IB-activiteiten samen met overige activiteiten geprioriteerd en opgenomen in het jaarplan. De tijdslijn van de IB-cyclus wordt afgestemd op de jaarlijkse P&C cyclus.

De doelstelling is om alle gewenste maatregelen voor informatiebeveiliging in kaart te hebben bij het bepalen van de invulling van de concept jaarplannen. Hiervoor is het nodig een nieuwe risicoanalyse en beoordeling van het Information Security Management System (ISMS) uit te voeren en op basis van de resultaten de bijpassende maatregelen te kiezen. Tijdens het vaststellen van de (concept) jaarplannen wordt een verdere afbakening gemaakt op basis van beschikbaar budget en overige middelen.

De externe beoordeling van het ISMS wordt uitgevoerd ten behoeve van het 'in control statement' voor de jaarrekening. Indien deze audit in september plaatsvindt, kunnen eventuele kritische bevindingen alleen via een escalatie naar de directie in het jaarplan worden opgenomen.

1.5 Doelstelling van het beleid(ISMS)

De primaire doelstelling van het ISMS is het waarborgen van informatiebeveiliging door het identificeren van welke informatie bedrijfsmiddelen beveiligd dienen te worden en tot welk niveau ze beveiligd dienen te worden. Bedrijfsmiddelen bestaan uit elektronische informatie, papieren documenten en fysieke bedrijfsmiddelen zoals computers.

Het ISMS stelt een raamwerk vast met een continue cyclus van activiteiten voor het beoordelen van risico's, ontwerpen en implementeren van beveiligingsprocedures om risico's te adresseren en het monitoren van de effectiviteit van de procedures in het adresseren van de risico's.

1.6 Risicodragende organisatie

De directie heeft besloten dat het CBR een risicodragende organisatie is, wat inhoudt dat niet alle risico's en gevolgen volledig worden afgedekt, door beperkte tijd en middelen. In plaats hiervan worden kosten van maatregelen afgewogen tegen de risico's, en worden restrisico's tot een bepaald niveau vanuit bedrijfseconomische overwegingen geaccepteerd. In het nastreven van een risicodragende organisatie worden risico's behandeld door deze te verminderen, vermijden, overdragen of te accepteren.

2 CBR Beveiligingsregels

Het CBR Algemeen Beveiligingsbeleid hanteert een aantal beveiligingsregels.

Voldoen aan wet- en regelgeving en contractuele verplichtingen.

Naast de afspraken die het CBR met derde partijen maakt moet het CBR zich houden aan toepasselijke wet- en regelgeving zoals bijvoorbeeld de Algemene Verordening Gegevensbescherming (AVG) en het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007) en bij bijzondere gegevens aan het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI 2013).

Veilige werkomgeving

Het CBR neemt passende beveiligingsmaatregelen om de veiligheid van personen te garanderen binnen de gebouwen en terreinen van het CBR.

Dataprivacy en databeveiliging

Het CBR draagt er zorg voor dat de persoonlijke data van onze klanten en medewerkers beschermd wordt door middel van logische en fysieke maatregelen teneinde misbruik te voorkomen.

Vertrouwen van onze klanten en partners

Het CBR borgt dat risico's voor onze bedrijfsvoering tot een acceptabel niveau worden teruggebracht en vertrouwelijke informatie bij ons in goede handen is. Het CBR is hierdoor een betrouwbare partner voor onze partners, klanten en omgeving.

Beveiligingscultuur

Het CBR stimuleert de verantwoordelijkheid van de medewerker en draagt er zorg voor dat de medewerker door middel van awareness campagnes zich bewust blijft van zijn verantwoordelijkheden.

Transparante verantwoordelijkheden

De taken en verantwoordelijkheden voor de beveiliging van informatie binnen het CBR zijn belegd. CBR draagt zorg voor een transparante verantwoordelijkheidstoewijzing met in achtname van noodzakelijke functiescheiding.

