Ministerie van Verkeer en Waterstaat

Directoraat-Generaal Rijkswaterstaat

Bouwdienst Rijkswaterstaat

Procedure voor Informatiebeveiliging

Toepassing van het Voorschrift Informatiebeveiliging Rijksdienst

1 juli 2002

Ministerie van Verkeer en Waterstaat

Directoraat-Generaal Rijkswaterstaat

Bouwdienst Rijkswaterstaat

Procedure voor Informatiebeveiliging

Toepassing van het Voorschrift Informatiebeveiliging Rijksdienst

1 juli 2002

Afdeling: BD - NIE
Naam: Merijn de Lange
Versie: 1.0
Datum: 1 juli 2002

Inhoudsopgave

Inleiding

Informatiebeveiliging bij de overheid speelt al sinds de jaren tachtig. Met de komst van het Voorschrift Informatiebeveiliging Rijksdienst uit 1994, kortweg het VIR, is gepoogd hier een meer structurele invulling aan te geven. Sinds de invoering van het VIR zijn er binnen V&W diverse beleidsnota's geschreven en behandeld. Na een in zekere mate voortvarende aanpak in den beginne, is informatiebeveiliging in het kader van het VIR ten koste van het millenniumproject in het slop geraakt. Nu de millenniumprojecten ten einde zijn, is het VIR opnieuw opgepakt. Intussen opgedane ervaringen, o.a. in het millenniumproject, zullen een koerswijziging van het oude maar nog steeds vigerende beleid bewerkstelligen. Ook nu zal blijken dat informatiebeveiliging niet een technisch-inhoudelijk maar een managementprobleem is, waarbij het vooral de vraag is hoe het centrale en decentrale lijnmanagement meer belangstelling voor, inzicht in en greep op informatiebeveiliging kan krijgen.

- **Aanleiding**

Vanwege de onbekendheid met het VIR op de afdeling installatietechniek (NIE) die valt onder de hoofdafdeling Natte Infrastructuur van de Bouwdienst, is mij de vraag gesteld om het een en ander over het VIR uit te zoeken en op papier zetten. De afdeling NIE kwam in aanraking met het VIR bij het ontwerpen van de nieuwe Verkeer Management Centrale Zuid-West Nederland in Rhoon.

- **Toepassing**

Dit rapport dient om een praktische invulling te geven aan het VIR voor de afdeling NIE en is gebaseerd op de bevindingen die de pilot "Regisseren bij Intensief Wegverkeer" in de ruit van Rotterdam hebben opgeleverd. Bij het ontwerpen van de nieuwe verkeersmanagement centrale in Rhoon bleek een pilot project informatiebeveiliging te zijn opgezet, waarin uitgangspunten voor het VIR in toepassing zijn gebracht.

- **Besluit**

Het VIR is een besluit dat op 22 juli 1994 is genomen door de Minister - President, Minister van Algemene Zaken, R.F.M. Lubbers. Dit besluit is op 1 januari 1995 van kracht geworden.

- **Ministerie van Verkeer en Waterstaat**

Het Ministerie van Verkeer en Waterstaat heeft gehoor gegeven aan dit besluit door een informatiebeveiligingsbeleid samen te stellen. Dit beleid is na te lezen op http://www.ib.venwnet.minvenw.nl. Er wordt op deze intranetpagina volledig uit de doeken gedaan wat de visie is van RWS op het beleid, hoe er moet worden gehandeld, wat de inhoud is van het informatiebeveiligingsbeleid en nog veel meer.

- **Achterliggende gedachte**

Het VIR is in het leven geroepen om te zorgen dat men zich bewust wordt van de risico's die processen en informatiesystemen met zich meebrengen. Een direct gevolg van dit gedachtegoed, is het handelen naar deze risico's, zoals bijvoorbeeld het afstemmen van beleid, het aanpassen van de technische infrastructuur en het beveiligen van informatiesystemen.

- **Procedure**

Om informatie zo goed mogelijk te beveiligen heeft RWS in navolging van V&W een baseline ontwikkeld. Hierin zijn een aantal minimumeisen vastgesteld wat voor ieder informatiesysteem en/of technische infrastructuur moet gelden. Verder moet er bij een maatschappelijk vitaal proces of vitaal generiek informatiesysteem naar een procedure worden gehandeld. Deze procedure is verder beschreven in dit rapport en is samengevat in een overzichtelijk schema (zie bijlage 1 en bijlage 2).

- **Standaarden**

Voor iedere stap in de procedure zijn standaarden gebruikt die het geheel overzichtelijk maken. Onder deze standaarden bevinden zich procedures, sjablonen, methoden en technieken. De sjablonen kunnen worden gebruikt bij deze procedure. In dit rapport wordt aangegeven waar de sjablonen van toepassing zijn. De sjablonen zijn opgenomen in de bijlagen.

1 Baseline RWS: Minimumeisen

Voor heel RWS is een baseline voor informatiebeveiliging geïntroduceerd. Deze baseline houdt in dat ieder informatiesysteem moet voldoen aan een pakket van minimumeisen. De minimumeisen zijn dus op ieder informatieproces, informatiesysteem en/of technische infrastructuur van toepassing. Op ieder maatschappelijk vitaal proces of vitaal generiek informatiesysteem dient behalve een afhankelijkheidsanalyse ook een kwetsbaarheidsanalyse te worden uitgevoerd. Hiervoor zijn sowieso de minimumeisen van toepassing. Echter voor alle andere informatie processen en systemen gelden deze minimumeisen ook.

De minimumeisen zijn afkomstig uit de code voor informatiebeveiliging. Deze code is opgesteld door het ministerie van Economische Zaken, ministerie van Verkeer en Waterstaat en het Nederlands Normalisatie-Instituut. Alle eisen uit deze norm staan beschreven in bijlage 3. De eisen staan beschreven op doelstellingen niveau. Voor een nadere uitleg van deze doelstellingen is bijlage 4 toegevoegd. Mocht deze uitleg nog onvoldoende zijn dan is de code voor informatiebeveiliging te raadplegen voor meer aanvullende informatie.

De eisen uit bijlage 3 zijn direct overgenomen uit de code voor informatiebeveiliging. De minimumeisen voor informatiebeveiliging zijn aangegeven in een speciale kolom van deze tabel.

In bijlage 15 staat een aantal minimummaatregelen die direct betrekking hebben op de minimumeisen zoals eerder beschreven. De minimummaatregelen zijn afkomstig uit de "Handreiking minimumeisen informatiebeveiliging". Achter ieder punt uit bijlage 15 staat een maatregel. Deze kunnen worden gekoppeld aan de minimumeisen. In de handreiking staat een aantal voorbeeldmaatregelen die gebruikt kunnen worden om te controleren of aan een bepaalde eis is voldaan. De minimummaatregelen kunnen tevens gebruikt worden als advies om te zorgen dat aan een bepaalde eis voldaan kan worden. Het geeft in ieder geval aan in welke richting gedacht kan worden. De handreiking minimumeisen informatiebeveiliging is terug te vinden op de intranetpagina http://www.ib.venwnet.minvenw.nl/.

2 Procedure Informatiebeveiliging

Om een zo goed mogelijk beeld te krijgen van de knelpunten in de informatiebeveiliging kan de procedure zoals beschreven in dit hoofdstuk van pas komen. De procedure informatiebeveiliging wordt toegepast op een proces. Bij een proces waar de informatievoorziening van vitaal belang is, dient de beveiliging optimaal te zijn. Dit heeft tot gevolg dat een onderzoek gedaan moet worden naar de risico's van verkeerde informatievoorziening bij een vitaal proces. Een dergelijk onderzoek begint met overeenstemming bereiken met alle betrokkenen over het plan van aanpak in het kader van het project informatiebeveiliging. Voor kennis en ervaring kan een specialist worden aangesteld op het gebied van procesbeschrijving, afhankelijkheidsanalyses en kwetsbaarheidsanalyses (risico en betrouwbaarheid). Eventueel kan de speciaal opgerichte infodesk "FABIN" worden geraadpleegd in deze kwestie. Vervolgens moet duidelijk worden van welk proces sprake is en met welke systemen het proces te maken heeft. Tevens moeten de kenmerken en aspecten van de systemen zichtbaar worden gemaakt. Hierop wordt dan een afhankelijkheidsanalyse uitgevoerd welke duidelijk moet maken in wat voor mate bepaalde systemen verantwoordelijk zijn voor een goede uitvoering van het proces. Een kwetsbaarheidsanalyse moet er op wijzen waar de kwetsbaarheden van diezelfde systemen liggen. Uiteindelijk moet de kwetsbaarheidsanalyse leiden tot een informatiebeveiligingsplan waarin alle risico's beschreven zijn en waarin maatregelen worden voorgeschreven om de risico's af te vangen.

In de rest van dit hoofdstuk wordt beschreven welke stappen er genomen moeten worden om uiteindelijk tot een goede informatiebeveiliging te komen. De stappen zijn tevens schematisch weergegeven in bijlage 1 en bijlage 2.

Voor het gehele proces wordt geadviseerd om een A&K-analist te raadplegen. Dit is een specialist op het gebied van A&K-analyses. Deze kan zorgen voor begeleiding bij het onderzoek van een informatiesysteem. Ook kan infodesk FABIN zorg dragen voor een goede begeleiding. Enkele specialisten op het gebied A&K-analyses zijn daar werkzaam. Een profielschets van een A&K-analist is vermeld in bijlage 7.

2.1 Plan van aanpak

(sjabloon "Plan van Aanpak Informatiebeveiliging", Bijlage 5)

Doel: Het vastleggen van het plan van aanpak voor het project informatiebeveiliging

Kernpunten:
1. Het vastleggen van de projectopdracht
2. Het vastleggen van de aanpak van het project
3. Het vastleggen van de inrichting en de voorwaarden van het project
4. De planning van de opdracht
5. Het vastleggen van de kwaliteitsborging

Uitleg:
1. Doelstelling, beschouwingsgebied, opdrachtformulering, op te leveren producten, eisen en beperkingen worden bepaald
2. Bepalen van de quick wins, minimumeisen en de A&K-analyses
3. De bepaling van de projectinrichting en de voorwaarden aan de opdrachtgever
4. Aangegeven moet worden welke normen en aannames gehanteerd worden en het activiteitenplan, productenplan, resourceplan en financieel plan worden vastgelegd
5. Hierin worden risico's aangegeven en bepaling gedaan van de beheersing van die risico's

Resultaat: Een plan van aanpak voor de rest van het project

2.2 Voortraject

Het voortraject van informatie beveiliging bestaat uit meerdere stappen. Om aan de procedure te voldoen dienen deze stappen stuk voor stuk te worden doorlopen.

- **Plan van aanpak voortraject**

(sjabloon "Plan van Aanpak Voortraject", Bijlage 6)

Doel: Het vastleggen van het plan van aanpak voor het voortraject

Kernpunten:
1. Vaststellen van de organisatiestructuur
2. Werkwijze vastleggen
3. Afbakening van het project

Uitleg:
1. Het toewijzen van verantwoordelijkheden en functies
2. Het vastleggen van de procedure van afhandeling
3. Alle (rand)voorwaarden vaststellen en duidelijk aangeven wat wel en wat niet moet worden gedaan

Resultaat: Een planning en kostencalculatie

- **Bepalen scope van het proces**

(sjabloon "Beschrijving Proces", Hoofdstuk 4, Bijlage 8)

Doel: Vastleggen van verantwoordelijkheden en de betrokken instanties inventariseren

Kernpunten:
1. Vastleggen van de organisatie waarin het proces zich afspeelt
2. De omgeving van het proces bepalen

Uitleg:
1. Beschrijf de organisatiestructuur
2. Beschrijf de organisatiestructuur die zich afspeelt rondom het proces. Geef gerelateerde processen en de betrokken instanties aan

Resultaat: De direct betrokkenen zijn benoemd en aan het proces gekoppeld. Bovendien dient er aangegeven welke personen van vitaal belang zijn voor het proces

- **Bepalen proces**

(sjabloon "Beschrijving Proces", Hoofdstuk 3, Bijlage 8)

Doel: Het vaststellen van een proces beschrijving

Kernpunten:
1. Het vaststellen van het proces op hoofdlijnen

Uitleg:
1. Een beschrijving van het doel, de aard, de afbakening, de beschrijving en de subprocessen van het proces

Resultaat: Een goede procesbeschrijving

- **Inventariseren mensen en hulpmiddelen**

(sjabloon "Beschrijving Proces", Hoofdstuk 5, Bijlage 8)

Doel: Inventarisatie van de mensen en de hulpmiddelen die van vitaal belang zijn voor een goede en tijdige uitvoering van het proces

Kernpunten:
1. Inventariseer de betrokken personen
2. Inventariseer de hulpmiddelen die nodig zijn bij de uitvoering van het proces

Uitleg:
1. Geef aan wie deze personen zijn en beschrijf hun functie
2. Geef aan welke hulpmiddelen nodig zijn voor de uitvoering van het proces en beschrijf hoe zij functioneren in het geheel

Resultaat: Een inventarisatie van mens en hulpmiddelen

- **Bepalen scope A&K-analyse**

Doel: Inhoud vaststellen van het document "beschrijving proces" en scope vaststellen voor A&K-analyse

Kernpunten:
1. Alle betrokkenen moeten overeenstemming hebben bereikt over de inhoud van het document "beschrijving proces"
2. De reikwijdte van de A&K-analyse wordt bepaald

Uitleg:
1. Overeenstemming over het te bestuderen proces
2. Vaststellen of er volstaan kan worden met één of meerdere A&K-analyses. Dit is afhankelijk van het aantal A&K-systemen (bij meer dan 3 A&K systemen is het verstandig om meerdere A&K-analyses uit te voeren)

Resultaat: Bepaling van de scope

- **Accorderen procesbeschrijving**

Doel: Acceptatie van het rapport "beschrijving proces"
Kernpunten:
1. Zorg ervoor dat de opdrachtgever akkoord gaat met de inhoud van het rapport "beschrijving proces"

Uitleg:
1. Laat duidelijkheid bestaan over de scope van de A&K-analyse en wijs de opdrachtgever op zijn eigen verantwoordelijkheden

Resultaten: Startsein voor de Afhankelijkheids- en Kwetsbaarheidsanalyse

2.3 Uitvoering

- **Plan van aanpak A&K-analyse**

(sjabloon "Plan van Aanpak A&K-analyse", Bijlage 9)

Doel: Het vastleggen van het plan van aanpak voor het uitvoeren van de A&K-analyse
Kernpunten:
1. Vaststellen van de organisatiestructuur
2. Werkwijze vastleggen
3. Afbakening van het project

Uitleg:
1. Het toewijzen van verantwoordelijkheden en functies
2. Het vastleggen van de procedure van afhandeling
3. Alle (rand)voorwaarden vaststellen, zoals wat wel en wat niet moet worden gedaan

Resultaten: Een planning en kostencalculatie

- **Beschrijven systemen**

(sjabloon "Beschrijving Systeem", Bijlage 10)

Doel: Een beschrijving opzetten van het systeem
Kernpunten:
1. Het maken van een systeemkaart
2. Het beschrijven van de koppelingen met andere systemen (architectuur)
3. Een korte beschrijving van de functionaliteit

Uitleg:
1. Een systeemkaart bevat bijvoorbeeld de omschrijving, input, output, eigenaar van het systeem verwerkt
2. Hierin worden de interfaces en interne architectuur beschreven
3. De functie van het systeem wordt bepaald

Resultaat: Een volledige systeembeschrijving

- **Uitvoeren afhankelijkheidsanalyse**

(sjabloon "Rapport Afhankelijkheidsanalyse", Hoofdstuk 4, Bijlage 11)

Doel: De afhankelijkheid bepalen van de betrokken systemen op het proces en deze waarderen op betrouwbaarheid

Kernpunten:
1. Eisen aan de betrouwbaarheid van systemen in het oog van het proces op basis van beschikbaarheid, exclusiviteit en integriteit
2. Uitleg over hoe de beoordeling tot stand is gekomen

Uitleg:
1. De eisen aan de betrouwbaarheid van een systeem worden beoordeeld op "essentieel","belangrijk","wenselijk"of "geen criterium". Hier wordt tevens een onderbouwing aan gegeven.
2. Per systeem staat beschreven hoe de beoordeling plaats heeft gevonden en hoe men tot die conclusie is gekomen.

Resultaat: Een selectie van de systemen die verder onderzocht dienen te worden in een kwetsbaarheidsanalyse

- **Accorderen A-analyse**

Doel: Acceptatie van het rapport "afhankelijkheidsanalyse"

Kernpunten:
1. Zorg ervoor dat de project groep en opdrachtgever akkoord gaan met het rapport "afhankelijkheidsanalyse"

Uitleg:
1. Zorg ervoor dat alle betrokkenen overeenstemming bereiken over de inhoud van het rapport "afhankelijkheidsanalyse" en alle betrouwbaarheidseisen die aan ieder systeem zijn gesteld

Resultaat: Startsein voor de uitvoering van kwetsbaarheidsanalyse

- **Uitvoering K-analyse**

(sjabloon "Rapport Kwetsbaarheidsanalyse", Bijlage 12)

Doel: De kwetsbaarheid bepalen van de betrokken systemen

Kernpunten:
1. Maak gebruik van de checklist om te controleren aan welke eisen nog niet voldaan zijn in het oog van informatiebeveiliging
2. Bekijk per systeem waar de kwetsbaarheden liggen

Uitleg:
1. Vul de checklist voor ieder systeem naar behoren in
2. Laat per systeem zien bij welke eis een kwetsbaarheid ligt, wat de bevindingen zijn, welke conclusie kan worden getroffen, welke maatregelen of voorzieningen getroffen moeten worden en eventueel enkele opmerkingen over het gevonden resultaat

Resultaat: Een overzicht van de maatregelen en voorzieningen die toegepast kunnen worden en een beoordeling over de haalbaarheid van een bepaalde maatregel

- **Opstellen informatiebeveiligingsplan**

(sjabloon "Informatiebeveiligingsplan", Hoofdstuk 3, Bijlage 13)

Doel: Zorgen voor een besluitvorming over de te treffen maatregelen in het licht van de informatiebeveiliging

Kernpunten:
1. Per systeem wordt de maatregel uit de K-analyse overgenomen
2. Bekijk hoeveel inspanning iedere maatregel met zich meebrengt
3. Geef een indicatie van de omvang van de mogelijke gevolgen van de risico's
4. Vorm een besluit op basis van de beschikbare informatie (zie ook "vaststellen te nemen maatregelen")
5. Geef enkele opmerkingen op basis van de genomen besluiten, maatregelen en beschikbare informatie

Uitleg:
1. De maatregelen zijn uitkomsten afkomstig uit de K-analyse
2. Geef aan of de maatregel of voorziening weinig, redelijk veel of veel inspanning vergt. Vermeldt ook een uitleg
3. Geef aan welk risico er wordt genomen als een maatregel niet wordt doorgevoerd
4. Geef welk besluit genomen wordt (zie ook "vaststellen te nemen maatregelen")
5. Geef aanvullende informatie over waarom de maatregel is genomen of wat de kosten zijn

Resultaat: Een pakket met te nemen maatregelen per systeem

- **Vaststellen te nemen maatregelen**

(sjabloon "Informatiebeveiligingsplan", Hoofdstuk 4, Bijlage 13)

Doel: Het samenvatten van de te nemen maatregelen

Kernpunten:
1. Laat de opdrachtgever besluiten of een maatregel doorgevoerd moet worden

Uitleg:
1. De opdrachtgever neemt een besluit op basis van het informatiebeveiligingsplan. Alle besluiten worden in een actielijst geplaatst waarin een planning voor de uitvoering van de maatregel, een verantwoordelijk voor de uitvoering en de mate van inspanning wordt genoemd

Resultaat: Een actielijst met uit te voeren maatregelen

- **Vaststellen informatiebeveiligingsplan**

Doel: Planning en uitvoering van het informatiebeveiligingsbeleid

Kernpunten:
1. Draag zorg voor het uitvoeren van de actielijst

Uitleg:
1. Laat de actielijst goedkeuren door het management en zorgen voor controle op de uitvoering

Resultaat: Een plan van aanpak voor het door te voeren informatiebeveiligingsbeleid

3 A-analyse

3.1 Procesbeschrijving

In de afhankelijkheidsanalyse wordt een analyse gemaakt welke systemen verantwoordelijk zijn voor het goed functioneren van het hoofdproces. In deze analyse is het van belang dat er een complete procesbeschrijving is op systeemniveau. Als eerste is deze procesbeschrijving in tekst uitgewerkt om duidelijk te maken wat van ieder systeem de functie is in het oog van het proces. Vervolgens worden de systemen schematisch weergegeven. De schematische procesbeschrijving is bedoeld om een goed beeld te schetsen van de systemen en de onderlinge koppelingen daartussen. Het proces is gevisualiseerd weergegeven op systeemniveau. Met dit beeld in gedachte wordt de afhankelijkheidsanalyse verder uitgewerkt.

3.2 Betrouwbaarheidseisen

De betrouwbaarheid van het proces is afhankelijk van de betrouwbaarheid van de systemen waar het proces van afhangt. De systemen worden beoordeeld op drie betrouwbaarheidsaspecten. De betrouwbaarheidsaspecten waar rekening mee gehouden wordt, zijn de beschikbaarheid, exclusiviteit en integriteit.

- **Beschikbaarheid**

Met beschikbaarheid wordt aangegeven de mate waarin ongestoorde voortgang van de informatievoorziening is verzekerd. Hiermee wordt aangegeven hoeveel uitval een systeem mag hebben.

- **Exclusiviteit**

Met exclusiviteit wordt aangegeven de mate waarin de bevoegdheid de mogelijkheid tot uitlezing, kopiëren of kennisnemen tot een gedefinieerde groep van gerechtigden is beperkt. Hiermee is een groep aangegeven die beschikking mag hebben over toegang tot de informatie.