Need-to-know

De toegangsrechten tot de geautomatiseerde en fysieke omgeving moeten zijn ingedeeld op basis van het 'need to know' principe. Hierbij geldt dat een medewerker (zowel intern als extern) enkel toegang mag hebben tot de gegevens en locaties die benodigd zijn voor het uitvoeren van de werkzaamheden die voor de betreffende functie minimaal noodzakelijk zijn. De rechten worden regelmatig geëvalueerd.

Laatste stand der techniek

Om er voor zorg te dragen dat de organisatie zo goed mogelijk inspeelt op de bedreigingen van buitenaf past CBR moderne technieken toe om mens, data en infrastructuur te beschermen.

Waarde toevoeging door geïntegreerde en kostenbewuste beveiligingsmaatregelen

Beveiligingsmaatregelen worden genomen met in achtname van een acceptabele kosten versus opbrengsten ratio. Informatiebeveiliging maakt integraal onderdeel uit van ontwikkelprojecten en wijzigingen op ICT-landschappen en business processen.

Beveiligingsstandaarden

CBR volgt de “Best Practices” en normen die van toepassing zijn op het gebied van informatie- en fysieke beveiliging zonder deze noodzakelijkerwijs volledig te willen implementeren.

Toetsing op naleving van het beleid

De toetsing van het beleid o.a. de wettelijke verplichting VIR en de jaarrekening vindt jaarlijks plaats door het toetsen van de maatregelen conform de BIR2017 en indien van toepassing de 10 additionele NEN 7510:2013 normen. Naast de toetsing zal de CISO een jaarlijkse risicoanalyse uitvoeren.

Indien een organisatieonderdeel of een toeleverancier haar zaken op orde heeft volgens ISO-27001, rekening houdend met de implementatiemaatregelen uit ISO-27002, en voldoende privacy maatregelen heeft getroffen zoals ‘Privacy by Design’ en handelt conform de Algemene Verordening Gegevensbescherming(AVG) dan hoeft die organisatie slechts te controleren op de aanvullende bepalingen voor bijvoorbeeld aansluitvoorwaarden voor een specifiek register.

3 Beveiligingsobjecten

CBR heeft als specifieke taak de bescherming en beveiliging van de volgende objecten:

3.1 Bescherming van de mens

Het welzijn van het individu – bijvoorbeeld de klanten, medewerkers, bezoekers, leveranciers die de gebouwen en locaties betreden van het CBR – heeft de prioriteit boven economische overwegingen. Afhankelijk van hun functie en individuele activiteiten worden de mensen blootgesteld aan verschillende bedreigingen zoals agressie, gezondheidsrisico's, en ongevallen. Het beleidsdocument Personeel & Event Beveiliging gaat met name over de maatregelen die getroffen worden om deze risico's te verminderen.

3.2 Bescherming van kennis, informatie en data

De documenten Informatie & data classificatie is geschreven om duidelijk vast te leggen hoe omgegaan wordt met informatie en data in lijn met hun classificatie gedurende de lifecycle van creatie tot vernietiging. In het CBR Privacybeleid is beschreven hoe het CBR uitvoering geeft aan de Algemene Verordening Gegevensbescherming(AVG).

3.3 Bescherming van netwerk en ICT-infrastructuur

Het CBR Informatiebeveiligingsbeleid is geschreven om bescherming te bieden aan de Vertrouwelijkheid, Integriteit en Beschikbaarheid van de data die verwerkt wordt in, verstuurd via en opgeslagen wordt in het netwerk en de ICT-infrastructuur. Het beleid voorziet in de fundamentele maatregelen voor de bescherming van de ICT-systemen door middel van duidelijke verantwoordelijkheden, processen, controlepunten en rapportages.

3.4 Bescherming van gebouwen, locaties en ruimtes

Medewerkers, klanten en leveranciers werken op en bezoeken onze kantoren, middelen worden opgeslagen en ICT-infrastructuur is aanwezig. De fysieke infrastructuur van de gebouwen en ruimtes moet bescherming bieden aan de mensen, technologie en middelen. Het Fysieke Beveiligingsbeleid definieert de basisprincipes voor een adequate bescherming.

3.5 Bescherming van bedrijfsmiddelen

De bedrijfsmiddelen van het CBR moeten beschermd worden door middel van genomen beveiligingsmaatregelen. Indien er overtredingen van de wet vermoed worden dan moeten deze overtredingen grondig worden onderzocht. Het doel van dit onderzoek is vaststellen wie verantwoordelijk, de gevolgen te minimaliseren, de kwetsbaarheden en/of beveiligingsgaten weg te nemen. Het onderzoek moet zich ook richten op hoe de overtreding tot stand heeft kunnen komen teneinde zorg te dragen voor preventieve maatregelen in de toekomst. In overeenstemming met geldende Wet- en Regelgeving zal informatiebeveiliging managementsystemen ontwikkelen en gebruiken om misstanden te detecteren, voorkomen. Daarnaast ook bewijs vast te leggen in het geval van fraude of elke andere vorm van misbruik. Het beleid met betrekking tot Fraudebeheersing (detectief en correctief) voorziet in de rechten en plichten van degenen die het onderzoek doen. Tevens voorziet het beleid in de minimale eisen voordat men overgaat tot onderzoek. Daarnaast worden de eisen gedefinieerd met betrekking tot documentatie en archief.

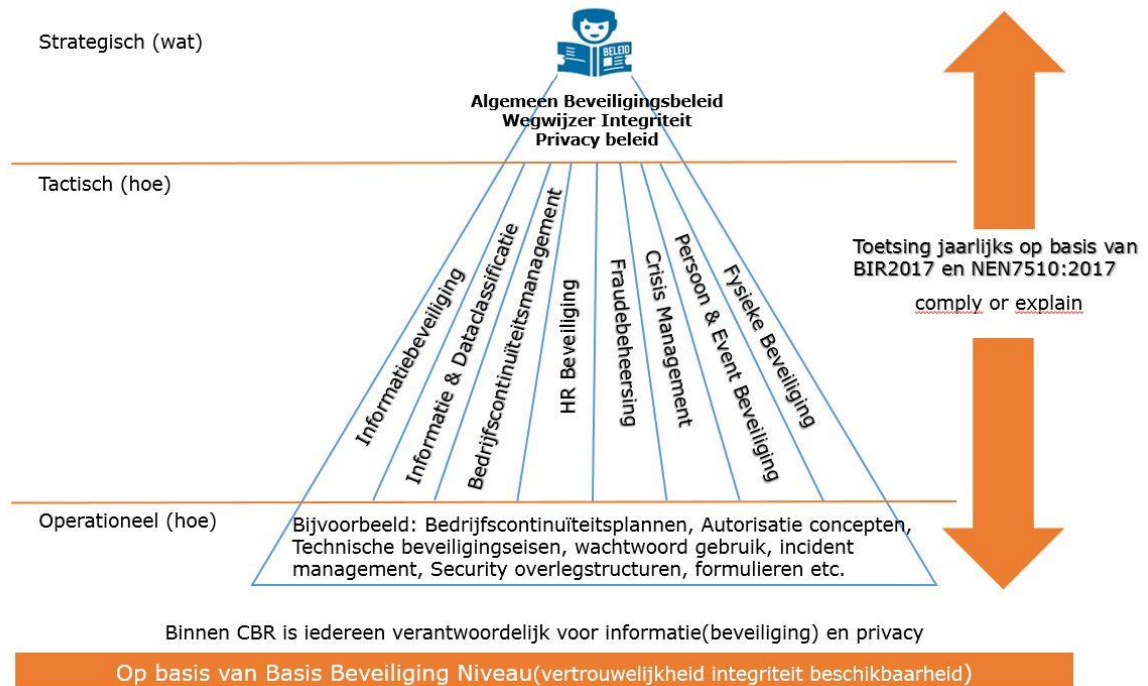
Het HR Beveiligingsbeleid (preventief) gaat in op de te nemen maatregelen voordat iemand aangenomen wordt, de werkzame periode binnen CBR en als de medewerker CBR verlaat.