- **Integriteit**

Met integriteit wordt aangegeven de mate waarin gegevens of informatie in overeenstemming is met de afgebeelde realiteit en niets ten onrechte wordt achterhouden. Hierbij gaat het om de juistheid, volledigheid, actualiteit, consistentie en betrouwbaarheid van de informatie.

Aan de betrouwbaarheidsaspecten worden waarderingsnormen toegekend in vier categorieën. De betrouwbaarheidsaspecten worden gewaardeerd op "essentieel","belangrijk","wenselijk" en "geen criterium". In een schema in bijlage 14 staan de verschillende waarderingsnormen en betrouwbaarheidsaspecten tegen elkaar afgezet. De bedoeling is dat ieder systeem op de verschillende betrouwbaarheidsaspecten wordt gewaardeerd met de norm zoals gegeven in bijlage 14. Het waarderen van de verschillende systemen gebeurt in overleg. Bij dit overleg zijn proces- en technische

specialisten, gebruikers, klankbordgroepleden, projectleden en eventueel managementteamleden aanwezig. Er wordt per systeem een besluit genomen welke waardering aan welk betrouwbaarheidsaspect word toegekend. De waarderingsnorm zoals in bijlage 14 is beschreven, is afkomstig van het ACIB (Advies en Coördinatiepunt InformatieBeveiliging).

3.3 Kwetsbaarheidsanalyse

Als alle systemen zijn beoordeeld moet er een selectie worden gemaakt van de systemen die in aanmerking komen voor een kwetsbaarheidsanalyse. Alleen de systemen die van vitaal belang zijn voor een goede tijdige uitvoering van het proces worden in de kwetsbaarheidsanalyse geanalyseerd. Dit houdt in dat alle systemen die als "essentieel" en "belangrijk" worden beoordeeld in de afhankelijkheidsanalyse, in aanmerking komen voor een kwetsbaarheidsanalyse. Het gaat hierbij om een globale inschatting van alle betrouwbaarheidsaspecten. Met andere woorden, uitgaande van de functie van het systeem wordt ieder betrouwbaarheidsaspect een weegfactor toegekend wat uiteindelijk tot een totaal oordeel van de waarderingsnorm leidt.

3.4 Voorstel

In mijn onderzoek is de vraag aan de orde gesteld te kijken of er een meer kwantitatieve manier is om tot een waarderingsnorm te komen. Hier heb ik naar gekeken en ben tot volgend voorstel gekomen.

Allereerst moet een maatstaf voor de betrouwbaarheid worden bepaald. De betrouwbaarheid is een kans dat een systeem niet functioneert zoals het zou moeten. Het gaat hierbij dus om de kans dat een systeem uitvalt.

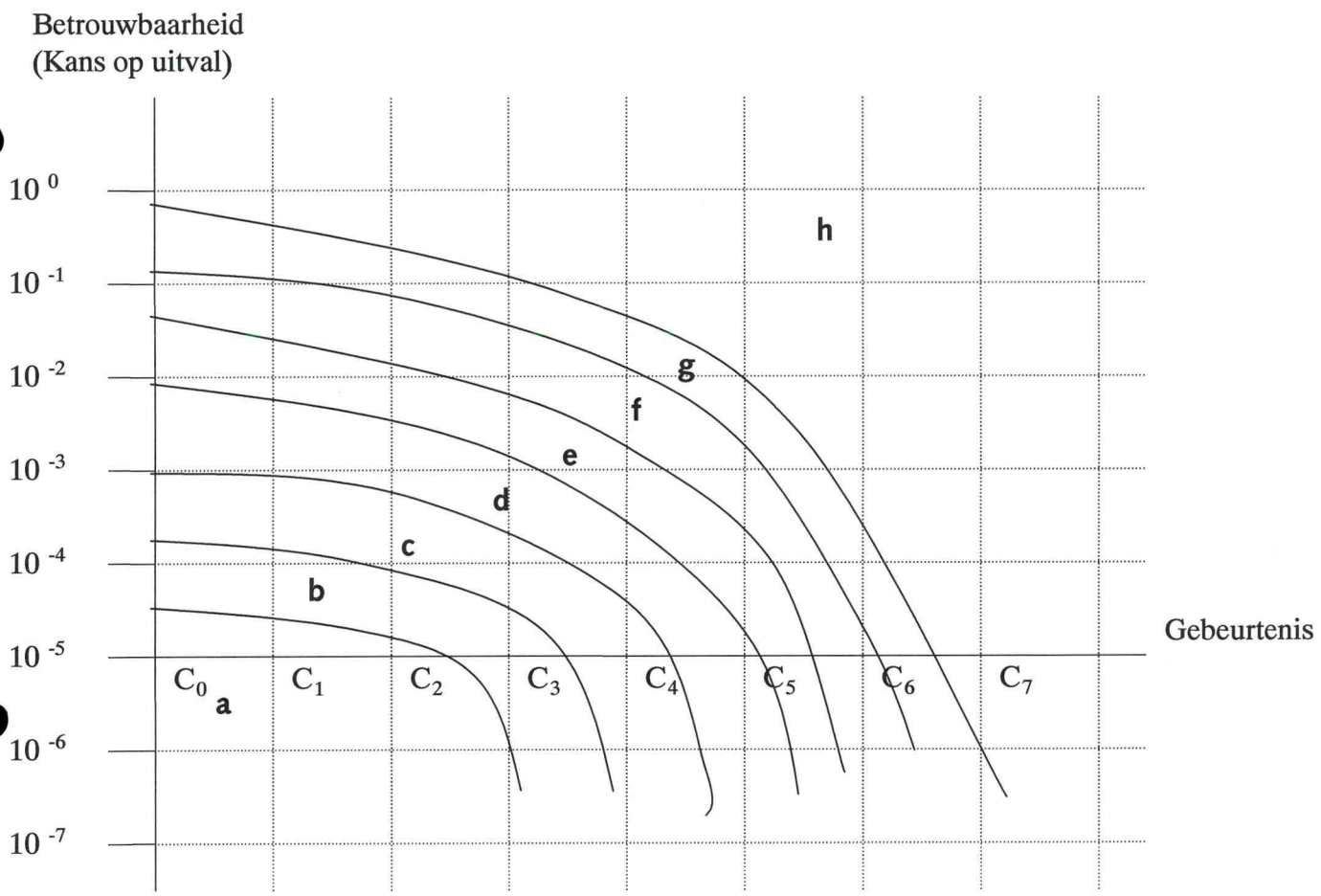
Ten tweede moet een maatstaf worden bepaald om de ernst van de gevolgen te bepalen. Geld is de meest tastbare maatstaf waarmee gerekend kan worden. Er zijn twee mogelijke gevolgen als een maatschappelijk vitaal proces uitvalt. Dit zijn gevolgen voor de mens en gevolgen voor de maatschappij. Bij gevolgen voor de maatschappij is te denken aan bijvoorbeeld files of beschadiging aan bruggen. Bij gevolgen voor de mens kunnen dat doden en gewonden zijn. Gevolgen voor de maatschappij zijn vrij gemakkelijk in geld uit te drukken. Bij de mens is dat veel complexer en kan dit bij veel mensen op ethische bezwaren stuiten. Voor mijn voorstel heb ik dit echter toch geprobeerd. Voor gevolgen voor de mens is een inschatting gemaakt, uitgedrukt in geld. Deze inschatting staat in de volgende tabel uitgewerkt.

Incident (1 persoon)	Gemiddelde economische verlies van de maatschappij in euro's
Licht gewond	10000 (geschat)
Zwaar gewond	500.000 (geschat)
Overleden	3.400.000 (bepaling EU)

Als de gevolgen voor de mens en de maatschappij bij elkaar worden opgeteld, is het bedrag bepaald van welke schade de maatschappij lijdt als een bepaalde gebeurtenis plaatsvindt. Vervolgens wordt een situatie geschetst, een gebeurtenis. De gebeurtenissen zijn in geld uitgedrukt. De gebeurtenissen zijn in de tabel op de volgende pagina bepaald.

Gebeurtenis	Maatschappelijke schade in euro's	Uitgeschreven
C_0	10^2	100
C_1	10^4	10.000
C_2	10^6	1.000.000
C_3	10^8	100.000.000
C_4	10^{10}	10.000.000.000
C_5	10^{12}	1.000.000.000.000
C_6	10^{14}	100.000.000.000.000
C_7	$> 10^{14}$	meer dan 100.000.000.000.000

Hierin is C_0 de minst erge gebeurtenis en C_7 de meest erge gebeurtenis. De kans en de gebeurtenis worden tegen elkaar uitgezet in een grafiek met logaritmische assen. De grafiek staat hieronder getekend.



In bovenstaande grafiek staat een kans op het falen van een systeem uitgezet tegen de kosten voor de maatschappij van de gebeurtenis als het gevolg van het falen. De ernst van het falen is onderverdeeld in 8 categorieën. Hiermee is de wenselijkheid van een gebeurtenis bepaald. Hier is "h" de meest ongewenste gebeurtenis en "a" de meest gewenste gebeurtenis.

Wat voor het VIR nu van belang is de bepaling van afhankelijkheid en kwetsbaarheid. Voor een proces hangt dat van systemen af. Er moet bepaald worden of een systeem "essentieel", "belangrijk" of "wenselijk" is voor een proces. Dit kan met behulp van de wenselijkheid. In onderstaande tabel is dat weergegeven.

Wenselijkheid	Wenselijkheidsbepaling voor het systeem
h	Geen maatregel is voldoende
g	Essentieel
f	Essentieel
e	Belangrijk
d	Belangrijk
c	Wenselijk
b	Wenselijk
a	Geen maatregelen nodig

Op deze manier is een meer kwantitatieve methode gegeven waarop de afhankelijkheid van een systeem beter bepaald kan worden. De indicaties die hier zijn gegeven zijn geen wet van meden en persen, maar een inschatting die de werkelijkheid benaderd. In onderling overleg moeten de grenzen worden bepaald. Het gaat om het idee wat hierachter steekt.

4 Checklist A&K-analyse

Het doel van de checklist om te controleren welke doelstellingen wel of niet behaald zijn bij een informatiesysteem. Voor ieder informatiesysteem dat in de afhankelijkheidsanalyse is genoemd, zijn alleen de minimumeisen van toepassing. Voor de informatiesystemen die in aanmerking komen voor een kwetsbaarheidsanalyse, zijn alle eisen (doelstellingen) van toepassing. De checklist is uit gewerkt op doelstellingenniveau en is daarentegen niet concreet. De doelstellingen zijn afkomstig uit de code voor informatiebeveiliging opgesteld door het Nederlands Normalisatie-Instituut in samenwerking met het ministerie van Binnenlandse Zaken en het ministerie van Verkeer en Waterstaat. Het voldoen aan een doelstelling is de verantwoordelijkheid van het management en mag naar eigen inzicht worden ingevuld. Als de checklist volledig is ingevuld kan er worden doorgegaan met de kwetsbaarheidsanalyse.

- **De opbouw van de checklist**

De checklist is als volgt opgebouwd. Allereerst dient het proces aangegeven te zijn waarop de checklist betrekking heeft. Vervolgens wordt aangegeven op welk informatiesysteem de checklist betrekking heeft. Hierna volgt de checklist zelf. De kolommen zijn als volgt ingedeeld:

1) Een *nummering*: De nummering vindt plaats op dezelfde manier als in de code voor informatiebeveiliging. Deze is ook in bijlage 4 terug te vinden.
2) Een *minimumeis*: Als een bepaalde doelstelling terugkomt in de handreiking minimumeisen is de deze met een gekleurd vlak aangegeven. Aan deze minimumeisen moet voldaan worden volgens de baseline die het ministerie van Verkeer en Waterstaat heeft ontwikkeld.
3) De *eisen*: Dit zijn de eisen (doelstellingen) die afkomstig zijn vanuit de code voor informatiebeveiliging.
4) De *conclusie*: Aan iedere eis kunnen drie mogelijke conclusies worden verbonden. Deze conclusies zijn:
   a) "Onvoldoende maatregelen" getroffen: De (minimum)eis is van toepassing en er zijn geen of onvoldoende maatregelen getroffen.
   b) "Voldoende maatregelen" getroffen: De (minimum)eis is van toepassing en er zijn voldoende maatregelen getroffen.
   c) "NVT": De (minimum)eis is niet van toepassing op het systeem.
5) Een *toelichting*: Op de conclusie die is getrokken, kan een toelichting worden gegeven met betrekking tot de beoordeling van de eis.

- **De invulling van de checklist**

De checklist is bestaat uit 10 categorieën. Elk van de deze categorieën is onderverdeeld in één of meerdere subcategorieën. De eisen / doelstellingen die betrekking hebben op de subcategorie staan daaronder genoemd. Voor alle systemen die in de afhankelijkheidsanalyse worden genoemd gelden alleen de minimumeisen. Voor de systemen waar een kwetsbaarheidsanalyse op dient te worden uitgevoerd, gelden alle eisen / doelstellingen die in de checklist zijn genoemd.

In de eerste kolom staat de nummering van de eis. De nummering is overgenomen uit de code voor informatiebeveiliging uit hoofdstuk 4. Van dezelfde nummering is gebruikgemaakt in bijlage 4.

De tweede kolom geeft aan of de eis een minimumeis is volgens de baseline die door het ministerie van Verkeer & Waterstaat is opgesteld. Deze minimumeisen zijn van toepassing op alle systemen die in de afhankelijkheidsanalyse worden genoemd.

In de derde kolom staan de eisen opgesomd. Een nadere uitleg voor deze eisen / doelstellingen staat beschreven in bijlage 4. Dit is het vierde hoofdstuk van deel 2 van de code voor informatiebeveiliging. Voor meer uitleg over de eisen / doelstelling kan de code voor informatiebeveiliging worden geraadpleegd.

In de vierde kolom kan worden aangegeven wat het eindoordeel is van de eis / doelstelling ten opzichte van het systeem dat wordt bekeken. Er zijn drie mogelijkheden:

- De eis is van toepassing en er zijn geen of onvoldoende maatregelen getroffen.
- De eis is van toepassing en er zijn voldoende maatregelen getroffen
- De eis is niet van toepassing op het systeem

Het eindoordeel kan simpel worden aangegeven door het zetten van bijvoorbeeld een kruis in het daarvoor bedoelde hokje. Later in dit hoofdstuk wordt nog aangegeven hoe de beoordeling plaatsvindt.

In de vijfde kolom is ruimte overgelaten om een toelichting te geven op de conclusie die is getrokken.

- **Beoordeling**

De beoordeling van een eis / doelstelling vindt plaats op zowel het betrouwbaarheidsaspect als de component waarop het systeem betrekking heeft. De betrouwbaarheidsaspecten zijn:

1. Beschikbaarheid
2. Exclusiviteit
3. Integriteit

De componenten waarop een systeem betrekking kan hebben zijn:

1. Mens
2. Apparatuur (hardware)
3. Programmatuur (software)
4. Gegevens
5. Omgeving
6. Organisatie
7. Diensten

Zowel het betrouwbaarheidsaspect als de component moeten worden meegenomen in het eindoordeel. De component en het betrouwbaarheidsaspect hebben invloed op elkaar. In onderstaande tabel zijn de betrouwbaarheidsaspecten uitgezet tegen de componenten. De combinatie tussen beiden is in deze tabel genummerd. Dit om onderscheidt te maken tussen de verschillende componenten en betrouwbaarheidsaspecten.

Component / Betrouwbaarheidsaspect	1. Mens	2. Apparatuur (Hardware)	3. Programmatuur (Software)	4. Gegevens	5. Omgeving	6. Organisatie	7. Diensten
1. Beschikbaarheid	1.1	1.2	1.3	1.4	1.5	1.6	1.7
2. Exclusiviteit	2.1	2.2	2.3	2.4	2.5	2.6	2.7
3. Integriteit	3.1	3.2	3.3	3.4	3.5	3.6	3.7

Als een eis / doelstelling van toepassing is, moet een beoordeling daarvan plaatsvinden. De eis / doelstelling wordt beoordeeld op ieder betrouwbaarheidsaspect van de component. Er moet worden gekeken of voldoende maatregelen zijn getroffen om eventueel falen van het systeem door toedoen van een betrouwbaarheidsaspect van een component is afgevangen. Niet ieder betrouwbaarheidsaspect of component zal voor bepaalde eisen van toepassing zijn. Echter voor degene die wel van toepassing zijn geldt dat een eis / doelstellingen pas op "voldoende maatregelen getroffen" mag worden beoordeeld als voor alle overgebleven combinaties een voldoende is gescoord. Als één van de combinaties wordt beoordeeld als onvoldoende, wordt de eis beoordeeld als "Onvoldoende maatregelen getroffen". In de kolom "toelichting" kan het nummer worden neergezet waarbij de combinatie tussen een betrouwbaarheidsaspect en een component een onvoldoende scoort. Als een eis / doelstelling wordt beoordeeld op "onvoldoende maatregelen getroffen", dan wordt die eis / doelstelling meegenomen in de kwetsbaarheidsanalyse. Als een systeem niet in aanmerking komt voor een kwetsbaarheidsanalyse en een minimumeis wordt niet behaald voor dat systeem dan dienen er maatregelen te worden getroffen om te zorgen dat een systeem wel voldoet aan de minimumeisen.

- **Voorbeeld**

Dit voorbeeld betreft een fictief systeem in een vitaal proces.

Hieronder staat een deel van de tabel die in bijlage 3 is genoemd.

Nummering	Minimumeis	Eisen	Onvoldoende maatregelen	Voldoende maatregelen	NVT	Toelichting
4.5.2		*Beveiliging van apparatuur*				
4.5.2.1	■	Het plaatsen en beveiligen van apparatuur				
4.5.2.2	■	Stroomvoorziening				
4.5.2.3		Beveiliging van kabels				
4.5.2.4		Onderhoud van apparatuur				
4.5.2.5		Beveiliging van apparatuur buiten de locatie				
4.5.2.6	■	Veilig afvoeren en hergebruiken van apparatuur				

De verklaring van de eisen / doelstellingen die in de tabel staan beschreven, staan opgesomd in bijlage 4. Van dit onderdeel van de tabel betekent dat het volgende.

4.5.2 Beveiliging van apparatuur

Doelstelling: het voorkomen van verlies, schade of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering.

4.5.2.1 Het plaatsen en beveiligen van apparatuur
Apparatuur moet zodanig geplaatst en beveiligd zijn dat de risico's van schade en storing van buitenaf en de kansen op ongeautoriseerde toegang beperkt zijn.
4.5.2.2 Stroomvoorziening
Apparatuur moet zijn beveiligd tegen stroomstoringen en andere elektrische storingen.
4.5.2.3 Beveiliging van kabels
Voedings- en telecommunicatiebekabeling die gebruikt worden voor dataverkeer of ondersteunende informatiediensten moeten zijn beveiligd tegen interceptie of beschadiging.
4.5.2.4 Onderhoud van apparatuur
Apparatuur moet op correcte wijze worden onderhouden, in overeenstemming met de instructies van de fabrikant en / of gedocumenteerde procedures, om de permanente beschikbaarheid en integriteit ervan te kunnen waarborgen.
4.5.2.5 Beveiliging van apparatuur buiten de locatie
Er moeten beveiligingsprocedures en –maatregelen worden gebruikt om apparatuur buiten het bedrijfsterrein van de organisatie te beveiligen.
4.5.2.6 Veilig afvoeren en hergebruiken van apparatuur
Vóór afvoer of hergebruik van apparatuur moet de informatie die erop aanwezig is worden verwijderd.

Voor het fictieve systeem kan de tabel als volgt worden ingevuld, als geen verder onderzoek in de vorm van een kwetsbaarheidsanalyse.

Dit resultaat betekent dat voor de eis / doelstelling 4.5.2.1 onvoldoende

Nummering	Minimumeis	Eisen	Onvoldoende maatregelen	Voldoende maatregelen	NVT	Toelichting
4.5.2		*Beveiliging van apparatuur*				
4.5.2.1		Het plaatsen en beveiligen van apparatuur	X			2.6
4.5.2.2		Stroomvoorziening		X		
4.5.2.3		Beveiliging van kabels				
4.5.2.4		Onderhoud van apparatuur				
4.5.2.5		Beveiliging van apparatuur buiten de locatie				
4.5.2.6		Veilig afvoeren en hergebruiken van apparatuur		X		

maatregelen zijn getroffen. Voor het betrouwbaarheidsaspect "exclusiviteit" dat betrekking heeft op de component "apparatuur" zijn niet voldoende maatregelen zijn getroffen. Voor dit systeem betekent dat aanpassingen moeten worden gedaan op dat vlak om wel te voldoen aan de eis, mits de oplossing binnen enige redelijkheid valt.

Nummering	Minimumeis	Eisen	Onvoldoende maatregelen	Voldoende maatregelen	NVT	Toelichting
4.5.2		*Beveiliging van apparatuur*				
4.5.2.1		Het plaatsen en beveiligen van apparatuur	X			2.6
4.5.2.2		Stroomvoorziening		X		
4.5.2.3		Beveiliging van kabels		X		
4.5.2.4		Onderhoud van apparatuur			X	
4.5.2.5		Beveiliging van apparatuur buiten de locatie	X			1.1 / 1.6 / 3.2
4.5.2.6		Veilig afvoeren en hergebruiken van apparatuur		X		

Voor het fictieve systeem kan de tabel als volgt worden ingevuld, als voor het systeem een kwetsbaarheidsanalyse nodig is.

Dit betekent dat de eisen / doelstellingen 4.5.2.1 en 4.5.2.5 worden meegenomen in de kwetsbaarheidsanalyse.

5 K-analyse

Het doel van de kwetsbaarheidsanalyse is aangeven waar de kwetsbaarheden van een vitaal systeem in een proces liggen. Naar aanleiding van de afhankelijkheidsanalyse is de checklist ingevuld voor ieder systeem die een kwetsbaarheidsanalyse moeten ondergaan. Uit deze checklist blijkt welke doelstellingen wel of niet behaald zijn. In de kwetsbaarheidsanalyse wordt per systeem iedere doelstelling die niet behaald is, opgesomd.

Als een bepaalde doelstelling niet behaald is, moeten de volgende zaken worden aangegeven:

1. Een *bevinding*: Eventuele risico's zijn aangegeven, als een bepaalde doelstelling niet behaald wordt.
2. Een *conclusie*: Hier kan de conclusie worden aangegeven die heeft geleid tot het noemen van de doelstelling in de kwetsbaarheidsanalyse.
3. Een *maatregel*: Een opsomming van maatregelen die leiden tot een vermindering van de risico's.
4. Een *opmerking*: Een toelichting op het voorgaande kan de materie verduidelijken.

Als alle niet behaalde doelstellingen voor alle systemen zijn behandeld, kan het traject worden vervolgd met het informatiebeveiligingsplan.

6 Informatiebeveiligingsplan

6.1 Inhoud

Het doel van het informatiebeveiligingsplan is om een document op te stellen waarin onomstotelijk vast is gelegd welke maatregelen moeten worden getroffen. Het document beschrijft de plannen voor de optimale informatiebeveiliging per systeem.

Per systeem worden de volgende zaken aangegeven:

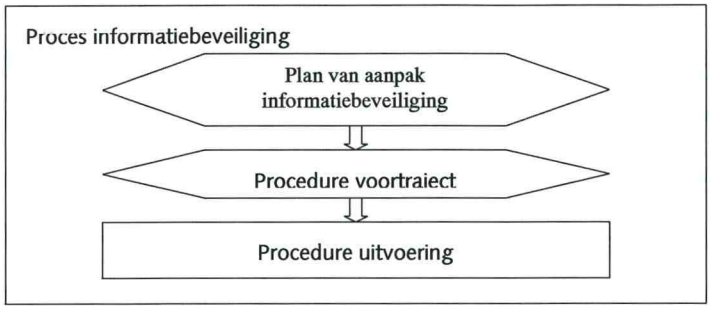
1. Een *maatregel*: Dit is de maatregel die uit de kwetsbaarheidanalyse naar voren is gekomen.
2. Een *indicatie van de inspanning*: Hier kan een indicatie van de inspanning van de maatregel worden gemaakt. Dit kan zowel een absolute als een relatieve inschatting zijn.
3. Een *omvang van de mogelijke gevolgen van risico's*: Hier kan worden aangegeven wat de mogelijke gevolgen kunnen zijn als een bepaalde maatregel niet wordt uitgevoerd.
4. Een *besluit*: Op basis van de gegeven informatie neemt het management een besluit of een bepaalde maatregel wel of niet genomen moet worden.
5. Een *opmerking*: Hier kunnen opmerkingen worden geplaatst die betrekking hebben op de maatregel of op de genomen beslissing.

6.2 Gevolgen Informatiebeveiligingsbeleid

Na het opstellen van dit document is het in het oog van de informatiebeveiliging van groot belang dat alle maatregelen waarvan is besloten om deze door te voeren, worden uitgevoerd. De maatregelen zijn namelijk weloverwogen tot stand gekomen en er is veel onderzoek aan te pas gekomen om te controleren of bepaalde systemen aan het informatiebeveiligingsbeleid van RWS / V&W voldoen. Het management moet na het opstellen van het informatiebeveiligingsplan er zorg voor dragen dat alle maatregelen worden uitgevoerd. Tevens moeten zij toezien op de naleving hiervan. Dit houdt ook in dat evaluatie en controle moet worden uitgevoerd op het informatiebeveiligingsplan. Als alle stappen in dit proces goed worden uitgevoerd en blijven worden uitgevoerd, dan kan men met recht spreken van een informatiebeveiligingsbeleid volgens het boekje. Alle risico's die na dit onderzoek nog bestaan worden bewust genomen. Er komt alleen een gevaar om de hoek kijken. Tijden veranderen snel en de technische mogelijkheden ook. Nieuwe gevaren kunnen opdoemen. Draag er zorg voor om nieuwe gevaren zo snel mogelijk te onderkennen en hier naar te handelen.

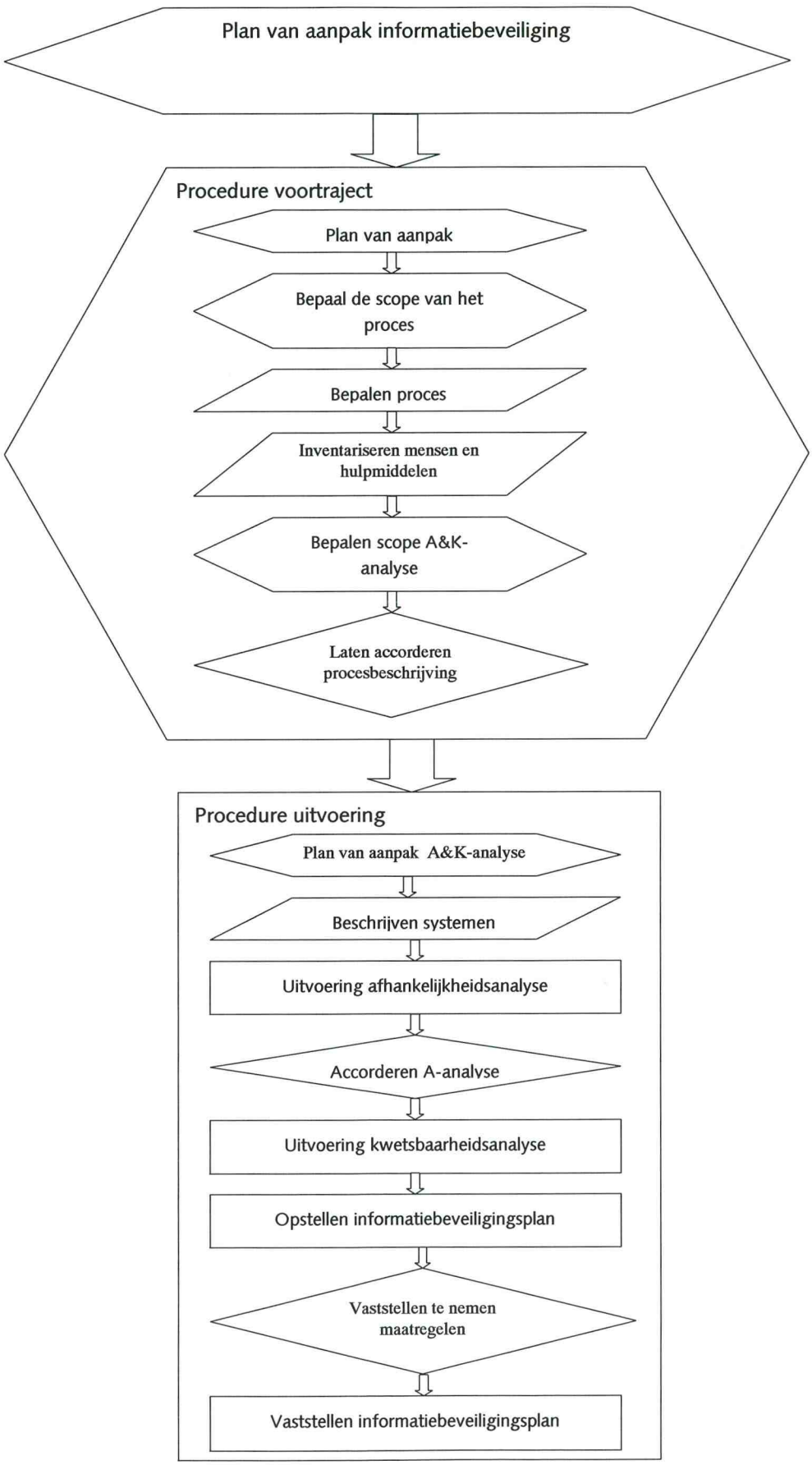
Bijlage 1

Procedure voor informatiebeveiliging



Bijlage 2

Proces voor informatiebeveiliging



Bijlage 3

Checklist minimumeisen

Component / Betrouwbaarheidsaspect	1. Mens	2. Apparatuur (Hardware)	3. Programmatuur (Software)	4. Gegevens	5. Omgeving	6. Organisatie	7. Diensten
1. Beschikbaarheid	1.1	1.2	1.3	1.4	1.5	1.6	1.7
2. Exclusiviteit	2.1	2.2	2.3	2.4	2.5	2.6	2.7
3. Integriteit	3.1	3.2	3.3	3.4	3.5	3.6	3.7

4	Gedetailleerde Beveiligingsdoelstellingen en Maatregelen					
Proces:						
Systeem:						
Nummering	Minimumeis	Eisen	Conclusie: Onvoldoende maatregelen	Conclusie: Voldoende maatregelen	Conclusie: NVT	Toelichting
4.1		**Beveiligingsbeleid**				
4.1.1		*Informatiebeveiligingsbeleid*				
4.1.1.1	■	Beleidsdocument voor informatiebeveiliging				
4.1.1.2	■	Beoordeling en evaluatie				
4.2		**Beveiligingsorganisatie**				
4.2.1		*De organisatorische infrastructuur voor informatiebeveiliging*				
4.2.1.1		Managementforum voor informatiebeveiliging				
4.2.1.2		Coördinatie van informatiebeveiliging				
4.2.1.3	■	Toewijzing van verantwoordelijkheden voor informatiebeveiliging				
4.2.1.4		Autorisatieproces voor IT-voorzieningen				
4.2.1.5		Specialistisch advies over informatiebeveiliging				
4.2.1.6		Samenwerking tussen organisaties				
4.2.1.7		Onafhankelijke beoordeling van informatiebeveiliging				
4.2.2		*Beveiliging van toegang door derden*				
4.2.2.1		Identificeren van risico's van toegang door derden				
4.2.2.2	■	Beveiligingseisen in contracten met derden				
4.2.3		*Uitbesteding*				
4.2.3.1	■	Beveiligingseisen in uitbestedingcontracten				
4.3		**Classificatie en beheer van bedrijfsmiddelen**				
4.3.1		*Verantwoording voor bedrijfsmiddelen*				
4.3.1.1		Overzicht van bedrijfsmiddelen				
4.3.2		*Classificatie van informatie*				
4.3.2.1	■	Richtlijnen voor het classificeren				
4.3.2.2		Labelen en verwerken van informatie				

Proces:						
Systeem:						
Nummering	Minimumeis	Eisen	Conclusie: Onvoldoende maatregelen	Conclusie: Voldoende maatregelen	Conclusie: NVT	Toelichting
4.4		**Beveiligingseisen ten aanzien van personeel**				
4.4.1		*Beveiligingseisen in de functieomschrijving en bij het aannemen van personeel*				
4.4.1.1		Beveiligingseisen in de functieomschrijving				
4.4.1.2		Screening en personeelsbeleid				
4.4.1.3		Geheimhoudingsverklaring				
4.4.1.4		Arbeidscontract				
4.4.2		*Training voor gebruikers*				
4.4.2.1		Opleiding en training voor informatiebeveiliging				
4.4.3		*Reageren op beveiligingsincidenten en storingen*				
4.4.3.1		Het rapporteren van beveiligingsincidenten				
4.4.3.2		Het rapporteren van zwakke plekken in de beveiliging				
4.4.3.3		Het rapporteren van onvolkomenheden in de programmatuur				
4.4.3.4		Lering trekken uit incidenten				
4.4.3.5		Disciplinaire maatregelen				
4.5		**Fysieke beveiliging en beveiliging van de omgeving**				
4.5.1		*Beveiligde ruimten*				
4.5.1.1		Fysieke beveiliging van de omgeving				
4.5.1.2		Fysieke toegangsbeveiliging				
4.5.1.3		Beveiliging van kantoren, ruimten en voorzieningen				
4.5.1.4		Werken in beveiligde ruimten				
4.5.1.5		Afzonderlijke ruimten voor laden en lossen van goederen				
4.5.2		*Beveiliging van apparatuur*				
4.5.2.1		Het plaatsen en beveiligen van apparatuur				
4.5.2.2		Stroomvoorziening				
4.5.2.3		Beveiliging van kabels				
4.5.2.4		Onderhoud van apparatuur				
4.5.2.5		Beveiliging van apparatuur buiten de locatie				
4.5.2.6		Veilig afvoeren en hergebruiken van apparatuur				
4.5.3		*Algemene beveiligingsmaatregelen*				
4.5.3.1		Clear desk en clear screen policy				
4.5.3.2		Het verwijderen van bedrijfseigendommen				

Proces:						
Systeem:						
Nummering	Minimumeis	Eisen	Conclusie: Onvoldoende maatregelen	Conclusie: Voldoende Maatregelen	Conclusie: NVT	Toelichting
4.6		**Beheer van communicatie - en bedieningsprocessen**				
4.6.1		*Bedieningsprocedures en verantwoordelijkheden*				
4.6.1.1		Gedocumenteerde bedieningsprocedures				
4.6.1.2	■	Het beheer van wijzigingen				
4.6.1.3		Procedures voor het behandelen van incidenten				
4.6.1.4		Functiescheiding				
4.6.1.5		Scheiding van voorzieningen voor ontwikkeling en productie				
4.6.1.6		Extern beheer van voorzieningen				
4.6.2		*Systeemplanning en -acceptatie*				
4.6.2.1		Capaciteitsplanning				
4.6.2.2		Acceptatie van systemen				
4.6.3		*Bescherming tegen kwaadaardige software*				
4.6.3.1	■	Maatregelen tegen kwaadaardige software				
4.6.4		*Huisregels*				
4.6.4.1	■	Reservekopieën maken (back-ups)				
4.6.4.2		Bijhouden van een logboek				
4.6.4.3		Storingen opnemen in een logboek				
4.6.5		*Netwerkbeheer*				
4.6.5.1	■	Maatregelen voor netwerken				
4.6.6		*Behandeling en beveiliging van media*				
4.6.6.1		Management van verwijderbare computermedia				
4.6.6.2		Afvoer van media				
4.6.6.3		Procedures voor de behandeling van informatie				
4.6.6.4		Beveiliging van systeemdocumentatie				
4.6.7		*Uitwisseling van informatie en software*				
4.6.7.1	■	Overeenkomsten over het uitwisselen van informatie en software				
4.6.7.2		Beveiliging van media tijdens transport				
4.6.7.3		Beveiliging van elektronische handel (e-commerce)				
4.6.7.4		Beveiliging van elektronische post (e-mail)				
4.6.7.5		Beveiliging van elektronische kantoorsystemen				
4.6.7.6		Publiek toegankelijke systemen				
4.6.7.7		Andere vormen van gegevensuitwisseling				

Nummering	Minimumeis	Eisen	Onvoldoende maatregelen	Voldoende maatregelen	NVT	Toelichting
4.7		**Toegangsbeveiliging**				
4.7.1		*Zakelijke eisen ten aanzien van toegangsbeveiliging*				
4.7.1.1	■	Beleid ten aanzien van toegangsbeveiliging				
4.7.2		*Management van toegangsrechten / autorisatiebeheer*				
4.7.2.1		Registratie van gebruikers				
4.7.2.2		Beheer van speciale bevoegdheden				
4.7.2.3	■	Beheer van gebruikerswachtwoorden				
4.7.2.4	■	Verificatie van toegangsrechten				
4.7.3		*Verantwoordelijkheden van gebruikers*				
4.7.3.1		Gebruik van wachtwoorden				
4.7.3.2		Onbeheerde gebruikersapparatuur				
4.7.4		*Toegangsbeveiliging voor netwerken*				
4.7.4.1		Beleid ten aanzien van het gebruik van netwerkdiensten				
4.7.4.2		Verplichte route				
4.7.4.3		Authenticatie van gebruikers bij externe verbindingen				
4.7.4.4	■	Node-authenticatie				
4.7.4.5	■	Beveiliging van diagnosepoorten op afstand				
4.7.4.6	■	Scheiding in netwerken				
4.7.4.7	■	Beheer van netwerkverbindingen				
4.7.4.8		Beheer van netwerkroutering				
4.7.4.9		Beveiliging van netwerkdiensten				
4.7.5		*Toegangsbeveiliging voor besturingssystemen*				
4.7.5.1		Automatische identificatie van werkstations				
4.7.5.2	■	Aanlogprocedures voor werkstations				
4.7.5.3	■	Gebruikersidentificatie en -authenticatie				
4.7.5.4	■	Wachtwoordmanagementsysteem				
4.7.5.5		Gebruik van systeemhulpmiddelen				
4.7.5.6		Stil alarm ter bescherming van gebruikers				
4.7.5.7	■	Time-out voor werkstations				
4.7.5.8		Beperking van verbindingstijd				
4.7.6		*Toegangsbeveiliging voor toepassingen*				
4.7.6.1	■	Beperking van toegang tot informatie				
4.7.6.2		Isolatie van gevoelige systemen				
4.7.7		*Monitoring van toegang tot en gebruik van systemen*				
4.7.7.1		Vastleggen van beveiligingsrelevante activiteiten ("event-logging")				
4.7.7.2		Monitoren van systeemgebruik				
4.7.7.3		Synchronisatie van systeemklokken				
4.7.8		*Mobiele computers en telewerken*				
4.7.8.1		Mobiele computers				
4.7.8.2		Telewerken				

Proces:						
Systeem:						
Nummering	Minimumeis	Eisen	Conclusie			Toelichting
			Onvoldoende maatregelen	Voldoende Maatregelen	NVT	
4.8		**Ontwikkeling en onderhoud van systemen**				
4.8.1		*Beveiligingseisen voor systemen*				
4.8.1.1	■	Analyse en specificatie van beveiligingseisen				
4.8.2		*Beveiliging in toepassingssystemen*				
4.8.2.1		Validatie van invoergegevens				
4.8.2.2		Validatie van de interne gegevensverwerking				
4.8.2.3		Authenticatie van berichten				
4.8.2.4		Validatie van uitvoergegevens				
4.8.3		*Cryptografische beveiliging*				
4.8.3.1		Beleid ten aanzien van het gebruik van cryptografische beveiliging				
4.8.3.2		Versleuteling (encryptie)				
4.8.3.3		Digitale handtekeningen				
4.8.3.4		Onweerlegbaarheid				
4.8.3.5		Sleutelbeheer				
4.8.4		*Beveiliging van systeembestanden*				
4.8.4.1		Beheersing van operationele software				
4.8.4.2	■	Beveiliging van testgegevens				
4.8.4.3		Toegangsbeveiliging voor softwarebibliotheken				
4.8.5		*Beveiliging bij ontwikkel- en ondersteuningsprocessen*				
4.8.5.1	■	Procedures voor het beheer van wijzigingen				
4.8.5.2	■	Technische controle van wijzigingen in het besturingssysteem				
4.8.5.3	■	Restricties op wijzigingen in softwarepakketten				
4.8.5.4		Geheime communicatiekanalen en Trojaanse paarden				
4.8.5.5		Uitbestede ontwikkeling van software				
4.9		**Continuïteitsmanagement**				
4.9.1		*Aspecten van continuïteitsmanagement*				
4.9.1.1	■	Het proces van continuïteitsmanagement				
4.9.1.2		Bedrijfscontinuïteit en analyse van de mogelijke gevolgen				
4.9.1.3		Het schrijven en invoeren van continuïteitsplannen				
4.9.1.4		Structuur van de continuïteitsplanning				
4.9.1.5		Testen, onderhouden en evalueren van continuïteitsplannen				

Proces:						
Systeem:						
Nummering	Minimumeis	Eisen	Conclusie: Niet voldoende maatregelen	Voldoende maatregelen	NVT	Toelichting
4.10		**Naleving**				
4.10.1		*Naleving van wettelijke voorschriften*				
4.10.1.1		Specificatie van de van toepassing zijnde wetgeving				
4.10.1.2	■	Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)				
4.10.1.3		Beveiliging van bedrijfsdocumenten				
4.10.1.4		Bescherming van persoonsgegevens				
4.10.1.5		Voorkomen van misbruik van IT-voorzieningen				
4.10.1.6		Voorschriften ten aanzien van het gebruik van cryptografische middelen				
4.10.1.7		Verzamelen van bewijsmateriaal				
4.10.2		*Beoordeling van de naleving van het veiligheidsbeleid en de technische vereisten*				
4.10.2.1		Naleving van het beveiligingsbeleid				
4.10.2.2	■	Controle op naleving van technische normen				
4.10.3		*Overwegingen ten aanzien van systeemaudits*				
4.10.3.1		Beveiligingsmaatregelen voor systeemaudits				
4.10.3.2		Beveiliging van hulpmiddelen voor systeemaudits				

Bijlage 4

Uitleg code voor informatiebeveiliging

4 Gedetailleerde beveiligingsdoelstellingen en –maatregelen

Inhoudsopgave

4.1 Beveiligingsbeleid

4.1.1 Informatiebeveiligingsbeleid

Doelstelling: het bieden van sturing en ondersteuning van het management ten behoeve van informatiebeveiliging.

4.1.1.1 Beleidsdocument voor informatiebeveiliging

Het management moet een beleidsdocument goed keuren, uitvaardigen en op passende wijze uitdragen aan alle werknemers.

4.1.1.2 Beoordeling en evaluatie

Het beleid moet regelmatig worden beoordeeld en moet, in het geval van relevante wijzigingen aangepast worden om zeker te stellen dat het actueel blijft.

4.2 Beveiligingsorganisatie

4.2.1 De organisatorische infrastructuur voor informatiebeveiliging

Doelstelling: het managen van de informatiebeveiliging binnen de organisatie.

4.2.1.1 Managementforum voor informatiebeveiliging

Er moet een managementforum ingesteld zijn, dat zorgt voor een heldere koers en voor zichtbare ondersteuning van het management bij beveiligingsinitiatieven.

4.2.1.2 Coördinatie van informatiebeveiliging

Indien passend voor de organisatie, moet een multidisciplinair forum van managementvertegenwoordigers uit alle betrokken onderdelen van de organisatie ingesteld worden om de implementatie van maatregelen voor informatiebeveiliging te coördineren.