3.6 Zeker stellen van de continuïteit van de business proces

Langdurige verstoringen van kritieke business processen of in de ICT-infrastructuur kunnen de missie van het CBR ernstig in gevaar brengen of grote gevolgen hebben voor de operatie van het CBR. Het Beleid Bedrijfscontinuïteitmanagement voorziet met name in hoe een continuïteitsproblemen binnen CBR gemanaged wordt. Het Crisismanagementplan beschrijft de modus operandi in het geval van zeer ernstige verstoring van de bedrijfsvoering.

4 Documentatie hiërarchie

Het algemene beveiligingsbeleid is vastgelegd in de top van de piramide (strategische). De onderliggende documenten (zie ook hoofdstuk 3) definiëren in meer detail het beleid op tactische niveau en geven richting aan de uitvoering van de verschillende onderwerpen.



Informatiebeveiliging en privacy heeft betrekking op alle bedrijfsprocessen van het CBR. Binnen de documenten vindt een overlap plaats tussen informatie en fysieke beveiliging. De borging van toetsing o.a. t.a.v. de wettelijk verplichting VIR zal minimaal plaatsvinden op basis van de BIR2017 controls en de NEN 7510.

5 Verantwoordelijkheden

Verantwoordelijkheden op hoofdlijnen.

Een medewerker is primair verantwoordelijk voor de uitvoer van zijn of haar taken. De taken en bijbehorende verantwoordelijkheden zijn vastgelegd in de functiebeschrijving, welke is opgenomen in de arbeidsovereenkomst van de werknemer. Separaat is een gedragscode ondertekend (integriteitsverklaring), waarmee de medewerker o.a. verklaart nu en in de toekomst integer om te gaan met vertrouwelijke informatie.

De divisie manager is verantwoordelijk voor informatiebeveiliging binnen zijn/haar divisie, waarin hij/zij zorg draagt voor het optimaal functioneren van de divisie, evenals het toezien op het naleven van gedragsregels en het beleid ten aanzien van de beveiliging.

Nieuwe medewerkers dienen door de divisie manager te worden ingelicht over de voor hen van belang zijnde regels uit het beveiligingsbeleid. Dit geldt eveneens voor tijdelijke medewerkers en stagiaires.

De verantwoordelijkheid voor beveiliging is helder belegd bij de daarvoor aangewezen functies en heeft de daarbij behorende bevoegdheden. De verantwoordelijkheden en bevoegdheden zijn opgenomen in functiebeschrijvingen en beschikbaar gemaakt worden aan iedere medewerker van het CBR.

Uitgangspunt 1 De directie legt formeel de rollen, verantwoordelijkheden en bevoegdheden voor beveiliging vast.

Directie

De directie geeft duidelijk richting, toont betrokkenheid en kent en erkent expliciet verantwoordelijkheden voor beveiliging.

Directeur bedrijfsvoering/Chief Operating Officer(COO)

De Directeur bedrijfsvoering(COO) is verantwoordelijk voor het dagelijks beleid. Voorzitter van de CBR Beveiligingscommissie.

Chief Information Officer

De CIO draagt zorg voor de inrichting en het functioneren van de gehele IT-organisatie. Lid van de CBR Beveiligingscommissie.