4.2.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging

De verantwoordelijkheden voor de bescherming van individuele bedrijfsmiddelen en voor het uitvoeren van bepaalde beveiligingsprocessen moeten duidelijk worden gedefinieerd.

4.2.1.4 Autorisatieproces voor IT-voorzieningen

Een goedkeuringsproces voor nieuwe IT-voorzieningen moet worden opgesteld.

4.2.1.5 Specialistisch advies over informatiebeveiliging

Advies over informatiebeveiliging moet worden ingewonnen bij interne of gespecialiseerde beveiligingsadviseurs en in de organisatie verspreid worden.

4.2.1.6 Samenwerking tussen organisaties

De juiste contacten moeten worden onderhouden met instanties voor wetshandhaving, regelgevende instanties, leveranciers van informatiediensten en telecommunicatiebedrijven.

4.2.1.7 Onafhankelijke beoordeling van informatiebeveiliging

De implementatie van het informatiebeveiligingsbeleid moet onafhankelijk worden beoordeeld.

4.2.2 Beveiliging van toegang door derden

Doelstelling: het handhaven van de beveiliging van IT-voorzieningen en informatie van de organisatie, waar derden toegang toe hebben.

4.2.2.1 Identificeren van risico's van toegang door derden

De risico's die verbonden zijn aan toegang door derden tot de IT-voorzieningen moeten ingeschat worden en er moeten geschikte beveiligingsmaatregelen geïmplementeerd worden.

4.2.2.2 Beveiligingseisen in contracten met derden

Overeenkomsten die betrekking hebben op de toegang tot de IT-voorzieningen van de organisatie door externe gebruikers, moeten gebaseerd zijn op een schriftelijk contract waarin alle noodzakelijke beveiligingseisen zijn opgenomen.

4.2.3 Uitbesteding

Doelstelling: het handhaven van de beveiliging van informatie, wanneer de verantwoordelijkheid voor informatieverwerking is uitbesteed aan een andere organisatie.

4.2.3.1 Beveiligingseisen in uitbestedingcontracten

Wanneer een organisatie het management en beheer over alle of een deel van haar informatiesystemen, netwerken en / of werkstations uitbesteedt, moeten de beveiligingseisen in een contract tussen de partijen aan de orde komen.

4.3 Classificatie en beheer van bedrijfsmiddelen

4.3.1 Verantwoording voor bedrijfsmiddelen

Doelstelling: het handhaven van een adequate bescherming van bedrijfsmiddelen.

4.3.1.1 Overzicht van bedrijfsmiddelen

Er moet een overzicht van alle belangrijke bedrijfsmiddelen zijn opgesteld en worden onderhouden.

4.3.2. Classificatie van informatie

Doelstelling: waarborgen dat informatiebedrijfsmiddelen een passend niveau van beveiliging krijgen.

4.3.2.1 Richtlijnen voor het classificeren

De beveiligingsclassificaties en de bijbehorende beschermende maatregelen moeten in overeenstemming zijn met de behoefte van de organisatie om informatie gemeenschappelijk te gebruiken of het gebruik ervan juist te beperken alsmede met de gevolgen voor de organisatie van een dergelijke behoefte.

4.3.2.2 Labelen en verwerken van informatie

Er moeten procedures zijn opgesteld voor het labelen en verwerken van informatie, overeenkomstig het classificatiesysteem dat door de organisatie is aangenomen.

4.4 Beveiligingseisen ten aanzien van personeel

Doelstelling: het verminderen van de risico's van menselijke fouten, diefstal, fraude of misbruik van voorzieningen.

4.4.1 Beveiligingseisen in de functieomschrijving en bij het aannemen van personeel

4.4.1.1 Beveiligingseisen in de functieomschrijving

Beveiligingsrollen en verantwoordelijkheden, zoals deze zijn vastgelegd in het beveiligingsbeleid, moeten in de functieomschrijvingen zijn opgenomen, als de functie dit vereist.

4.4.1.2 Screening en personeelsbeleid

Screening van eigen werknemers moet tijdens de sollicitatieprocedure plaats vinden.

4.4.1.3 Geheimhoudingsverklaring

Werknemers moeten bij indiensttreding een geheimhoudingsverklaring ondertekenen als onderdeel van het arbeidscontract.

4.4.1.4 Arbeidscontract

In het arbeidscontract moet de verantwoordelijkheid van de werknemer op het gebied van informatiebeveiliging zijn vastgelegd.

4.4.2 Training voor gebruikers

Doelstelling: te waarborgen dat gebruikers zich bewust zijn van de bedreigingen voor en de belangen van informatiebeveiliging en hen voorzien van de juiste middelen om het beveiligingsbeleid te ondersteunen tijdens het uitvoeren van hun normale werkzaamheden.

4.4.2.1 Opleiding en training voor informatiebeveiliging

Alle werknemers binnen de organisatie en, indien van toepassing, ook externe gebruikers, moeten een passende training en regelmatige nascholing krijgen inzake het beleid en de procedures van de organisatie.

4.4.3 Reageren op beveiligingsincidenten en storingen

Doelstelling: het minimaliseren van de schade die wordt veroorzaakt door beveiligingsincidenten en storingen, monitoren van dergelijke incidenten en er lering uit trekken.

4.4.3.1 Het rapporteren van beveiligingsincidenten

Beveiligingsincidenten moeten zo snel mogelijk via de juiste managementkanalen worden gerapporteerd.

4.4.3.2 Het rapporteren van zwakke plekken in de beveiliging

Gebruikers van IT-voorzieningen moeten verplicht worden om alle waargenomen of vermoede zwakke plekken in of bedreigingen van de beveiliging van systemen of diensten te noteren en te rapporteren.

4.4.3.3 Het rapporteren van onvolkomenheden in de programmatuur

Er moeten procedures opgesteld zijn en worden opgevolgd voor het rapporteren van onvolkomenheden in de programmatuur.

4.4.3.4 Lering trekken uit incidenten

Er moeten mechanismen beschikbaar zijn, waarmee de aard, de omvang en de kosten van incidenten en storingen kunnen worden gekwantificeerd en bewaakt.

4.4.3.5 Disciplinaire maatregelen

De schending van het beveiligingsbeleid en de beveiligingsprocedures van de organisatie door de werknemers wordt middels een formeel disciplinair proces afgehandeld.

4.5 Fysieke beveiliging en beveiliging van de omgeving

4.5.1 Beveiligde ruimten

Doelstelling: het voorkomen van ongeautoriseerde toegang tot, schade aan, of verstoring van de gebouwen en informatie van de organisatie.

4.5.1.1 Fysieke beveiliging van de omgeving

Organisaties moeten gebruik maken van beveiligde zones om ruimten die IT-voorzieningen bevatten, te beveiligen.

4.5.1.2 Fysieke toegangsbeveiliging

Beveiligde zones moeten beschermd zijn door adequate toegangsbeveiliging, zodat alleen geautoriseerd personeel toegang heeft.

4.5.1.3 Beveiliging van kantoren, ruimten en voorzieningen

Er moeten beveiligde zones zijn gecreëerd ter beveiliging van kantoren, ruimten en voorzieningen waarvoor speciale beveiligingseisen gelden.

4.5.1.4 Werken in beveiligde ruimten

Er moeten aanvullende maatregelen en richtlijnen worden toegepast bij het werken in beveiligde ruimten, om de beveiliging te vergroten van de fysieke beveiligingsmaatregelen die de beveiligde ruimte beschermen.

4.5.1.5 Afzonderlijke ruimten voor laden en lossen van goederen

Laad- en losruimten moeten zijn bewaakt en zo mogelijk zijn afgezonderd van de ITvoorzieningen, om toegang door ongeautoriseerde personen te voorkomen.

4.5.2 Beveiliging van apparatuur

Doelstelling: het voorkomen van verlies, schade of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering.

4.5.2.1 Het plaatsen en beveiligen van apparatuur

Apparatuur moet zodanig geplaatst en beveiligd zijn dat de risico's van schade en storing van buitenaf en de kansen op ongeautoriseerde toegang beperkt zijn.

4.5.2.2 Stroomvoorziening

Apparatuur moet zijn beveiligd tegen stroomstoringen en andere elektrische storingen.

4.5.2.3 Beveiliging van kabels

Voedings- en telecommunicatiebekabeling die gebruikt worden voor dataverkeer of ondersteunende informatiediensten moeten zijn beveiligd tegen interceptie of beschadiging.

4.5.2.4 Onderhoud van apparatuur

Apparatuur moet op correcte wijze worden onderhouden, in overeenstemming met de instructies van de fabrikant en / of gedocumenteerde procedures, om de permanente beschikbaarheid en integriteit ervan te kunnen waarborgen.

4.5.2.5 Beveiliging van apparatuur buiten de locatie

Er moeten beveiligingsprocedures en –maatregelen worden gebruikt om apparatuur buiten het bedrijfsterrein van de organisatie te beveiligen.

4.5.2.6 Veilig afvoeren en hergebruiken van apparatuur

Vóór afvoer of hergebruik van apparatuur moet de informatie die erop aanwezig is worden verwijderd.

4.5.3 Algemene beveiligingsmaatregelen

Doelstelling: het voorkomen van beschadiging of diefstal van informatie en IT-voorzieningen.

4.5.3.1 Clear desk en clear screen policy

Organisaties moeten een "clear desk policy" en een "clear screen policy" invoeren, om het risico van ongeautoriseerde toegang tot, verlies van, en schade aan informatie te voorkomen.

4.5.3.2 Het verwijderen van bedrijfseigendommen

Apparatuur, gegevens en software van de organisatie mogen niet zonder autorisatie worden verwijderd van het bedrijfsterrein.

4.6 Beheer van communicatie - en bedieningsprocessen

4.6.1 Bedieningsprocedures en verantwoordelijkheden

Doelstelling: het garanderen van een correcte en veilige bediening van IT-voorzieningen.

4.6.1.1 Gedocumenteerde bedieningsprocedures

De bedieningsprocedures die in het beveiligingsbeleid in **4.1.1.1** zijn vastgesteld, moeten gedocumenteerd en onderhouden worden.

4.6.1.2 Het beheer van wijzigingen

Wijzigingen in IT-voorzieningen en systemen moeten worden beheerst.

4.6.1.3 Procedures voor het behandelen van incidenten

Er moeten verantwoordelijkheden en procedures zijn vastgesteld, die waarborgen dat beveiligingsincidenten snel, effectief en ordelijk worden afgehandeld.

4.6.1.4 Functiescheiding

Taken en verantwoordelijkheidsgebieden moeten worden gescheiden om het risico van onbevoegde verandering of misbruik van informatie of diensten te verkleinen.

4.6.1.5 Scheiding van voorzieningen voor ontwikkeling en productie

Ontwikkel - en testvoorzieningen moeten worden gescheiden van productievoorzieningen.

4.6.1.6 Extern beheer van voorzieningen

Vóór het inschakelen van een extern bedrijf voor het beheer van externe voorzieningen moeten de risico's worden bepaald. Verder moeten er met het externe bedrijf passende beveiligingsmaatregelen worden overeengekomen die worden opgenomen in het contract.

4.6.2 Systeemplanning en -acceptatie

Doelstelling: het risico van systeemstoringen tot een minimum beperken.

4.6.2.1 Capaciteitsplanning

De capaciteitseisen moeten gemonitored worden en er moet een prognose worden gemaakt van de toekomstige capaciteitseisen, zodat er voldoende verwerkingscapaciteit en opslagvermogen beschikbaar is.

4.6.2.2 Acceptatie van systemen

Acceptatiecriteria voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten worden vastgesteld en passende testen moeten worden uitgevoerd voor tot acceptatie wordt overgegaan.

4.6.3 Bescherming tegen kwaadaardige software

Doelstelling: het beschermen van de integriteit van software en informatie.

4.6.3.1 Maatregelen tegen kwaadaardige software

Er moeten preventieve en detecterende maatregelen worden getroffen ter bescherming tegen kwaadaardige software en adequate procedures moeten worden ingevoerd om het bewustzijn van de gebruikers te vergroten.

4.6.4 Huisregels

Doelstelling: het handhaven van de integriteit en beschikbaarheid van informatieverwerkende en communicatiediensten.

4.6.4.1 Reservekopieën maken (back-ups)

Regelmatig moeten er reservekopieën worden gemaakt van essentiële zakelijke informatie en software.

4.6.4.2 Bijhouden van een logboek

Systeembeheerders moeten een logboek bijhouden van de werkzaamheden die zij verrichten.

4.6.4.3 Storingen opnemen in een logboek

Storingen moeten worden gerapporteerd en gecorrigeerd.

4.6.5 Netwerkbeheer

Doelstelling: het handhaven van de beveiliging van informatie in netwerken en de bescherming van de ondersteunende infrastructuur.

4.6.5.1 Maatregelen voor netwerken

Om de beveiliging van computernetwerken te bewerkstelligen en te onderhouden moet een reeks van beveiligingsmaatregelen zijn getroffen.

4.6.6 Behandeling en beveiliging van media

Doelstelling: het voorkomen van schade aan bedrijfsmiddelen en van onderbreking van bedrijfsactiviteiten.

4.6.6.1 Management van verwijderbare computermedia

Het management van verwijderbare computermedia, zoals banden, schijven, cassettes, afgedrukte rapporten moet zijn geregeld.

4.6.6.2 Afvoer van media

Media moeten op een veilige en beveiligde manier worden afgevoerd wanneer zij niet langer nodig zijn.

4.6.6.3 Procedures voor de behandeling van informatie

Er moeten procedures zijn opgesteld voor de behandeling en opslag van informatie om deze informatie te beschermen tegen ongeoorloofde openbaarmaking of misbruik.

4.6.6.4 Beveiliging van systeemdocumentatie

Systeemdocumentatie moet beveiligd zijn tegen ongeautoriseerde toegang.

4.6.7 Uitwisseling van informatie en software

Doelstelling: voorkomen dat informatie die wordt uitgewisseld tussen organisaties verloren gaat, gewijzigd of misbruikt wordt.

4.6.7.1 Overeenkomsten over het uitwisselen van informatie en software

Er moeten – in sommige gevallen formele – overeenkomsten zijn opgesteld voor het elektronisch of handmatig uitwisselen van gegevens en software tussen verschillende organisaties.

4.6.7.2 Beveiliging van media tijdens transport

Media die getransporteerd worden, moeten beschermd worden tegen ongeautoriseerde toegang, misbruik of manipulatie.

4.6.7.3 Beveiliging van elektronische handel (e-commerce)

Elektronische handel moet worden beschermd tegen frauduleuze handelingen, contractgeschillen en openbaarmaking of wijziging van informatie.

4.6.7.4 Beveiliging van elektronische post (e-mail)

Er moet een beleid zijn ontwikkeld inzake het gebruik van elektronische post en maatregelen moeten worden getroffen om de beveiligingsrisico's als gevolg van e-mail te verkleinen.

4.6.7.5 Beveiliging van elektronische kantoorsystemen

Er moet een beleid en richtlijnen zijn opgesteld en geïmplementeerd om de zakelijke en beveiligingsrisico's die elektronische kantoorsystemen met zich meebrengen te beheersen.

4.6.7.6 Publiek toegankelijke systemen

Er moet een formeel autorisatieproces plaats vinden, voordat de informatie publiek toegankelijk wordt gemaakt en de integriteit van dergelijke informatie moet worden beveiligd, om ongeoorloofde wijzigingen te voorkomen.

4.6.7.7 Andere vormen van gegevensuitwisseling

Er moeten procedures en andere maatregelen zijn ingesteld om de uitwisseling van informatie via het gebruik van stem-, fax- en videocommunicatie te beschermen.

4.7 Toegangsbeveiliging

4.7.1 Zakelijke eisen ten aanzien van toegangsbeveiliging

Doelstelling: het beheersen van de toegang tot informatie.

4.7.1.1 Beleid ten aanzien van toegangsbeveiliging

De zakelijke eisen voor toegangsbeveiliging moeten gedefinieerd en gedocumenteerd zijn en de toegang moet worden beperkt tot hetgeen bepaald is in het beleidsdocument voor toegangsbeveiliging.

4.7.2 Management van toegangsrechten / autorisatiebeheer

Doelstelling: het voorkomen van ongeautoriseerde toegang tot informatiesystemen.

4.7.2.1 Registratie van gebruikers

Er moeten formele procedures voor het registreren en afmelden van gebruikers opgesteld zijn voor toegang tot alle informatiesystemen en -diensten met meerdere gebruikers.

4.7.2.2 Beheer van speciale bevoegdheden

De toewijzing en het gebruik van speciale bevoegdheden moeten worden beperkt en gecontroleerd.

4.7.2.3 Beheer van gebruikerswachtwoorden

De toewijzing van wachtwoorden moet worden beheerst aan de hand van een formeel proces.

4.7.2.4 Verificatie van toegangsrechten

Middels een formeel proces moeten periodiek de toegangsrechten van gebruikers worden herzien.

4.7.3 Verantwoordelijkheden van gebruikers

Doelstelling: het voorkomen van ongeautoriseerde toegang door gebruikers.

4.7.3.1 Gebruik van wachtwoorden

Gebruikers moeten de goede beveiligingsgewoonten in acht nemen bij het kiezen en gebruiken van wachtwoorden.

4.7.3.2 Onbeheerde gebruikersapparatuur

Gebruikers moeten ervoor zorgen dat apparatuur bij hun (tijdelijke) afwezigheid voldoende is beveiligd.

4.7.4 Toegangsbeveiliging voor netwerken

Doelstelling: bescherming van netwerkdiensten.

4.7.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten

Gebruikers mogen alleen directe toegang krijgen tot die diensten waarvoor zij specifiek geautoriseerd zijn.

4.7.4.2 Verplichte route

De route van het werkstation naar de computerservice moet worden beheerst.

4.7.4.3 Authenticatie van gebruikers bij externe verbindingen

Voor toegang door gebruikers op afstand is een authenticatieprocedure nodig.

4.7.4.4 Node-authenticatie

De authenticiteit van verbindingen naar computers op afstand moet worden geverifieerd.

4.7.4.5 Beveiliging van diagnosepoorten op afstand

Toegang tot diagnosepoorten moet nauwlettend worden beheerst.

4.7.4.6 Scheiding in netwerken

In netwerken moeten maatregelen worden getroffen om groepen informatiediensten, gebruikers en informatiesystemen te scheiden.

4.7.4.7 Beheer van netwerkverbindingen

De mogelijkheden van gebruikers van gezamenlijke netwerken om verbindingen te maken moet worden beperkt overeenkomstig het beleid ten aanzien van toegangsbeveiliging, zoals uiteengezet in **4.7.1.1**.

4.7.4.8 Beheer van netwerkroutering

Bij gemeenschappelijke netwerken moeten beveiligingsmaatregelen voor de routering worden getroffen, overeenkomstig het beleid ten aanzien van toegang tot zakelijke toepassingen, zoals uiteengezet in **4.7.1.1**.

4.7.4.9 Beveiliging van netwerkdiensten

Er moet een duidelijke omschrijving bestaan van de beveiligingskenmerken van alle netwerkdiensten die door de organisatie worden gebruikt.

4.7.5 Toegangsbeveiliging voor besturingssystemen

Doelstelling: het voorkomen van ongeautoriseerde toegang tot computers.

4.7.5.1 Automatische identificatie van werkstations

Automatische identificatie van werkstations moet worden gebruikt om verbindingen naar bepaalde locaties en mobiele apparatuur te verifiëren.

4.7.5.2 Aanlogprocedures voor werkstations

Toegang tot informatiediensten moet verlopen via een veilig aanlogproces.

4.7.5.3 Gebruikersidentificatie en -authenticatie

Alle gebruikers moeten een unieke gebruikersidentificatie (gebruikers-ID) hebben voor eigen persoonlijk gebruik om ervoor te zorgen dat activiteiten terug te voeren zijn tot de daarvoor verantwoordelijke persoon.

4.7.5.4 Wachtwoordmanagementsysteem

Er moet een wachtwoordmanagementsysteem van kracht zijn om een effectieve, interactieve voorziening te bieden die de kwaliteit van wachtwoorden zeker stelt.

4.7.5.5 Gebruik van systeemhulpmiddelen

Het gebruik van systeemhulpmiddelen moet worden beperkt en nauwlettend worden beheerst.

4.7.5.6 Stil alarm ter bescherming van gebruikers

Er moet een stil alarm worden gebruikt voor gebruikers die de kans lopen het doelwit te worden van dwang.

4.7.5.7 Time-out voor werkstations

Voor inactieve werkstations op locaties met een verhoogd risico of werkstations die systemen met een verhoogd risico bedienen, moet na een bepaalde periode van inactiviteit een time-out worden ingesteld om toegang door onbevoegden te voorkomen.

4.7.5.8 Beperking van verbindingstijd

De verbindingstijd moet beperkt worden als aanvullende beveiliging voor toepassingen met een verhoogd risico.

4.7.6 Toegangsbeveiliging voor toepassingen

Doelstelling: het voorkomen van ongeautoriseerde toegang tot informatie in informatiesystemen.

4.7.6.1 Beperking van toegang tot informatie

Toegang tot functies van informatie- en toepassingssystemen moet worden beperkt overeenkomstig het toegangsbeleid van de organisatie zoals bepaald in **4.7.1.1**.

4.7.6.2 Isolatie van gevoelige systemen

Gevoelige systemen moeten een eigen, vast toegewezen (geïsoleerde) computeromgeving hebben.

4.7.7 Monitoring van toegang tot en gebruik van systemen

Doelstelling: het ontdekken van ongeautoriseerde activiteiten.

4.7.7.1 Vastleggen van beveiligingsrelevante activiteiten ("event-logging")

Uitzonderingen en andere gebeurtenissen die van belang zijn voor de beveiliging moeten vastgelegd worden in zogenaamde "audit logs". Deze audit logs moeten worden bijgehouden en gedurende een overeengekomen periode worden bewaard, ter ondersteuning van toekomstige onderzoeken en toegangsbewaking.

4.7.7.2 Monitoren van systeemgebruik

Er moeten procedures voor het bewaken van het gebruik van IT-voorzieningen zijn opgesteld en het resultaat van de monitoringsactiviteiten moet regelmatig worden geëvalueerd.

4.7.7.3 Synchronisatie van systeemklokken

Voor een nauwkeurige registratie moeten de systeemklokken zijn gesynchroniseerd.

4.7.8 Mobiele computers en telewerken

Doelstelling: het waarborgen van informatiebeveiliging bij het gebruik van mobiele computers en voorzieningen voor telewerken.

4.7.8.1 Mobiele computers

Er moet een formeel beleid bestaan en passende maatregelen worden genomen ter bescherming tegen de risico's van het werken met mobiele computers, met name in onbeveiligde omgevingen.

4.7.8.2 Telewerken

Er moeten een beleid en procedures zijn ontwikkeld voor het goedkeuren en beheersen van telewerkactiviteiten.

4.8 Ontwikkeling en onderhoud van systemen

4.8.1 Beveiligingseisen voor systemen

Doelstelling: waarborgen dat beveiliging wordt ingebouwd in informatiesystemen.

4.8.1.1 Analyse en specificatie van beveiligingseisen

In de eisen ten aanzien van nieuwe systemen of uitbreidingen van bestaande systemen moeten de eisen voor beveiligingsmaatregelen zijn gespecificeerd.

4.8.2 Beveiliging in toepassingssystemen

Doelstelling: het voorkomen van verlies, wijziging of misbruik van gegevens in toepassingssystemen.

4.8.2.1 Validatie van invoergegevens

Gegevens die worden ingevoerd in toepassingssystemen moeten worden gevalideerd op juistheid en geschiktheid.

4.8.2.2 Validatie van de interne gegevensverwerking

Om verminking van gegevens te kunnen opsporen, moeten geldigheidscontroles zijn ingebouwd in systemen.

4.8.2.3 Authenticatie van berichten

Authenticatie van berichten moet zijn geïmplementeerd in toepassingen, waarbij het vereist is dat de integriteit van de inhoud van het bericht wordt beveiligd.

4.8.2.4 Validatie van uitvoergegevens

Gegevensuitvoer vanuit een toepassingssysteem moet worden gevalideerd, om zeker te stellen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en passend is gezien de omstandigheden.

4.8.3 Cryptografische beveiliging

Doelstelling: het beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie.

4.8.3.1 Beleid ten aanzien van het gebruik van cryptografische beveiliging

Er moet een beleid voor het gebruik van cryptografische beveiliging zijn en worden nagevolgd.

4.8.3.2 Versleuteling (encryptie)

Versleuteling moet worden toegepast om de vertrouwelijkheid van gevoelige of kritieke informatie te beschermen.

4.8.3.3 Digitale handtekeningen

Digitale handtekeningen moeten gebruikt worden om de authenticiteit en integriteit van elektronische informatie te waarborgen.

4.8.3.4 Onweerlegbaarheid

Een dienst voor onweerlegbaarheid moet worden gebruikt om geschillen over het al dan niet plaatsvinden van een gebeurtenis of handeling op te lossen.

4.8.3.5 Sleutelbeheer

Er moet een sleutelbeheersysteem worden opgezet op basis van overeengekomen normen, procedures en methoden, ter ondersteuning van het gebruik van cryptografische technieken.

4.8.4 Beveiliging van systeembestanden

Doelstelling: ervoor zorgen dat IT-projecten en ondersteunende activiteiten op een veilige manier worden uitgevoerd.

4.8.4.1 Beheersing van operationele software

De implementatie van software op operationele systemen moet nauwlettend beheerst zijn.

4.8.4.2 Beveiliging van testgegevens

Testgegevens moeten zijn beveiligd en beheerst.

4.8.4.3 Toegangsbeveiliging voor softwarebibliotheken

Er moet een strikt toezicht worden gehouden op de toegang tot bibliotheken met bronprogramma's.

4.8.5 Beveiliging bij ontwikkel- en ondersteuningsprocessen

Doelstelling: de beveiliging van toepassingssoftware en -informatie waarborgen.

4.8.5.1 Procedures voor het beheer van wijzigingen

De implementatie van wijzigingen moet beheerst zijn door middel van een formeel proces voor het managen van wijzigingen, om corruptie van informatiesystemen zo veel mogelijk te beperken.

4.8.5.2 Technische controle van wijzigingen in het besturingssysteem

Toepassingssystemen moeten opnieuw worden beoordeeld en getest wanneer wijzigingen plaatsvinden.

4.8.5.3 Restricties op wijzigingen in softwarepakketten

Wijzigingen in softwarepakketten moeten worden ontraden en essentiële wijzigingen in software moeten nauwgezet worden beheerst.

4.8.5.4 Geheime communicatiekanalen en Trojaanse paarden

Er moet toezicht en controle plaats vinden op de aanschaf, het gebruik en de aanpassing van software, ter beveiliging tegen eventuele geheime communicatiekanalen en Trojaanse paarden.

4.8.5.5 Uitbestede ontwikkeling van software

Er moeten maatregelen worden getroffen ter beveiliging van uitbestede ontwikkeling van software.

4.9 Continuïteitsmanagement

Doelstelling: het reageren op verstoringen van bedrijfsactiviteiten en het beschermen van de kritieke bedrijfsprocessen tegen de effecten van grote storingen of calamiteiten.

4.9.1 Aspecten van continuïteitsmanagement

4.9.1.1 Het proces van continuïteitsmanagement

Er moet een beheerst proces ingesteld zijn voor het ontwikkelen en handhaven van de bedrijfscontinuïteit in de gehele organisatie.

4.9.1.2 Bedrijfscontinuïteit en analyse van de mogelijke gevolgen

Er moet een strategisch plan, op basis van een passende risicoanalyse, zijn ontwikkeld om de algehele benadering van bedrijfscontinuïteit te bepalen.

4.9.1.3 Het schrijven en invoeren van continuïteitsplannen

Er moeten plannen worden ontwikkeld om de bedrijfsactiviteiten na een onderbreking of verstoring van kritieke bedrijfsprocessen in stand te houden of tijdig te herstellen.

4.9.1.4 Structuur van de continuïteitsplanning

Er moet een consistente structuur voor bedrijfsplannen worden gehandhaafd om ervoor te zorgen dat alle plannen consistent zijn en om prioriteiten te stellen voor het uitvoeren van tests en onderhoud.

4.9.1.5 Testen, onderhouden en evalueren van continuïteitsplannen

Continuïteitsplannen moeten regelmatig worden getest en door middel van regelmatige evaluaties worden geactualiseerd, om zeker te stellen dat ze up-to-date en effectief zijn.

4.10 Naleving

4.10.1 Naleving van wettelijke voorschriften

Doelstelling: het voorkomen van schendingen van strafrechtelijke of civielrechtelijke wetgeving, wettelijke, reglementaire of contractuele verplichtingen of beveiligingseisen.

4.10.1.1 Specificatie van de van toepassing zijnde wetgeving

Alle toepasselijke wettelijke, reglementaire en contractuele vereisten moeten expliciet zijn gespecificeerd en gedocumenteerd voor ieder informatiesysteem.

4.10.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)

Er moeten passende maatregelen zijn getroffen om te waarborgen dat wordt voldaan aan de wettelijke beperkingen met betrekking tot het gebruik van materiaal, waarop intellectuele eigendomsrechten rusten, zoals auteursrecht, ontwerprechten of handelsmerken en op het gebruik van software van derden.

4.10.1.3 Beveiliging van bedrijfsdocumenten

Belangrijke bedrijfsdocumenten moeten beveiligd zijn tegen verlies, vernietiging en vervalsing.

4.10.1.4 Bescherming van persoonsgegevens

Er moeten maatregelen zijn getroffen om persoonsgegevens te beschermen overeenkomstig de desbetreffende wet- en regelgeving.

4.10.1.5 Voorkomen van misbruik van IT-voorzieningen

Voor het gebruik van deze voorzieningen moet toestemming worden verkregen van het management en er moeten maatregelen zijn getroffen om misbruik van dergelijke voorzieningen te voorkomen.

4.10.1.6 Voorschriften ten aanzien van het gebruik van cryptografische middelen

Er moeten maatregelen zijn getroffen om te waarborgen dat de nationale overeenkomsten, wetgeving, voorschriften en andere instrumenten om de toegang tot of het gebruik van cryptografische voorzieningen te controleren, worden nageleefd.

4.10.1.7 Verzamelen van bewijsmateriaal

Wanneer tegen een persoon of organisatie maatregelen moeten worden getroffen, die verband houden met de wetgeving, hetzij civielrechtelijk, hetzij strafrechtelijk, moet het voorgelegde bewijsmateriaal in overeenstemming zijn met de regels ten aanzien van bewijsmateriaal, zoals die in de betreffende wetgeving of in de regelgeving van een bepaald gerecht, waar de zaak zal worden behandeld, zijn neergelegd. Dit omvat tevens de naleving van gepubliceerde normen of praktijkcodes voor de verwerving van toelaatbaar bewijsmateriaal.

4.10.2 Beoordeling van de naleving van het veiligheidsbeleid en de technische vereisten

Doelstelling: Waarborgen dat systemen voldoen aan het beveiligingsbeleid en de geldende beveiligingsnormen van de organisatie.

4.10.2.1 Naleving van het beveiligingsbeleid

Managers moeten ervoor zorgen dat alle beveiligingsprocedures binnen hun verantwoordelijkheids-gebied op de juiste manier worden uitgevoerd en dat alle verantwoordelijkheidsgebieden binnen de organisatie regelmatig aan een beoordeling worden onderworpen, om te waarborgen dat voldaan wordt aan het beveiligingsbeleid en de beveiligingsnormen.

4.10.2.2 Controle op naleving van technische normen

Informatiesystemen moeten regelmatig worden gecontroleerd op naleving van beveiligingsnormen en standaarden.

4.10.3 Overwegingen ten aanzien van systeemaudits

Doelstelling: de effectiviteit van systeemaudits maximaliseren en de interferentie tijdens de systeemaudits minimaliseren.

4.10.3.1 Beveiligingsmaatregelen voor systeemaudits

Audits en andere activiteiten waarbij controles worden uitgevoerd op operationele systemen, moeten zorgvuldig worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.

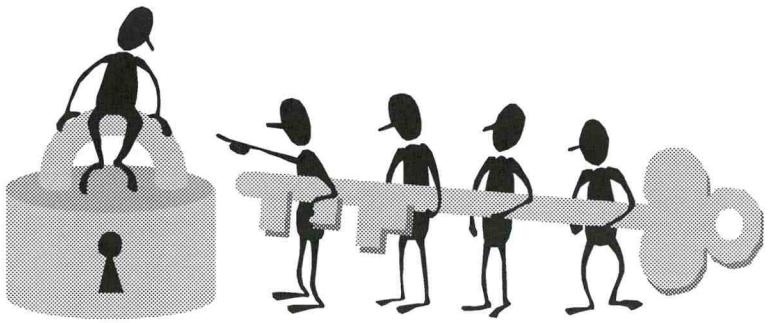
4.10.3.2 Beveiliging van hulpmiddelen voor systeemaudits

De toegang tot hulpmiddelen voor systeemaudits moet worden beveiligd, om eventueel misbruik of beschadiging te voorkomen.

Bijlage 5

Sjabloon "Plan van Aanpak Informatiebeveiliging"

Plan van Aanpak
Informatiebeveiliging bij
<naam Dienst>



Ministerie van Verkeer en Waterstaat

Colofon

Uitgave	:	
Dienst	:	
Product	:	Plan van Aanpak Informatiebeveiliging
Versie :	:	[Klik hier voor versie]
Status :	:	[Klik hier voor status]
Datum	:	[Klik hier voor datum]

Inhoudsopgave

Samenvatting

De projectopdracht is drieledig:
- voer de Quick Wins voortkomend uit de Nulmeting uit
- implementeer de Minimumeisen Informatiebeveiliging 2001 Ministerie van Verkeer en Waterstaat in de organisatie
- Inventariseer de maatschappelijk vitale processen, voer hiervoor A&K-analyses uit en implementeer de hieruit voortvloeiende maatregelen.

Verantwoordelijk projectmanager is.....

Geef verder een samenvatting van enkele essentiële onderdelen van het plan van aanpak. In aanmerking komen onder meer:
- *Cruciale succesfactoren*
- *Projectinrichting*
- *Activiteitenplan op niveau hoofdactiviteit*
- *Financiële consequenties.*

1. Introductie

In deze standaard gelden de gearceerde teksten als instructies en toelichtingen, toegespitst op de Projectmanager die het Plan van Aanpak opstelt. Deze instructies/toelichtingen vormen dus geen onderdeel van het door u op te stellen plan van aanpak. De niet gearceerde teksten, met name de indeling in hoofdstukken en paragrafen, zijn algemeen geldend en kunt u dus handhaven.

1.1. Aanleiding

Dit Plan van Aanpak van de dienst vormt een onderdeel van het project informatiebeveiliging V&W; Het doel is de informatiebeveiliging binnen de dienst en V&W-breed op een adequaat niveau te brengen. *Refereer hier aan de aanschrijving door D1 of D2).*

1.2. Accordering en bijstelling

Zowel D1 als D2 accorderen, na eventuele correctie, dit Plan van Aanpak, waarmee het definitief is. Later noodzakelijke bijstellingen op het plan accorderen D1 en D2 als afzonderlijke documenten. Het actuele Plan van Aanpak bestaat op deze wijze uit het oorspronkelijke Plan van Aanpak en de geaccordeerde bijstellingen daarop.

1.3. Toelichting structuur

De structuur van dit Plan van Aanpak is als volgt.

Na deze introductie in hoofdstuk 1 vermeldt hoofdstuk 2 wat de projectopdracht inhoudt.

Hoofdstuk 3 geeft de indeling van de uit te voeren activiteiten en beschrijft hoe die uitvoering zal gebeuren.

Hoofdstuk 4 gaat nader in op de inrichting van het project met als aspecten: organisatie, personeel, AO, financiering, informatie en techniek.

Hoofdstuk 5 geeft inzicht in de planning en de kosten.

Hoofdstuk 6 ten slotte beschrijft op welke wijze de kwaliteit van de uitvoering van het project zal worden geborgd.

2. Projectopdracht

Dit hoofdstuk dient om de gewenste veranderingen in beeld te brengen. Het beantwoordt de WAT-vraag.

2.1. Beschouwingsgebied

Het beschouwingsgebied is de informatiebeveiliging (IB) binnen de hele dienst.

Onder dienst hier te verstaan het organisatie-niveau, waarop D1 of D2 stuurt en gerapporteerd wenst te worden.

2.2. Doelstelling project

De doelstelling is het VIR inbedden in de organisatie bij de dienst als onderdeel van de hogere doelstelling: het VIR inbedden in de V&W-organisatie.

2.3. Opdrachtformulering

De projectopdracht is drieledig:
- voer de Quick Wins voortkomend uit de Nulmeting uit
- implementeer de Minimumeisen Informatiebeveiliging 2001 Ministerie van Verkeer en Waterstaat in de organisatie
- Inventariseer de maatschappelijk vitale processen en voer hiervoor A&K-analyses uit.

De gestelde volgorde geeft tevens de prioriteitsvolgorde aan.

2.4. Op te leveren producten

Het resultaat van het project moet zijn dat voor de informatiesystemen binnen de dienst alle maatregelen zijn getroffen om de IB op een in eerste instantie minimum informatiebeveiligingsniveau te brengen. Hiermee zijn tevens de voorwaarden geschapen om de IB minimaal op dat niveau te handhaven.

Tussenproducten zijn:
- Implementatieplan quick wins
- Migratieplan voor invoeren Minimumeisen Informatiebeveiliging 2001 Ministerie van Verkeer en Waterstaat
- Rapporten A&K-analyses
- Communicatie- en bewustwordingsplan

Tastbare eindproducten zijn:
- In kaart gebrachte bestuurlijke- en bedrijfsprocessen; onderverdeeld naar de categorieën "maatschappelijk vitaal" en "overig" met daarbij de keuze ten aanzien van welke processen A&K- analyses dienen plaats te vinden
- In kaart gebrachte informatiesystemen in relatie met de processen waar ze ondersteuning aan bieden
- Documentatie waaruit blijkt welke maatregelen getroffen zijn
- Beschrijving IB-beleid voor de dienst
- Beschrijving IB-organisatie

2.5. Eisen en beperkingen

De eisen die D1 of D2 stelt zijn verwoord in de aanschrijving. Het tegemoet komen aan die eisen is verwerkt in dit Plan van Aanpak. De dienst is verantwoordelijk voor het tijdig uitvoeren van de activiteiten volgens dit Plan van Aanpak.

2.6. Cruciale succesfactoren

Vermeld hier de in overleg met betrokkenen vastgestelde cruciale succesfactoren. Deze zijn sterk dienstafhankelijk. Te denken valt aan:
- *Beheersbare risico's (zie hoofdstuk 6 Kwaliteitsborging)*
- *De bewustwording van informatiebeveiliging binnen de dienst. De zorg voor IB moet breed gedragen worden door de organisatie.*
- *Een klankbordgroep of projectgroep met beslissingsbevoegdheid is van essentieel belang voor de Projectmanager.*

- *Het beschikbaar hebben van de juiste expertise, met name voor wat specialistische activiteiten, zoals het uitvoeren van een A&K-analyse,*

3. Aanpak

Bij de aanpak gaat het om de HOE-vraag: om welke activiteiten gaat het en hoe voeren we die uit. Dit hoofdstuk geeft alvast het kader aan door de hoofdactiviteiten te benoemen voor de drie trajecten en daarbij een toelichting te geven op de inhoud. Het is aan de dienst om de hoofdactiviteiten verder te verdelen in activiteiten en te bedenken hoe ieder van die activiteiten moet worden uitgevoerd. Waar zinvol verwijst dit hoofdstuk naar andere documenten die voor dat onderwerp ondersteuning kan bieden.

3.1. Quick wins

Als onderdeel van het opstellen van dit Plan van Aanpak dient u in overleg met de uitvoerders een implementatieplan op te stellen voor de noodzakelijke maatregelen uit de Nulmeting. Onderstaand is aangegeven hoe zo'n implementatieplan er uit dient te zien.

Identificatie	Maatregel	Verantwoordelijke	Mensuren	Begindatum	Einddatum

Per maatregel geeft men aan:

- *Identificatie = een verwijzing naar de maatregel in de 0-meting*
- *Maatregel = de omschrijving van de maatregel*
- *Verantwoordelijke = functionaris/persoon die verantwoordelijk is voor de tijdige uitvoering*
- *Mensuren = schatting van de inspanning voor het uitvoeren van de maatregel*
- *Begindatum = datum waarop een aanvang is of wordt gemaakt met het uitvoeren van de maatregel*
- *Einddatum = datum waarop de maatregel uitgevoerd is of zal zijn*

3.1.1. Uitvoeren implementatieplan

Het is van groot belang dat de tijdige uitvoering van het implementatieplan goed bewaakt wordt. Stel daartoe vast welk college of welke functionaris belast wordt met die bewaking. De bewaking moet actief gebeuren, waarbij de verantwoordelijke ook de getroffen maatregel moet aantonen.

3.2. Minimumeisen Informatiebeveiliging

Om voldoende inzicht te krijgen in de hoeveelheid werk die het invoeren van de Minimumeisen Informatiebeveiliging 2001 Ministerie van Verkeer en Waterstaat met zich brengt, dient u het toetsen van de bestaande situatie aan de Minimumeisen als onderdeel van het opstellen van dit Plan van Aanpak te zien.

3.2.1. Opstellen migratieplan

Definitie

Onder een migratieplan in dit verband te verstaan een plan waarin het totale traject wordt geschetst bij het stap voor stap invoeren van de maatregelen volgens de Minimumeisen Informatiebeveiliging 2001 Ministerie van Verkeer en Waterstaat. De geleidelijke invoering, met name van de organisatie, leidt tot steeds een tijdelijke situaties, waarvan de consequenties tevoren moeten worden onderkend. Uit het migratietraject moet duidelijk blijken wanneer welke (tijdelijke) maatregelen getroffen moeten worden.

Volgorde

De Handreiking Minimumeisen Informatiebeveiliging geeft reeds voldoende informatie over hoe je de verschillende onderdelen van de Minimumeisen Informatiebeveiliging 2001 Ministerie van Verkeer en Waterstaat invoert, maar niet over de volgorde. Voorrang moet worden gegeven aan:

- *het beveiligingsbeleid*
- *de beveiligingsorganisatie*
- *het beveiligingsbewustzijn.*

Als deze onderdelen goed geregeld zijn is de organisatie voldoende toegerust om het niveau van informatiebeveiliging in het vervolg te handhaven.

Processen

Houd er rekening mee dat bij het invoeren van de Minimumeisen Informatiebeveiliging 2001 Ministerie van Verkeer en Waterstaat het wenselijk kan zijn enig inzicht in de processen te hebben.

Afstemming

De planning voor de uitvoering van de maatregelen moet goed met alle betrokkenen zijn afgestemd.

3.2.2. Uitvoeren migratieplan

Het is belangrijk dat het migratieplan nauwgezet gevolgd wordt bij de uitvoering. Stel daartoe vast welk college of welke functionaris belast wordt met die bewaking. De bewaking moet actief gebeuren, waarbij de verantwoordelijke ook de getroffen maatregel moet aantonen.

3.3. A&K-analyse

De opdracht heeft alleen betrekking heeft op dat deel van een maatschappelijk vitaal proces en die informatiesystemen die zo'n proces ondersteunen waarvoor de dienst verantwoordelijk is. Onder

informatiesysteem te verstaan ieder systeem, handmatig of geautomatiseerd, dat informatie levert.