Corporate Information Security Officer

De CISO is aanspreekpunt en verantwoordelijk voor informatiebeveiliging en is tevens voor het CBR contactpersoon richting het Nationaal Cyber Security Centrum(NCSC) van de overheid. De CISO ontwikkelt beleid op het gebied van informatiebeveiliging en stuurt erop aan dat de noodzakelijke informatiebeveiligingsmaatregelen worden getroffen op basis van een gedegen risicoanalyse. De CISO stuurt er daarnaast op aan dat de noodzakelijke informatiebeveiligingsmaatregelen door ketenpartners en bewerkers worden getroffen op basis van een gedegen risicoanalyse. Tevens rapporteert de CISO aan de directie over de status van het informatiebeveiligingsbeleid. Lid van de CBR Beveiligingscommissie.

Informatiebeveiliging ICT

Het ontwikkelen, bevorderen, coördineren en beheersen van richtlijnen gericht op informatiebeveiligingsmaatregelen. De Informatiebeveiliging ICT ondersteunt de CISO en zorgt eveneens voor afhandeling van de CBR responsible disclosure proces.

Security Manager

Verantwoordelijk voor het bewaken, toetsen en continu verbeteren van het fysieke beveiligingsbeleid, dat bijdraagt aan een ongestoorde bedrijfsvoering en het CBR ondersteunt in het waarmaken van haar ambitie.

Lid van de CBR Beveiligingscommissie.

Functionaris Gegevensbescherming (FG)

De FG informeert en adviseert over en houdt toezicht op de bescherming van Persoonsgegevens en treedt op als contactpersoon van de Autoriteit Persoonsgegevens(AP).

Lid van de CBR Beveiligingscommissie.

Interne Audit Dienst

Verantwoordelijk voor het onafhankelijk beoordelen en toetsen van de handhaving, naleving en uitvoering van het beveiligingsbeleid in opdracht van de directie en doet aanbevelingen ter zake aan de directie. Verantwoordelijk voor het bewaken, toetsen en continu verbeteren van fraudebeheersingsbeleid.

Divisie & stafmanagers

De divisie en stafmanagers zijn eindverantwoordelijk voor het treffen van de noodzakelijke beveiligingsmaatregelen op basis van een gedegen risicoanalyse. Daarnaast zijn zij eindverantwoordelijk voor het treffen van de noodzakelijke beveiligingsmaatregelen op basis van een gedegen risicoanalyse door ketenpartners en bewerkers.

Informatiemanagers

De Informatiemanagers hebben een rol als informatiebeveiligers, zij zijn verantwoordelijk voor het treffen van de noodzakelijke beveiligingsmaatregelen op basis van een gedegen risicoanalyse. Daarnaast zijn zij verantwoordelijk voor het treffen van de noodzakelijke beveiligingsmaatregelen op basis van een gedegen risicoanalyse door ketenpartners en bewerkers.

Werknemer

Onder werknemer wordt verstaan een persoon die ten behoeve van het CBR werkzaam is. Alle werknemers zijn gehouden de voorgeschreven beveiligingsmaatregelen na te leven en afwijkingen en incidenten te melden via één aangewezen meldpunt.

6 Overlegstructuren

Binnen het CBR zijn de CISO en de Informatiebeveiliging ICT (IBTEAM) de verantwoordelijken voor het managen van het Beveiligingsraamwerk. Om te waarborgen dat de getroffen en de te treffen informatiebeveiligingsmaatregelen conform de beoogde doelstelling(en) van het CBR zijn dient met regelmaat op verschillende niveaus overleg plaats te vinden. De onderstaande overleggen moeten hierbij periodiek worden gehouden:

Strategisch	Security Directieoverleg (jaarlijks)
Strategisch/ Tactisch	Security Board (1x kwartaal)
Operationeel	Security Overleg (1x maand)

7 Information Security Management System(ISMS)

Om de beveiligingsdoelen te bereiken heeft het CBR een Information Security Management System (ISMS) gebaseerd op de BIR2017. Voor medische gegevens zijn 10 aanvullende maatregelen gebaseerd op de NEN 7510:2017. Het ISMS wordt jaarlijks geëvalueerd door het management en in speciale gevallen door een interne of externe audit. Het ISMS voorziet ook in een raamwerk voor een risico gebaseerde aanpak in de gebieden vallend onder de ondergeschikte documenten van het CBR - Algemeen Beveiligingsbeleid. (de tactische beleidsdocumenten)

Uitgangspunt 2 Het Beveiligingsmanagement draagt zorg voor een Information Security Management Systeem (ISMS) wat van toepassing is op de specifieke beveiligingsrisico's van het CBR.