De definitie van een informatiesysteem houdt dus in dat men niet alleen aan geautomatiseerde systemen moet denken, maar ook aan (grotendeels) handmatige. De definitie houdt ook in dat systemen uitsluitend ontwikkeld voor het uitvoeren proceshandelingen (openen bruggen, bedienen sluizen) buiten de scope van het VIR vallen.

De mate van verantwoordelijkheid van de dienst voor de IB van een ondersteunend informatiesysteem hangt af van het eigenaarschap en de vorm van beheer. Zie hiervoor paragraaf 3.3.2. Informatiesystemen beschrijven.

3.3.1. Processen beschrijven

Selectie

Beschrijf alleen de maatschappelijk vitale processen voor dat deel waar de dienst verantwoordelijk voor is. We hanteren namelijk het uitgangspunt dat maatschappelijk vitale processen de hoogste prioriteit krijgen voor een A&K-analyse.

Ondersteuning

Desgewenst kan de BOF het document Proces Regisseren Verkeersdoorstroming van de Directie Zuid-Holland beschikbaar stellen als voorbeeld van een procesbeschrijving.

3.3.2. Informatiesystemen beschrijven

Inventarisatie

Inventariseer alle informatiesystemen die aan de beschreven maatschappelijk vitale processen ondersteuning geven. Stel vervolgens vast of zo'n informatiesysteem van vitaal belang is voor de uitvoering van het proces. Het is duidelijk dat de eerste aandacht uit moet gaan naar informatiesystemen die van vitaal belang zijn voor een maatschappelijk vitaal proces.

Gemeenschappelijk

Voor informatiesystemen van V&W die gemeenschappelijk zijn voor diensten geldt dat de centrale IB onder de dienst valt waar het centrale beheer organisatorisch is ondergebracht. De gebruikende diensten zijn dan alleen verantwoordelijk voor de lokale IB. Het centrale beheer bepaalt hoe de verantwoordelijkheid is verdeeld tussen centraal en lokaal beheer.

Eigen

Voor eigen informatiesystemen van de dienst is de dienst zelf volledig verantwoordelijk voor de IB. Dit geldt onverminderd wanneer (delen van) het beheer is uitbesteed. Alleen deze categorie informatiesystemen dient beschreven te worden.

Derden

Voor informatiesystemen waar V&W geen eigenaar van is, beperkt de invloed van de dienst zich tot de lokale IB en tot het stellen van IB-eisen aan het informatiesysteem in de contracten met de leverancier.

Matrix

Breng de relatie tussen de processen en de informatiesystemen die daar ondersteuning aan bieden in kaart via een matrix. Onderstaand is een vereenvoudigd voorbeeld van een matrix voor processen en informatiesystemen weergegeven. Hierbij betekent 'V' op het snijpunt

dat het informatiesysteem vitaal is voor het proces en een 'X' dat het informatiesysteem wel het proces ondersteunt, maar dat die ondersteuning niet van vitaal belang is voor het proces.

Processen	Begeleiden zeeschepen	.....
Informatiesystemen		
IVS-SRK	V	
Radar waarnemingen	V	
Marifoon	V	
Meetnet ZEGE	X	
BIG	X	
SPS	X	

3.3.3. A&K-analyse uitvoeren

Bepaal of er processen zijn met informatiesystemen waarvoor een A&K-analyse moet worden uitgevoerd. Voorwaarden daarvoor zijn:

- *het betreft een maatschappelijk vitaal proces én*
- *één of meer informatiesystemen zijn van vitaal belang voor dat proces én*
- *de dienst is verantwoordelijk voor het (centrale) beheer van het (gemeenschappelijke) informatiesysteem.*

Het uitvoeren van een A&K-analyse is dermate specialistisch werk, dat het is aan te bevelen om daar via de Projectleiding D1 de expertise voor in te huren. Zo'n consultant moet zich dan wel conformeren aan de standaard methoden en technieken die reeds bij FABIN in gebruik zijn en die door een werkgroep, waarin verschillende Directies vertegenwoordigd zijn, geëvalueerd en bijgesteld worden.

4. Inrichting en voorwaarden

4.1. Projectinrichting

Het doel van projectinrichting is het zichtbaar maken van de wijze waarop de projectmanager van plan is het project in te richten om de opdracht uit te voeren volgens de voorgestelde aanpak. Hierbij zal de gekozen inrichting afhankelijk zijn van de resultaten van de risico analyse, kwaliteitseisen en de cruciale succesfactoren.

Speciaal punt van aandacht is de mate van decentralisatie bij de uitvoering. Bij een centrale uitvoering formeert men een centrale projectgroep die door de hele organisatie heen het werk uitvoert. Decentrale eenheden zijn slechts behulpzaam bij de uitvoering. Bij een decentrale uitvoering formeert men decentraal projectgroepen voor de uitvoering van het werk. In dat geval vindt centraal alleen de coördinatie plaats, zoals het samenvoegen van de voortgangsrapportages tot de voortgangsrapportage op het niveau van dit plan van aanpak.

Afhankelijk van de opdracht en de organisatie komen de OPAFIT aspecten aan de orde:

- *Organisatie; waarbij aangegeven wordt hoe de projectorganisatie eruit komt te zien inclusief taken en verantwoordelijkheden. Deze worden per persoon en per rol gesteld*
- *Personeel, waarbij de eisen aan de gewenste inzet en beschikbaarheid van personeel worden aangegeven zoals condities voor het betrekken van personeel, per groep de vereiste vakkennis, skills gerelateerd aan de plannen*
- *Administratieve procedures, waarin alle binnen en rond het project van toepassing zijnde procedures worden genoemd*
- *Financiering, alle financiële zaken worden hier behandeld, bij voorkeur met verwijzingen of, bij afwezigheid, expliciet opgenomen zoals tariefwijzigingen, facturering, subcontractors, btw en dergelijke;*
- *Informatie, waarbij ingegaan wordt op alle informatie rond het project, overleg- en rapportagestructuren; voor de (externe) voortgangsrapportage moet men gebruik maken van het standaard sjabloon daarvoor*
- *Techniek, waarbij wordt ingegaan op de voorgestelde inrichting qua hard- en software, werkplekken, hulpmiddelen en dergelijke.*

4.2. Voorwaarden aan opdrachtgever

Opsomming van voorwaarden, die gerealiseerd dienen te worden door de opdrachtgever om het project volgens plan te kunnen uitvoeren. Deze voorwaarden zijn gerelateerd aan en aanvullend op de inrichtingsaspecten.

De dienst is bij de tijdige uitvoering van het project afhankelijk van een aantal producten die D1/2 moeten leveren. De dienst gaat er van uit dat:

- het nieuwe V&W-brede informatiebeveiligingsbeleid tijdig beschikbaar is en helder het beleid verwoordt
- de Handreiking Minimumeisen tijdig beschikbaar en praktisch goed hanteerbaar is
- het centrale beheer tijdig inzicht verschaft in het aandeel verantwoordelijkheid bij een gemeenschappelijk systeem.

5. Plannen

In het hoofdstuk plannen wordt de resultante vastgelegd van het evenwicht tussen activiteiten, tijd, geld en middelen teneinde de opdracht te kunnen uitvoeren.

5.1. Normen en aannames

Hierbij worden de gehanteerde normen, aannames en veronderstellingen zowel ten aanzien van de schattingen als ten aanzien van planning vermeld, zoveel mogelijk per eenheid verbijzonderd. Deze kunnen afkomstig zijn uit geraadpleegde literatuur aangevuld met "ervaringscijfers".

5.2. Activiteitenplan

Deze paragraaf sluit aan bij hoofdstuk 3. Aanpak. De daar beschreven activiteiten worden hier gepland. Per activiteit wordt weergegeven de benodigde inspanning, de datum van aanvang, de datum gereed en de verantwoordelijke voor de uitvoering van de activiteit. Onderstaand is alvast de structuur van zo'n activiteitenplan opgenomen.

IDENT	ACTIVITEIT	UIT TE VOEREN DOOR	GEPLAN -DE UREN	BEGIN DATUM	EIND DATUM
3.1.1	Uitvoeren implementatieplan				
3.1	Quick wins	**Trajecttotaal**			
3.2.1	Opstellen migratieplan				
3.2.2.1					
3.2.2.2					
3.2.2	Uitvoeren migratieplan				
3.2	Minimumeisen Informatiebeveiliging	**Trajecttotaal**			
3.3.1	Processen beschrijven				
3.3.2	Infosystemen beschrijven				
3.3.3	Keuze maken ten aanzien van processen in aanmerking voor A&K-analyses en deze uitvoeren				
3.3	A&K-analyse	**Trajecttotaal**			
3	Project	**Projecttotaal**			

Houd er rekening mee dat de drie trajecten min of meer onafhankelijk van elkaar kunnen worden uitgevoerd. Maar het is van groot belang de

traject volgorde als prioriteitsvolgorde te hanteren. Binnen het traject Baseline moet de hoogste prioriteit worden gegeven aan:

- *het beveiligingsbeleid*
- *de beveiligingsorganisatie*
- *het beveiligingsbewustzijn.*

Iedere in hoofdstuk 3 onderscheiden activiteit wordt afzonderlijk gepland. De kolom " IDENT" verwijst dan ook naar die activiteit. Bijvoorbeeld kan 3.2.1.1 de activiteit " Invoeren IB beleid en organisatie" zijn als eerste activiteit binnen de hoofdactiviteit 3.2.1 Uitvoeren migratieplan.

In dit voorbeeld zijn totalen voorzien de niveaus hoofdactiviteit, traject en project. Zo'n totaal vermeldt het totaal aantal geplande uren. De begindatum vermeldt dan de datum waarop de eerste activiteit binnen de hoofdactiviteit, het traject of project start. De einddatum vermeldt dan de einddatum van de activiteit binnen de hoofdactiviteit, het traject of project, die het laatste klaar zal zijn.

Ter bevordering van het overzicht verdient het aanbeveling de activiteiten ook in een balkenschema of in een netwerkstructuur in onderlinge samenhang te tonen.

5.3. Productenplan

Het productenplan geeft de momenten weer waarop de (tussen)producten zullen worden opgeleverd en geaccepteerd. Deze paragraaf moet aansluiten bij paragraaf 2.4, waar de opsomming van (tastbare) producten is weergegeven.

5.4. Resourceplan

Het resourceplan verschaft duidelijkheid over personele en overige middelen. Het plan geeft weer over welke perioden inzet benodigd is. Bij de personele middelen wordt tevens het niveau van de resource aangegeven.

5.5. Financieel plan

In deze paragraaf wordt inzicht gegeven in de kosten (mensen, middelen en overig) van het project. Aangegeven worden de resources die in de planning zijn opgenomen, de hiervoor gehanteerde tarieven en de hieruit resulterende verwachte kosten.

6. Kwaliteitsborging

Het verdient sterk aanbeveling dat de projectmanager zich laat bijstaan door een kwaliteitsfunctionaris. Hij moet daar bij de inrichting van het project rekening mee houden. Daarnaast heeft hij de mogelijkheid om productaudits te laten uitvoeren waar daar behoefte aan bestaat.

De borging van de kwaliteit wordt in belangrijke mate verkregen door met name in de initiële fase van het project, dat resulteert in dit Plan van Aanpak, aandacht te geven aan risico beheersing.

Risico beheersing

Je moet als manager van een project niet uitgaan van het nemen van risico's, maar van het beheersen van risico's. Een risico definiëren we in dit verband als "een potentiële gebeurtenis welke het succes van het project kan verstoren." Voorwaarden voor risico beheersing zijn:

- *goed vooruit zien*
- *inzien welke zaken het bereiken van de doelstellingen in de weg kunnen staan*
- *weten welke maatregelen te treffen om de risico's te beperken*
- *accepteren van de extra inspanning/kosten om de risico's beheersbaar te maken.*

Opdracht

De opdracht moet volstrekt duidelijk zijn, niet alleen voor jezelf, maar ook voor anderen. Ga daartoe in dit plan na of de WAT-vraag in hoofdstuk 2 goed is beantwoord.

- *Ligt het beschouwingsgebied (projectomgeving) duidelijk vast?*
- *Is het achterliggende doel van het project (doelstelling) duidelijk? Is duidelijk wat wil V&W met het resultaat bereiken?*
- *Is duidelijk wat de projectopdracht inhoudt? En, vooral, is de reikwijdte van de opdracht duidelijk? Is daarbij duidelijk waar de dienst verantwoordelijk voor is? Is duidelijk wie verantwoordelijk is voor de producten waar de dienst voor de uitvoering van het project afhankelijk van is?*
- *Is duidelijk wat het resultaat, de producten van het project moeten zijn?*
- *Is duidelijk welke eisen D1 of D2 stelt? Kennen we het verwachtingspatroon van D1 of D2? Is duiselijk wat voor (voortgangs)rapportage D1 of D2 verwacht?*
- *Bestaat bij de betrokkenen overeenstemming over wat de cruciale succesfactoren voor dit project zijn?*

Vraag bij eventuele onduidelijkheden D1 of D2 om uitsluitsel

Afspraken

Je moet als Projectmanager heldere afspraken maken met de beheerders van mensen en van middelen, die in het project moeten worden ingezet. Maak via de randvoorwaarden duidelijk dat je het proces (= project) alleen maar goed en op tijd kunt uitvoeren, wanneer de benodigde mensen, middelen en producten op tijd en van de juiste kwaliteit worden geleverd. Stem met ieder van de verantwoordelijken het projectplan af, laat zien wat je wanneer van hen verwacht en laat ze weten wat je als randvoorwaarde opneemt in het plan.

Werkwijze

Het moet duidelijk zijn hoe het project wordt uitgevoerd. Realiseer je dat dit plan niet voor niets plan van aanpak heet. Pas hierbij binnen de reeds vastgestelde structuur een goede verdeling in activiteiten toe. Bepaal voor iedere onderscheiden activiteit HOE deze zal worden uitgevoerd.

Daar moet in overleg met de verantwoordelijken voor de uitvoering nu al over zijn nagedacht

Planning

Maak duidelijk hoe de trajecten en daarbinnen de (hoofd)activiteiten in elkaar grijpen. Geef daarbij het kritieke pad aan.

Ga na of voldoende aandacht is gegeven aan het capaciteitsbeslag van menskracht. Zorg dat de leveranciers van de benodigde menskracht zich committeren aan de claim die daar op gelegd wordt.

Risico bepaling

In theorie biedt een goed uitgevoerde initiële fase een plan van aanpak op waarin alle risico's zijn afgedekt. De praktijk is anders. Kijk daarom vooral naar die zaken, waarbij je als projectmanager water bij de wijn moet doen, bijvoorbeeld:

- *de producten moeten eerder klaar dan uit planningsoogpunt wenselijk is*
- *de toegezegde medewerkers voldoen niet volledig aan de kwalitatieve voorwaarden*
- *de gewenste hulpmiddelen zijn niet op tijd leverbaar.*

Ieder facet dat afwijkt van het ideale plan houdt een risico in dat zich waarschijnlijk voor zal doen. Voor ieder geïdentificeerd risico bepaal je afzonderlijk:

- *hoe waarschijnlijk de verstoring optreedt (Hoog, Midden, Laag)*
- *hoe groot de impact is als de verstoring optreedt (Hoog, Midden, Laag)*

Bepaal het resultaat volgens onderstaande matrix.

Waarschijnlijkheid Impact	Laag	Midden	Hoog
Hoog	maatregelen	onacceptabel	onacceptabel
Midden	aandacht	maatregelen	maatregelen
Laag	acceptabel	acceptabel	aandacht

Als je de impact laag inschat dan kun jet risico accepteren. Alleen als de kans van verstoring groot is, moet je daar gedurende de uitvoering aandacht aan schenken.

Bij risico's met impact midden is het project wel uitvoerbaa. Als de kans op de verstoring redelijk groot is, moet je, al dan niet in overleg met D1 of D2,nadere maatregelen treffen om het risico af te dekken of te verminderen. Dit kan tot extra kosten leiden.

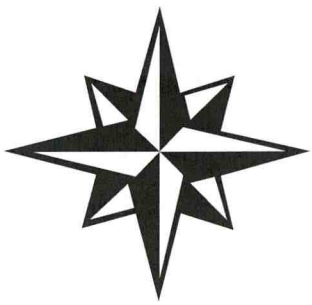
Als één risico veel impact heeft (hoog), bijvoorbeeld een vereiste opleverdatum loopt gevaar, overleg dan eerst met D1 of D2.

Bijlage 6

Sjabloon "Plan van Aanpak Voortraject"

Ministerie van Verkeer en Waterstaat
Directoraat-Generaal Rijkswaterstaat
Directie <Naam directie>

Plan van Aanpak Voortraject [Naam proces]



Colofon

Uitgegeven door: DG RWS / Directie [Klik hier voor naam directie]

Informatie: [Klik hier voor naam opsteller]
Telefoon: [Klik hier voor telefoonnummer opsteller]

Kenmerk: [Klik hier voor specifiek documentkenmerk]
Status: [Klik hier voor concept / definitief]
Versie: [Klik hier voor versie]

Datum: [Klik hier voor datum]

Document historie

Versie	Datum	Auteur	Omschrijving	Distributie
[Nr]	[Datum]	[Auteurnaam]	[Klik hier voor versiebeschrijving]	[Klik hier om doelgroep aan te geven]

Inhoudsopgave

1 Opdracht

Doelstelling project
Het project Voortraject <Naam proces> wordt opgestart om de uitvoering van een A&K analyse op het project <Naam project> binnen de directie <Naam directie> voor te bereiden.

Aanleiding
In het kader van de invoering van het VIR binnen Rijkswaterstaat is afgesproken om voor alle maatschappelijk vitale processen een A&K analyse uit te voeren en een Informatiebeveiligingsplan op te stellen. Eén van die maatschappelijk vitale processen is <Naam proces>.

Doel plan van aanpak
Het doel van dit plan van aanpak is om overeenstemming te verkrijgen over een systematische aanpak om een A&K analyse op het proces <Naam proces> goed voor te bereiden.

Doelgroep plan van aanpak
Dit plan van aanpak is bestemd voor <hid Directie / afdelingshoofd / VIR-coördinator / etc.>

Voortgangsbewaking project
<De VIR-coördinator / het hoofd van de afdeling xxy> bewaakt de voortgang van dit project.

Afbakening
<Geef hier duidelijk aan wat de begrenzingen van de opdracht zijn. Dit doe je door aan te geven wat binnen de opdracht valt, maar vooral ook wat buiten de opdracht valt. Kortom: schets de context: wat doe je wel, wat doe je niet>

Randvoorwaarden
<Geef hier de randvoorwaarden die nodig zijn om het voortraject te laten slagen. Geef daarbij aan wie je verantwoordelijk houdt voor het voldoen aan die randvoorwaarden en bespreek dat met hen. Denk hierbij aan tijdige beschikbaarheid van producten en capaciteit, tijdige besluiten en accorderingen c.q. betrokkenheid van het management>.

Op te leveren producten
De op te leveren producten zijn:
- Een beschrijving van het proces
- Een onderbouwde keuze voor het te beschouwen subproces.
- Een inventarisatie van de informatiesystemen en technische infrastructuren die het (nader te beschouwen sub)proces ondersteunen
- Een overzicht van de vitaliteit van informatiesystemen en technische infrastructuren
- De scope voor de A&K analyse op het (nader te beschouwen sub)proces

Einddatum
Volgens planning zal deze opdracht op <datum> zijn afgerond.

Gerelateerde documenten
(Vermeld met name de documenten die als brondocumenten voor de uitvoering van de opdracht dienen.>

- FABIN / werkgroep methoden en technieken (2001), *Procedure voortraject A&K analyse* (Docs-#10596).

2 Aanpak

2.1 Organisatiestructuur

Beschrijf hier duidelijk de projectorganisatie, waar zinvol aan de hand van een organigram. Uit de schets moet duidelijk blijken hoe de verantwoordelijkheden liggen, wie projectleider is, opbouw van projectgroep, en dergelijke

Ten minste aangeven hoe de verantwoordelijkheden liggen en plaatsen van de volgend functies:

- *Opdrachtgever / eindverantwoordelijke (intern)*
  - *De persoon die binnen de organisatie, vanuit de lijn, verantwoordelijk is voor het proces*
- *Projectleider (intern)*
  - *Opsteller van dit plan van aanpak en de persoon die verantwoordelijk is voor het op tijd en binnen budget opleveren van de producten*
- *A&K analist (in- of extern)*
  - *Specialist met kennis van A&K analyses; profiel is te vinden op de IB-site (www.ib.venwnet.minvenw.nl)*
- *Inhoudsdeskundige(n) (intern)*
  - *Specialisten met specifieke kennis van het proces of de systemen die het proces ondersteunen.*

2.2 Werkwijze

De werkwijze is gebaseerd op de procedure voortraject zoals die op de IB-site staat.

2.a Bepalen scope van het proces
Stel vast welke afdeling verantwoordelijk is voor de uitvoering van het proces. Plaats deze afdeling binnen de Directie. Schets met behulp van een contextdiagram de omgeving van het proces. Bepaal daarbij in de eerste plaats met welke andere primaire processen, waarvoor andere instanties verantwoordelijk zijn, een directe relatie bestaat. Laat duidelijk maken waar de grenzen liggen van verantwoordelijkheid en welke uitwisseling van informatie tussen beide processen bestaat. Bepaal vervolgens de overige instanties waarmee een relatie wordt onderhouden en welke informatie daarbij betrokken is. Beschrijf de organisatie en de omgeving in hoofdstuk 4 van het sjabloon Beschrijving proces en volg daarbij de aanwijzingen in het sjabloon.

2.b Bepalen proces
Stel de doelstelling, de aard en de afbakening van het proces vast. Bepaal tegen die achtergrond het proces op hoofdlijnen, zoals de verantwoordelijke afdeling dat uitvoert. Verdeel het proces in subprocessen als de uitvoering in verschillende A&K-analyses als gevolg van complexiteit/omvang van het proces dit noodzakelijk maakt. Beschrijf dit geheel in hoofdstuk 3 van het sjabloon Beschrijving proces en volg daarbij de aanwijzingen in het sjabloon.

2.c Inventariseren mensen en hulpmiddelen
Inventariseer de functionarissen en hulpmiddelen die van vitaal belang zijn voor de goede en tijdige uitvoering van het proces. Bepaal van die hulpmiddelen de informatiesystemen die in aanmerking komen voor een A&K-analyse. Criteria waaraan een A&K-systeem moet voldoen:

- geautomatiseerd systeem
- verwerking van input tot output
- eigendom gegevens bij RWS.

Stel vast waar het beheer van de A&K-systemen is belegd. Beschrijf het resultaat van de inventarisatie in hoofdstuk 5 van het sjabloon Beschrijving proces en volg daarbij de aanwijzingen in het sjabloon. Verbind aan de A&K-systemen de conclusie dat die in aanmerking komen voor de A&K-analyse. Geef van de functionarissen en overige hulpmiddelen aan dat de verantwoordelijke organisatie zelf de maatregelen moet treffen om steeds over de juiste kwantiteiten en kwaliteiten te beschikken voor het goed en tijdig uitvoeren van het proces.

2.e Bepalen scope A&K-analyse
Stel met alle betrokkenen de inhoud van document Beschrijving proces vast en bepaal met hen de scope voor de A&K-analyse. Dit betreft bij voorkeur het hele proces met alle A&K-systemen. Bij een complex proces met meer dan drie A&K-systemen is de scope te groot voor één A&K-analyse. Bepaal dan met de betrokkenen de meest optimale verdeling van subprocessen en A&K-systemen over meerdere A&K-analyses en stel de prioriteiten vast. Leg dit vast in het document Beschrijving proces en met name in het hoofdstuk Vervolg.

2.f Laten accorderen procesbeschrijving
Zorg dat de opdrachtgever het document Beschrijving proces accordeert. Regel daarbij dat de opdrachtgever goed op de hoogte is van de inhoud van het rapport. Zie toe dat er geen misverstand bestaat over de scope van de A&K-analyse(s) en dat duidelijk is dat de opdrachtgever zelf verantwoordelijk is voor het zeker stellen van vitale functionarissen en overige hulpmiddelen.

2.3 Communicatie

Beschrijf hier welke vormen van communicatie binnen het voortraject worden gehanteerd. Denk hierbij aan afstemming opdrachtgever / opdrachtnemer, workshops, interviews etc.

2.4 Kwaliteit

(Aangeven op welke wijze je de kwaliteit zal borgen, welke standaards je hanteert, de resultaten van een eventuele risico-analyse, welke acceptatie criteria je hanteert voor aan te leveren producten).

3 Planning en Kosten

3.1 Planning

In tabel hieronder staat de planning van het project.

FASE	AKTIVITEIT	UIT TE VOEREN DOOR	GEPLAN-DE UREN	BEGIN DATUM	EIND DATUM
1	Opstellen beschrijving proces				
2	Verkrijgen akkoord beschrijving proces				
3	Kiezen te beschouwen subproces				
4	Inventariseren informatiesystemen en technische infrastructuren				
5	Bepalen vitaliteit ondersteuning				
6	Bepalen scope A&K analyses				
		TOTAAL			

Tabel 1. Planning

(Hanteer hierbij de fasen en activiteiten zoals die onderscheiden zijn in Hoofdstuk 2 Aanpak. Houd met het aantal uren rekening met het feit dat onze tarieven dagtarieven zijn.)

3.2 Kosten

<Geef hier, indien mogelijk gescheiden naar in- en externe kosten, aan welke kosten gepaard gaan met dit project.>

Bijlage 7

Profiel "A&K-analist"

Ministerie van Verkeer en Waterstaat
Directoraat-Generaal Rijkswaterstaat

Directie Kennis

Profiel
A&K analist

<datum>

Colofon

Uitgegeven door: DG RWS / Directie Kennis

Informatie: Werkgroep M&T
Telefoon: 070-3114750

Kenmerk: DMS #13379
Status: Definitief
Versie: V1

Datum: 11 september 2001

Document historie

Versie	Datum	Auteur	Omschrijving	Distributie
1	110901	H. Geijsen	Profiel A&K-analist	Via IB-site

Inhoudsopgave

1 Achtergrond

Voor informatie over de VIR, informatiebeveiliging, het uitvoeren van een A&K analyse en de rol van FABIN is meer informatie beschikbaar op Intranet (http://www.ib.venwnet.minvenw.nl/)

Rol FABIN

Bij FABIN (ondergebracht bij de FEZ-Directie BVS) is veel kennis aanwezig van het VIR. Ook is er veel ervaring met het uitvoeren van afhankelijkheids- en kwetsbaarheidsanalyses (A&K analyses). Deze kennis en ervaring is zeer schaars binnen het departement. Daarom betrekken andere departementsonderdelen (waaronder het Hoofdkantoor van de RWS) steeds vaker FABIN bij vraagstukken die met het VIR te maken hebben.

Dit heeft geleid tot verschillende vormen van dienstverlening waaronder het uitvoeren van A&K analyses voor andere departementsonderdelen.

FABIN heeft te weinig capaciteit om alle opdrachten voor het uitvoeren van A&K analyses zelf uit te voeren. Daarom wordt capaciteit ingehuurd van externe bureaus.

In het volgende hoofdstuk is een functiebeschrijving opgenomen van een A&K analist.

2 Functiebeschrijving A&K analist

2.1 Werkzaamheden

De volgende werkzaamheden zijn van toepassing:

- Opstellen plan van aanpak voor de uitvoering van een A&K analyse
- Uitvoeren van afhankelijkheidsanalyse. Hieronder vallen:
  - Analyseren en beschrijven proces.
  - Analyseren en beschrijven informatiesystemen waarvan proces afhankelijk is.
  - Vaststellen eisen aan beschikbaarheid, exclusiviteit en integriteit van de informatie.
- Uitvoeren van kwetsbaarheidsheidsanalyse. Hieronder vallen:
  - Vaststellen bedreigingen.
  - Bepalen vereiste maatregelen.
- Opstellen informatiebeveiligingsplan
  - Vergelijken vereiste maatregelen met bestaande maatregelen.
  - Vaststellen aanvullende maatregelen.
- Zorgen dat het plan van aanpak wordt uitgevoerd binnen de hiervoor afgesproken eisen met betrekking tot kwaliteit, beveiliging, capaciteit en budget.
- Bespreken (tussen)resultaten project met overleggroepen en opdrachtgever.

Voor het opstellen van het plan van aanpak, de (tussen)producten van de A&K analyse en het informatiebeveiligingsplan dient gebruik gemaakt te worden van de RWS-methodiek als vastgelegd op de IB-site.

2.2 Eisen kennis, ervaring en eigenschappen

- Academisch werk- en denkniveau.
- Ervaring met uitvoeren procesanalyse.
- Communicatieve vaardigheden
- Organisatorische vaardigheden.
- Minimaal 2 jaar ervaring in de automatiseringsbranche*.
- Minimaal 1 jaar werkervaring binnen de Rijksoverheid.
- Klantgerichtheid.
- Hoog kwaliteits- en beveiligingsbewustzijn.
- Kritische instelling.
- Analytisch vermogen.
- Kennis van wet- en regelgeving op het gebied van beveiliging waaronder het VIR (Voorschrift Informatiebeveiliging Rijksdienst).
- Ervaring met betrekking tot het adviseren over en het implementeren van logische en fysieke beveiligingsmaatregelen.

** Het uitvoeren van een proces- en afhankelijkheidsanalyse vereist een goed organisatorisch inzicht en wat minder specifieke ICT-kennis. Voor het uitvoeren van een kwetsbaarheidsanalyse ligt dit net andersom. Daarom is een toegestane invulling van deze functie dat degene die de proces- en afhankelijkheidsanalyse uitvoert onder zijn verantwoordelijkheid een*

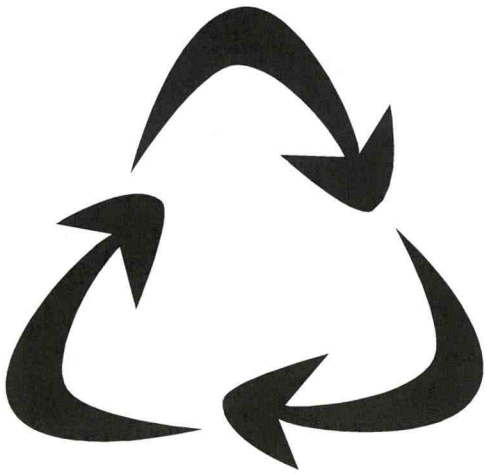
medewerker die wat meer specifieke ICT-kennis heeft de kwetsbaarheidsanalyse laat uitvoeren.

Bijlage 8

Sjabloon "Beschrijving Proces"

Ministerie van Verkeer en Waterstaat
Directoraat-Generaal Rijkswaterstaat
Directie <Naam directie>

Beschrijving proces [Naam proces]



Colofon

Uitgegeven door: DG RWS / Directie [Klik hier voor naam directie]

Informatie: [Klik hier voor naam opsteller]
Telefoon: [Klik hier voor telefoonnummer opsteller]

Kenmerk: [Klik hier voor specifiek documentkenmerk]
Status: [Klik hier voor concept / definitief]
Versie: [Klik hier voor versie]

Datum: [Klik hier voor datum]

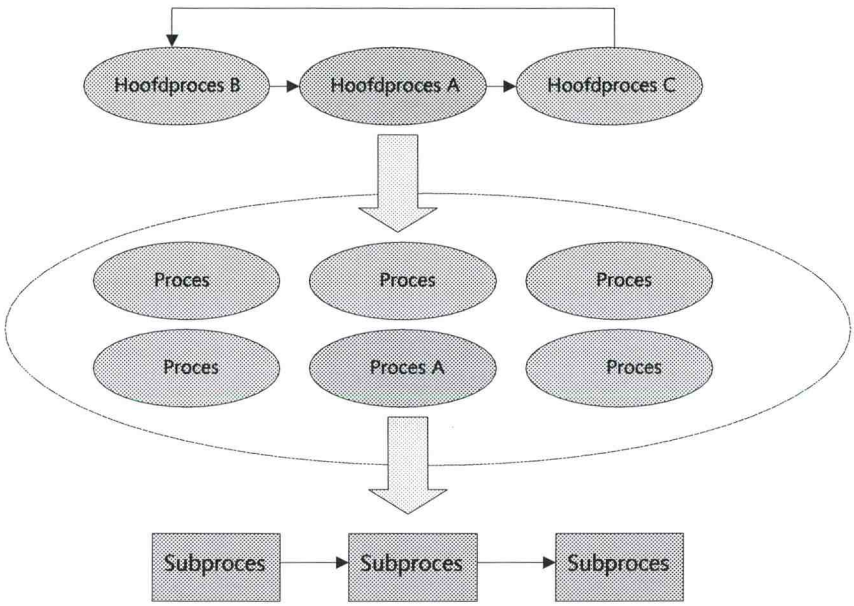
Document historie

Versie	Datum	Auteur	Omschrijving	Distributie
[Nr]	[Datum]	[Auteurnaam]	[Klik hier voor versiebeschrijving]	[Klik hier om doelgroep aan te geven]

Inhoudsopgave

1 Samenvatting

<Voeg hier een beknopte procesbeschrijving in. Het kan erg verhelderend werken om hier een overzicht te geven van de hoofdprocessen, processen en subprocessen die je in deze procesbeschrijving onderkent. Zo mogelijk kun je dit grafisch weergeven (zie voorbeeld).>



Figuur 0 – Overzicht processen

2 Inleiding

Doel rapport
Dit rapport heeft als doel het proces <Naam proces> te beschrijven binnen het hoofdproces <Naam hoofdproces> bij de Directie <Naam organisatie-onderdeel>.

Doelgroep
De doelgroepen van dit rapport zijn:
- *<Beschrijf voor wie het rapport bestemd is;*
- *kan beperkt blijven tot een opsomming>*
-

Aanleiding
<Geef kort aan wat de aanleiding is geweest om het proces uit te werken>

Opdracht
<Wie heeft opdracht tot het beschrijven van het proces gegeven, en hoe luidt de opdracht>

Indeling rapport
Na deze inleiding wordt in hoofdstuk 3 het proces op hoofdlijnen beschreven, waarbij de volgende aspecten aan de orde komen:
- Doel van het proces
- Aard van het proces
- Afbakening van het proces
- Indeling van het proces in subprocessen

Hoofdstuk 4 beschrijft de spelers in het proces. De volgende indeling is daarbij gehanteerd:
- Organisatie: dit bevat de plaats die <Organisatieonderdeel dat verantwoordelijk is voor het proces> heeft binnen de Directie, alsmede de eigen organisatie
- Omgeving: dit bevat de processen die gerelateerd zijn aan het proces <Naam proces>, alsmede de actoren rondom het proces.

Hoofdstuk 5 vermeldt de functionarissen en de hulpmiddelen, die van vitaal belang zijn voor de goede en tijdige uitvoering van het proces. Informatiesystemen vormen een subset van de hulpmiddelen.

Hoofdstuk 6 geeft een beschrijving van de subprocessen in geval die worden onderkend.

In hoofdstuk 7 tot slot wordt aangegeven welk vervolg deze procesbeschrijving kent (A&K analyse, informatiebeveiligingsplan).

3 Proces op hoofdlijnen

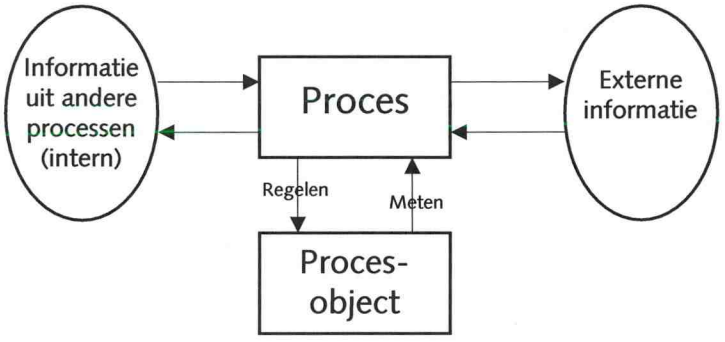
3.1 Doel proces

Het doel van het proces <Naam proces> is:

<Beschrijf het doel van het proces>
<Geef zo mogelijk ook een toelichting op de doelstelling>

3.2 Aard proces

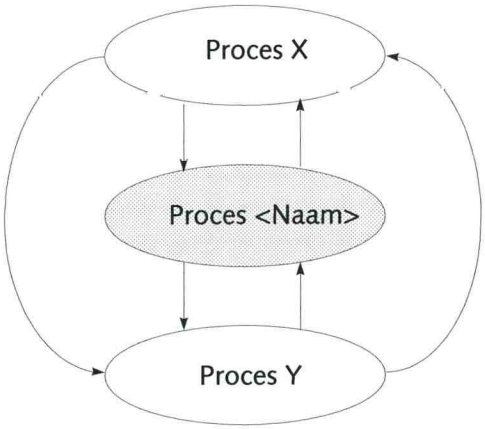
<Beschrijf welk type proces het is (bijvoorbeeld meet- en regelproces). Licht bij voorkeur met een plaatje toe hoe het proces er in hoofdlijnen uitziet. Hier hoeven de processen uit de omgeving niet uitputtend beschreven te worden; dat volgt bij de afbakening van het proces. Hieronder een generiek voorbeeld>



Figuur 1 – Proces <Naam proces> op hoofdlijnen.

3.3 Afbakening proces

<Geef de relatie aan tussen het beschreven proces en andere processen binnen het verantwoordelijke organisatieonderdeel. Ook hier weer bij voorkeur toelichten met een schema>



Figuur 2 – Afbakening proces

3.4 Procesbeschrijving

<Beschrijf globaal het proces zoals dat onder verantwoordelijkheid van de proceseigenaar wordt uitgevoerd. Bepaal of verdeling in subprocessen noodzakelijk is. **Pas op:** *gebruik de verdeling in subprocessen niet om de verschillende fasen binnen een proces aan te geven.>*

3.5 Subprocessen

Het proces <Naam proces> bestaat uit de volgende subprocessen:

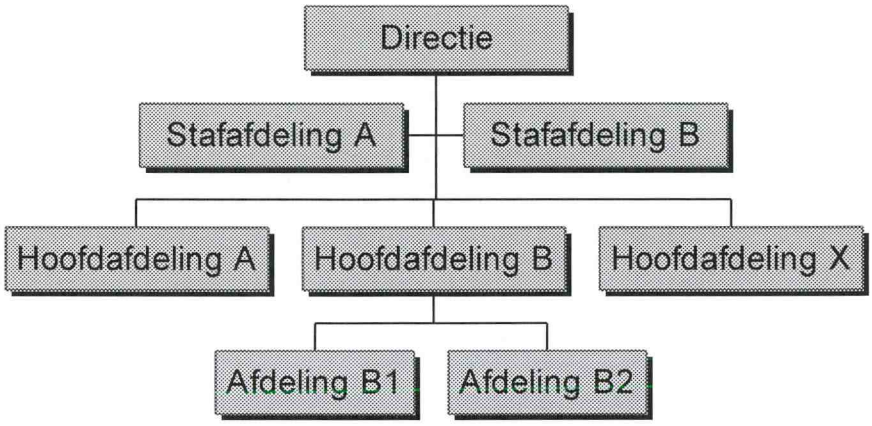
- <Naam subproces 1>
- <Naam subproces 2>
- <etc.>

De bovenstaande subprocessen zijn uitgewerkt in hoofdstuk 6.

4 Spelers in het proces

4.1 Organisatie

<Beschrijf de organisatie van de Directie waar het verantwoordelijke organisatie onderdeel van uitmaakt; licht dat toe met een organogram. Het onderstaande organogram is gemaakt met MS Organogram in PowerPoint (standaard bij Office95 en Office2000).>



Figuur 3 – Organogram <Naam organisatieonderdeel>

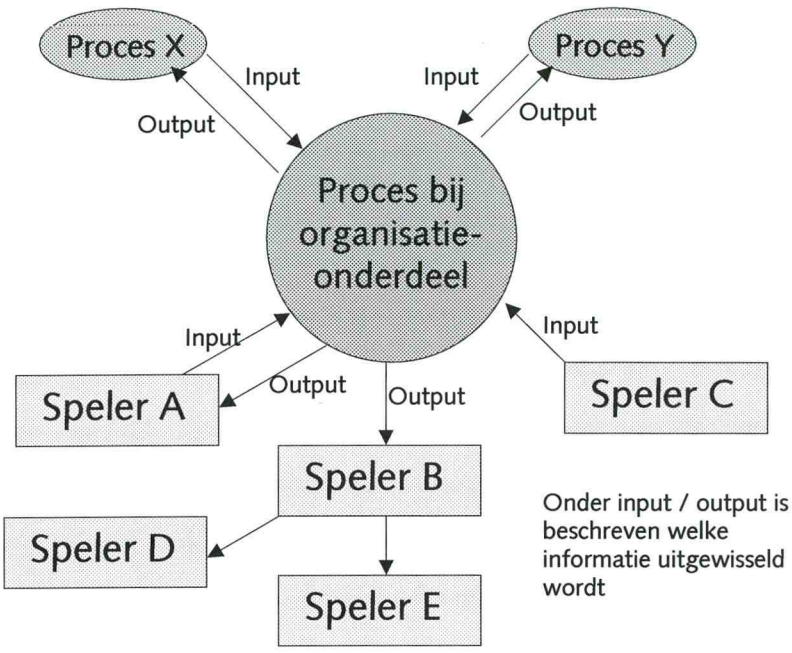
<Licht de verschillende organisatieonderdelen toe in een korte beschrijving, gericht op hun rol in het proces (doelstelling, verantwoordelijkheden, relatie met andere interne spelers, eventueel structuur).>

<Indien nodig, kunnen de interne spelers nader uitgewerkt worden naar (onder) afdelingen>.

4.2 Omgeving

<Beschrijf de processen en actoren buiten het proces, waarmee het proces relaties onderhoudt, voor zover dit voor het proces relevant is. Geef hierbij ook de gegevensstroom aan. Geef dit grafisch weer in een zogenaamd "contextdiagram", waarin aan het proces en het organisatieonderdeel gerelateerde processen en actoren worden weergegeven>.

<Hieronder een voorbeeld van een contextdiagram. Een dergelijk contextdiagram is te maken in PowerPoint>



Figuur 5 – Contextdiagram proces <Naam proces> bij <Naam organisatieonderdeel>

4.2.1 Gerelateerde processen

<Beschrijf hier welke andere processen direct aan het proces gerelateerd zijn. Laat hierbij goed uitkomen waar het proces ophoudt en het gerelateerde proces begint. Geef daartoe ook aan waar de verantwoordelijkheid ligt voor het gerelateerde proces. Geef via input en output aan welke informatie tussen de processen wordt uitgewisseld.>

4.2.2 Instanties

<Beschrijf hier welke instanties direct aan het proces gerelateerd zijn. Dit zijn andere instanties dan die reeds genoemd zijn als verantwoordelijke voor een gerelateerd proces. Geef de relatie door via input en output te beschrijven welke informatie de instantie levert aan het proces en welke informatie het proces levert aan het proces.>

5 Mensen en hulpmiddelen

Dit hoofdstuk vermeldt welke functionarissen en welke hulpmiddelen van vitaal belang zijn voor de juiste en tijdige uitvoering van het proces.. Een subset van deze hulpmiddelen zijn de systemen die bij de A&K-analyse zullen worden betrokken. Het is aan de procesverantwoordelijke om een risico-analyse los te laten op de overige hulpmiddelen en op de functionarissen om vast te stellen in hoeverre met name de beschikbaarheid is gewaarborgd.