Minimaal op jaarbasis zal het ISMS geëvalueerd worden op geschiktheid en toepasselijkheid.

Plan-Do-Check-Act als cyclisch proces

Het managementsysteem voor informatiebeveiliging omvat een continu en cyclisch proces. Dit betekent dat op basis van de uitkomsten van evaluaties en controles of door nieuwe ontwikkelingen de noodzaak aanwezig kan zijn het informatiebeveiligingsbeleid aan te passen, een nieuwe risicoanalyse uit te voeren, extra maatregelen te treffen of de implementatie hiervan aan te passen. Ook is het mogelijk dat nieuwe ontwikkelingen, zoals de introductie van nieuwe bedrijfsprocessen of informatiesystemen, aanleiding geven om het informatiebeveiligingsbeleid te heroverwegen. Een dergelijke beoordeling vindt minimaal één maal per jaar plaats en wordt geïnitieerd door de CISO.

7.1 Plan

In Plan worden de **betrouwbaarheidseisen** en de organisatie van de informatiebeveiliging vastgesteld. Deze zijn gebaseerd op het beveiligingsbeleid, wet- en regelgeving en risicoanalyses. De maatregelen komen voort uit geïdentificeerde risico's. Er worden maatregelen ontwikkeld waarmee gewaarborgd wordt dat aan de betrouwbaarheidseisen wordt voldaan. Hierbij wordt gebruik gemaakt van 'best practices', relevante standaarden en eigen expertise. De maatregelen worden door divisie- en stafmanagers uitgevoerd. Divisie- en stafmanagers zullen de uitvoering van de maatregelen documenteren om aantoonbaar te voldoen aan dit beleid. De divisie- en stafmanagers worden hierin ondersteund door de informatiebeveiliging van hun divisie of stafafdeling, te weten de informatiemanagers.

In het geval van uitbesteding van informatiediensten aan derden geldt een vergelijkbare aanpak: op basis van een risicoanalyse worden (contractueel) vastgelegde afspraken gemaakt met deze 'bewerkers' over de te treffen maatregelen, de uitvoering en de vastlegging daarvan.

De documenten in Plan zijn de volgende:

- **Het algemeen beveiligingsbeleid**; door de Directie vastgesteld, waarin basisverantwoordelijkheden zijn vastgelegd rond de beveiliging van de organisatie. Naar het beveiligingsbeleid wordt in het informatiebeveiligingsbeleid regelmatig verwezen.
- **De risicoanalyse informatiebeveiliging**; door de informatiebeveiligingsautoriteit vastgesteld, waarin de belangrijkste risico's op het gebied van informatiebeveiliging zijn opgenomen. Op basis van deze risicoanalyse wordt bepaald welke maatregelen noodzakelijk zijn in de organisatie.
- **Het informatiebeveiligingsbeleid**; door de Directie vastgesteld, waarin de beleidsuitspraken inzake informatiebeveiliging zijn opgenomen en waarin de **informatiebeveiligingsrichtlijnen** worden vastgesteld. De richtlijnen zijn in veel gevallen (deel van) reeds bestaande documenten, welke hier als richtlijn zijn benoemd.

7.2 Do

De uitvoering van het informatiebeveiligingsbeleid. De technische kant van de informatiebeveiliging wordt uitgevoerd door de afdeling ICT, in samenspraak met andere afdelingen. Daarnaast is het de verantwoordelijkheid van iedere medewerker om het informatiebeveiligingsbeleid uit te voeren.

Op basis van de uitkomsten van de risicoanalyse wordt, zowel op centraal als op decentraal niveau, een verbeterplan opgesteld. In dit plan worden de verbeteractiviteiten voor de realisatie van het gewenste beveiligingsniveau op projectmatige wijze vastgelegd.

Het informatiebeveiligingsplan wordt op centraal niveau vastgesteld door de Directie en op decentraal niveau door divisie- en stafmanagers.

Aan de hand van het informatiebeveiligingsplan wordt de implementatie van de aanvullende beveiligingsmaatregelen ter hand genomen. Dit betekent onder andere het opstellen van richtlijnen en procedures voor informatiebeveiliging, het invoeren van beveiligingshulpmiddelen en het voorlichten en opleiden van personeel.

7.3 Check

Jaarlijks wordt de informatiebeveiliging gemonitord en beoordeeld op conformiteit aan het geldende beleid, wet- en regelgeving. Belangrijke checks in de cyclus zijn:

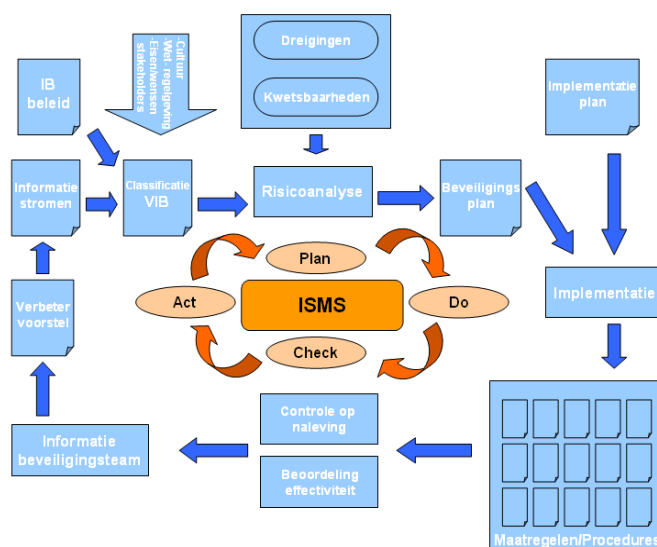
- Bestaan alle voorgenomen maatregelen?
- Zijn de maatregelen bekend bij medewerkers die een rol hebben bij de uitvoering?
- Worden de maatregelen conform doelstelling uitgevoerd?
- Zijn de maatregelen effectief in werking?

Controles vinden plaats op activiteiten van de eigen lijnorganisatie en de externe bewerkers.

7.4 Act

Op grond van de resultaten van de audit wordt geëvalueerd en worden eventueel noodzakelijke wijzigingen aangebracht in het beleid of de maatregelen.

De PDCA cyclus wordt zowel continu als periodiek doorlopen.



Figuur 1 Information Security management System (ISMS)

8 Melden en registreren informatiebeveiligingsincidenten

Alle medewerkers(intern/extern) zijn gehouden de voorgeschreven beveiligingsmaatregelen na te leven.

Medewerker(intern/extern)

- Iedere medewerker is verplicht om een (vermoeden van een) informatiebeveiligingsincident te melden. Ook afwijkingen van de normale gang van zaken ('iets vreemds'), zelfs als dit op het eerste oog geen negatieve gevolgen lijkt te hebben, moet worden gemeld;
- Medewerkers melden *informatiebeveiligingsincidenten* of vermoeden hiervan via
 - o de ICT Servicedesk: bel (088 227) 5800 of mail ict.servicedesk@cbr.nl
 - o Securitydesk@cbr.nl
- Meld datalekken via melden.datalekken@cbr.nl
- Meld fraude via melding@cbr.nl

--- Veilig thuiskomen door toetsen, informeren en monitoren ---