5.1 Mensen

<Bepaal van welke functionarissen de goede en tijdige uitvoering van het proces sterk afhankelijk is.. Geef een korte beschrijving van de functie en vermeld waarom de uitvoering van het proces zo afhankelijk is van de functionaris.>

5.2 Hulpmiddelen

<Bepaal van welke hulpmiddelen de goede en tijdige uitvoering van het proces sterk afhankelijk is. .Geef een korte beschrijving van het hulpmiddel en vermeld waarom de uitvoering van het proces zo afhankelijk is van het hulpmiddel.Als het hulpmiddel een A&K systeem is, moet dat hier vermeld worden.>

5.3 Afkortingenlijst

<Neem hier een lijst op met afkortingen die in het rapport zijn gebruikt. Vermijd afkortingen te vermelden die iedere lezer geacht wordt te kennen, zoals VenW, RWS, en dergelijke.Plaats de afkortingen in alfabetische volgorde. Zie onderstaand voorbeeld.>

A&K	*Afhankelijkheid & Kwetsbaarheid*
BAS	*Bericht Aan de Scheepvaart*
BICS	*Binnenvaart Informatie en Communicatie Systeem*
HMCZ	*Hydro Meteo Centrum Zeeland*
IVR	*Internationale Vereniging Rijnvaart*
IVS90	*Informatie & Volgsysteem Scheepvaart*
KLPD	*Koninklijk Landelijke Politie Dienst*
MID	*Meetkundige Inspectie Dienst*
SD	*ScheepvaartDienst*
VMD	*Vaarweg Markerings Dienst*
VPW	*VerkeersPost Wemeldinge*
VVN	*Verkeer & Vervoer Nautisch*
WED	*Werktuigkundige Elektrotechnische Dienst*
ZHIS	*Zeeuwse Havens Informatie Systeem*

6 Subprocessen

In dit hoofdstuk worden de volgende subprocessen van het proces <Naam proces> nader uitgewerkt:

- <Naam subproces 1>
- <Naam subproces 2>
- <etc.>

<In dit hoofdstuk wordt vervolgens elk van de subprocessen beschreven, van start tot einde. In de beschrijving wordt ook aangegeven wie wanneer welke verantwoordelijkheden in dat subproces heeft, en welke relatie het subproces heeft met andere subprocessen. Ook kunnen in deze beschrijving al de hulpmiddelen genoemd worden die het subproces ondersteunen (waaronder informatiesystemen!). NB: hulpmiddelen enkel noemen voor zover zij een rol spelen in het proces. Een eventuele uitputtende beschrijving van de hulpmiddelen c.q.informatiesystemen volgt bij de A-analyse >

6.1 Subproces 1

<Beschrijving subproces 1 (definitie, verloop, samenhang met andere subprocessen)>

6.2 Subproces 2

<Beschrijving subproces 2 (definitie, verloop, samenhang met andere subprocessen)>

<Eventueel andere subprocessen tussenvoegen>.

6.3 Overzicht van subprocessen

In het onderstaande overzicht zijn de verschillende subprocessen in onderlinge samenhang weergegeven.

<Sluit af met een afbeelding, waarin de subprocessen t.o.v. elkaar zijn gepositioneerd; zie het voorbeeld in de samenvatting>

7 Vervolg

<Geef hier aan welke volgende stap gezet wordt in de A&K analyse. Dat zal in de regel het uitvoeren van een afhankelijkheidsanalyse op het gehele proces of bepaalde subprocessen zijn. NB: beperk je hier tot de informatie die dit document koppelt met het volgende document. Stappenplan en planning staan in het plan van aanpak.>

Bijlage 9

Sjabloon "Plan van Aanpak A&K-analyse"

Ministerie van Verkeer en Waterstaat
Directoraat-Generaal Rijkswaterstaat
Directie [Klik hier voor naam directie]

Plan van Aanpak A&K analyse [Naam proces]

Colofon

Uitgegeven door: DG RWS / Directie [Klik hier voor naam directie]

Informatie: [Klik hier voor naam opsteller]
Telefoon: [Klik hier voor telefoonnummer opsteller]

Kenmerk: [Klik hier voor specifiek documentkenmerk]
Status: [Klik hier voor concept / definitief]
Versie: [Klik hier voor versie]

Datum: [Klik hier voor datum]

Document historie

Versie	Datum	Auteur	Omschrijving	Distributie
[Nr]	[Datum]	[Auteurnaam]	[Klik hier voor versiebeschrijving]	[Klik hier om doelgroep aan te geven]

Inhoudsopgave

1 Opdracht

Doelstelling project
Het project A&K analyse op <Naam proces> wordt opgestart om de uitvoering van een A&K analyse op het project <Naam project> binnen de directie <Naam directie> uit ten voeren.

Aanleiding
In het kader van de invoering van het VIR binnen Rijkswaterstaat is afgesproken om voor alle maatschappelijk vitale processen een A&K analyse uit te voeren en een Informatiebeveiligingsplan op te stellen. Eén van die maatschappelijk vitale processen is <Naam proces>.

Doel plan van aanpak
Het doel van dit plan van aanpak is om overeenstemming te verkrijgen over een systematische aanpak om een A&K analyse op het proces <Naam proces> goed uit te voeren.

Doelgroep plan van aanpak
Dit plan van aanpak is bestemd voor <hid Directie / afdelingshoofd / VIR-coördinator / etc.>

Voortgangsbewaking project
<De VIR-coördinator / het hoofd van de afdeling xxy> bewaakt de voortgang van dit project.

Afbakening
<Geef hier duidelijk aan wat de begrenzingen van de opdracht zijn. Dit doe je door aan te geven wat binnen de opdracht valt, maar vooral ook wat buiten de opdracht valt. Kortom: schets de context: wat doe je wel, wat doe je niet>

Randvoorwaarden
<Geef hier de randvoorwaarden die nodig zijn om het voortraject te laten slagen. Geef daarbij aan wie je verantwoordelijk houdt voor het voldoen aan die randvoorwaarden en bespreek dat met hen. Denk hierbij aan tijdige beschikbaarheid van producten en capaciteit, tijdige besluiten en accorderingen c.q. betrokkenheid van het management>.

Op te leveren producten
De op te leveren producten zijn:
- Een rapport Afhankelijkheidsanalyse
- Een (of meerdere) systeembeschrijving(en).
- Een rapport Kwetsbaarheidsanalyse
- Een Informatiebeveiligingsplan (IBP)

Einddatum
Volgens planning zal deze opdracht op <datum> zijn afgerond.

Gerelateerde documenten
(Vermeld met name de documenten die als brondocumenten voor de uitvoering van de opdracht dienen.>

- FABIN / werkgroep methoden en technieken (2001), *Procedure voortraject A&K analyse* (Docs-#10596).
- Producten voortraject (onder meer procesbeschrijving).

2 Aanpak

2.1 Organisatiestructuur

(Beschrijf hier duidelijk de projectorganisatie, waar zinvol aan de hand van een organigram. Uit de schets moet duidelijk blijken hoe de verantwoordelijkheden liggen, wie projectleider is, opbouw van projectgroep, en dergelijke)

Ten minste aangeven hoe de verantwoordelijkheden liggen en plaatsen van de volgend functies:

- *Opdrachtgever / eindverantwoordelijke (intern)*
  - *De persoon die binnen de organisatie, vanuit de lijn, verantwoordelijk is voor het proces*
- *Projectleider (intern)*
  - *Opsteller van dit plan van aanpak en de persoon die verantwoordelijk is voor het op tijd en binnen budget opleveren van de producten*
- *A&K analist (in- of extern)*
  - *Specialist met kennis van A&K analyses; profiel is te vinden op de IB-site (www.ib.venwnet.minvenw.nl)*
- *Inhoudsdeskundige(n) (intern)*
  - *Specialisten met specifieke kennis van het proces of de systemen die het proces ondersteunen.*

2.2 Werkwijze

De werkwijze is gebaseerd op de procedure uitvoering zoals die vastligt op de IB-site:

2.a Beschrijven systemen
Zorg voor beschrijvingen van de te beschouwen systemen. Beoordeel in hoeverre de beschikbare systeembeschrijvingen aan het doel beantwoorden. Het gaat hier om de algemene systeemkenmerken, los van wat het systeem doet voor het te beschouwen proces. Gebruik voor het beschrijven van een systeem het sjabloon *Beschrijving systeem*. Volg hierbij de aanwijzingen in het sjabloon.

2.b Beschrijven proces
Beschrijf het te beschouwen proces en op welke wijze de te beschouwen systemen daar ondersteuning aan geven. Gebruik daarvoor het sjabloon *Rapport Afhankelijkheidsanalyse*. Volg hierbij de aanwijzingen in hoofdstuk 2 van het sjabloon.

2.c Uitvoeren afhankelijkheidsanalyse
Voer de afhankelijkheidsanalyse uit per systeem. Leg de resultaten vast in hoofdstuk 3 van het sjabloon *Rapport Afhankelijkheidsanalyse*. Volg hierbij de aanwijzingen in het sjabloon.

2.d Accorderen afhankelijkheidsanalyse

Zorg voor acceptatie van het Rapport afhankelijkheidsanalyse in de Projectgroep. Peil bij deze gelegenheid vooral ook bij de Projectgroep of de betrouwbaarheidseisen aan de systemen onderling in evenwicht zijn. Zorg voor accordering van het rapport door de Opdrachtgever.

2.e Uitvoeren kwetsbaarheidsanalyse
Voer de kwetsbaarheidsanalyse uit voor ieder van de systemen die daar volgens de afhankelijkheidsanalyse voor in aanmerking komen. Doe dit aan de hand van de Werkinstructie bij checklists K-analyse. Selecteer conform de werkinstructie de eisen die niet in aanmerking komen voor nadere uitwerking. Leg het resultaat van die selectie, eveneens conform de werkinstructie, vast in de checklists per systeem. Werk de daarvoor in aanmerking komende eisen conform de werkinstructie nader uit. Maak daarbij gebruik van het sjabloon Rapport kwetsbaarheidsanalyse.

2.f Opstellen informatiebeveiligingsplan
Stel het informatiebeveiligingsplan op aan de hand van de Werkinstructie bij checklists K-analyse op. Doe dit zodanig dat de opdrachtgever op basis van de informatie per aanbevolen maatregel in de K-analyse kan besluiten tot uitvoering. Deze informatie houdt in:

- de mogelijke consequentie bij niet treffen van de maatregel
- de grootte van de kans dat de consequentie zich voor doet
- een indicatie van de te leveren inspanning voor het uitvoeren van de maatregel.

Maak hierbij gebruik van het sjabloon Informatiebeveiligingsplan. Neem de voorgestelde maatregel uit het Rapport kwetsbaarheidsanalyse over. Volg hierbij de aanwijzingen in het sjabloon.

2.g Vaststellen te nemen maatregelen
Leg de voorgestelde maatregelen in het Informatiebeveiligingsplan voor aan het management van de Directie. Het management moet besluiten welke maatregelen getroffen moeten worden met een indicatie van prioriteit. Van iedere maatregel waarover het management besluit deze niet te nemen, moet de motivatie helder zijn en worden vastgelegd in het Informatiebeveilgingsplan ("bewust risico nemen").

2.i Vaststellen IB-plan
Laat het IB-plan (2e fase) formeel vaststellen door het management. Zorg dat het management een overleg of een functionaris verantwoordelijk stelt voor de planning van en de bewaking op de uitvoering van het IB-plan.

2.3 Communicatie

Beschrijf hier welke vormen van communicatie binnen het voortraject worden gehanteerd. Denk hierbij aan afstemming opdrachtgever / opdrachtnemer, workshops, interviews etc.

2.4 Kwaliteit

(Aangeven op welke wijze je de kwaliteit zal borgen, welke standaards je hanteert, de resultaten van een eventuele risico-analyse, welke acceptatie criteria je hanteert voor aan te leveren producten).

3 Planning en Kosten

3.1 Planning

In onderstaande tabel komt de planning van het project naar voren.

FASE	AKTIVITEIT	UIT TE VOEREN DOOR	GEPLAN-DE UREN	BEGIN DATUM	EIND DATUM
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
		TOTAAL			

Tabel 1. Planning

(Hanteer hierbij de fasen en activiteiten zoals die onderscheiden zijn in Hoofdstuk 2 Aanpak. Houd met het aantal uren rekening met het feit dat onze tarieven dagtarieven zijn.)

3.2 Kosten

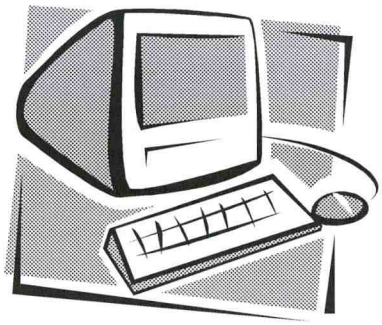
<Geef hier, indien mogelijk gescheiden naar in- en externe kosten, aan welke kosten gepaard gaan met dit project.>

Bijlage 10

Sjabloon "Beschrijving Systeem"

Ministerie van Verkeer en Waterstaat
Directoraat-Generaal Rijkswaterstaat
Directie <Naam directie>

Beschrijving systeem [Naam systeem]



Colofon

Uitgegeven door:	DG RWS / Directie [klik hier voor naam directie]
Informatie:	[Klik hier voor naam opsteller]
Telefoon:	[Klik hier voor telefoonnummer opsteller]
Kenmerk	[Klik hier voor specifiek documentkenmerk]
Status:	[Klik hier voor concept / definitief]
Versie:	[Klik hier voor versie]
Datum:	[Klik hier voor datum]

Document historie

Versie	Datum	Auteur	Omschrijving	Distributie
[Nr]	[Datum]	[Auteurnaam]	[Klik hier voor versiebeschrijving]	[Klik hier om doelgroep aan te geven]

Inhoudsopgave

1 Inleiding

De beschrijving van het systeem <naam systeem> in dit document is een algemene beschrijving, onafhankelijk van de processen waaraan het systeem ondersteuning verleent. Deze systeembeschrijving is daardoor bruikbaar voor meerdere A&K analyses.

Deze systeembeschrijving bestaat uit drie onderdelen: ten eerste een systeemkaart (hoofdstuk 2), waarin specifieke systeemkenmerken worden beschreven. Ten tweede bevat deze systeembeschrijving overzicht van de koppelingen die het systeem met andere systemen kent (hoofdstuk 3 – Architectuur). Tot slot volgt in hoofdstuk 4 een beknopte beschrijving van de functionaliteit van het systeem.

NB: de beschrijving van het gebruik van dit systeem in een specifiek proces is opgenomen in het rapport afhankelijkheidsanalyse op dat specifieke proces.

FAKIR

Deze systeembeschrijving is ook te vinden in FAKIR, het faciliterend systeem voor A&K-analyses. In het FAKIR zijn naast systeembeschrijvingen ook organisatiebeschrijvingen, procesbeschrijvingen en rapportages over afhankelijkheidsanalyses te vinden. Het FAKIR is via het VenW intranet te benaderen onder het thema Informatiebeveiliging (rechtstreeks adres is www.venwnet.ib.minvenw.nl).

2 Systeemkaart

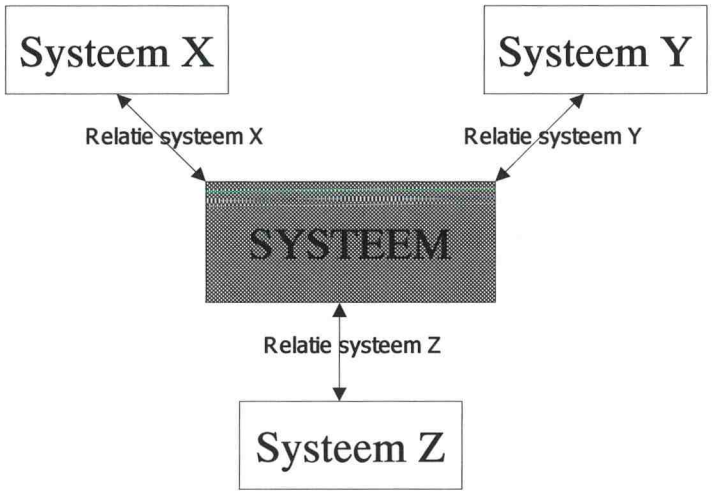
Naam systeem	<Vul hier de naam van het systeem in (afkorting)>
Volledige naam	*<Schrijf hier de systeemnaam voluit>*
Omschrijving	*<Geef hier in een of enkele zinnen weer waartoe het systeem dient>*
Versie en releasedatum	*<Geef hier aan welke versie van het systeem operationeel is en wat de releasedatum van die versie is>*
Soort systeem	*<Geef hier de systeemsoort aan. Belangrijk onderscheid:* • *Meerdere implementaties (algemeen) vs één implementatie (specifiek)* • *Raamwerksysteem vs standaardsysteem>*
Technische gegevens	*<Geef hier relevante technische gegevens in, bijvoorbeeld over de hardware, de systeemsoftware, het netwerk>*
Input	*<Geef hier aan welke gegevens in welke vorm input is voor het systeem>*
Output	*<Geef hier aan welke informatie in welke vorm het systeem levert. Output kan ook een opdracht tot handelen zijn>*
Interfaces	*<Geef hier, gescheiden naar input en output, aan met welke systemen het systeem geautomatiseerde interfaces kent; zie ook 3.1 Interfaces>*
Eigenaar systeem	*<Geef hier aan welk organisatieonderdeel van VenW eigenaar is van het systeem>*
Leverancier systeem	*<Geef hier de naam van de leverancier, eventueel inclusief contactpersoon>*
Functioneel beheer	*<Geef hier aan bij welk organisatieonderdeel het (centrale) functioneel beheer is belegd en wie contactpersoon is>*
Technisch Beheer	*<Geef hier aan bij welk organisatieonderdeel het (centrale) technisch beheer is belegd en wie contactpersoon is>*
Opmerkingen	*<Vermeld hier alle relevante informatie buiten één van de onderkende kenmerken>*

3 Architectuur

<Het is belangrijk om een informatiesysteem op het juiste niveau te benoemen. Voorwaarde is dat het een geautomatiseerd systeem is, waarvan de gegevens eigendom zijn van RWS en waarbinnen verwerking van input gegevens plaats vindt.>

3.1 Interfaces

<Beschrijf hier de geautomatiseerde koppelingen met andere systemen. Geef ook aan in welke mate het systeem zelfstandig is (afhankelijk is van de input uit andere systemen). Maak een schets ten behoeve van het overzicht. Onderstaand voorbeeld is gemaakt met PowerPoint>



<Beschrijf voor ieder gekoppeld systeem relevante bijzonderheden. Denk daarbij aan:

- *doel van het systeem*
- *belang van de gegevens uit het gekoppeld systeem voor het systeem*
- *acceptatie van geleverde gegevens door het systeem*
- *belang van gegevens uit het systeem voor het gekoppeld systeem*
- *wijze waarop de koppeling is gerealiseerd>.*

3.2 Interne architectuur

<Beschrijf hier de interne architectuurr van het systeem. Benoem de samenstellende componenten en hun rol binnen het systeem. Maak, bij een wat meer complexe architectuur zoals bijvoorbeeld bij MSW, een overzichtelijke schets>.

4 Functionele beschrijving

Het systeem <Naam systeem> wordt gebruikt om <.....>

<Beschrijf hier kort de functionaliteit van het systeem. Bijvoorbeeld aan de hand van een beschrijving van de systeemfuncties.

Voeg zo mogelijk een (functioneel) datamodel met toelichting toe, of geef anderszins schematisch weer welke functionaliteiten het systeem kent.

NB: het is niet de bedoeling hier een volledig functioneel (detail)ontwerp te geven. Het gaat met name om inzicht in de verschillende functies van het systeem en de samenhang tussen die functies.

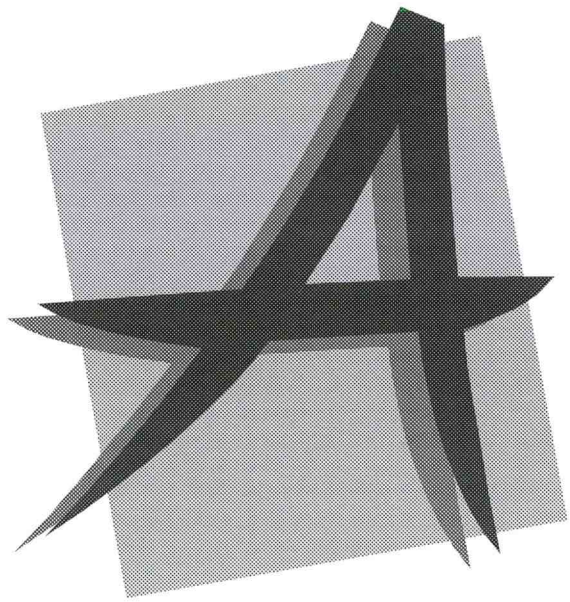
Als het een raamwerksysteem betreft, zoals Simona of Sobek, dan dient aangegeven te worden welke onderdelen per model aangepast moeten worden. In het rapport Afhankelijkheidsanalyse moet nader aangegeven worden welk model het daar betreft.>

Bijlage 11

Sjabloon "Rapport Afhankelijkheidsanalyse"

Ministerie van Verkeer en Waterstaat
Directoraat-Generaal Rijkswaterstaat
Directie <Naam directie>

Rapport afhankelijkheidsanalyse [Naam proces]



Colofon

Uitgegeven door: DG RWS / Directie [Klik hier voor naam directie]

Informatie: [Klik hier voor naam opsteller]
Telefoon: [Klik hier voor telefoonnummer opsteller]

Kenmerk: [Klik hier voor specifiek documentkenmerk]
Status: [Klik hier voor concept / definitief]
Versie: [Klik hier voor versie]

Datum: [Klik hier voor datum]

Document historie

Versie	Datum	Auteur	Omschrijving	Distributie
[Nr]	[Datum]	[Auteurnaam]	[Klik hier voor versiebeschrijving]	[Klik hier om doelgroep aan te geven]

Inhoudsopgave

1 Samenvatting

Dit rapport is het resultaat van een afhankelijkheidsanalyse op het proces <Naam proces>. De opdracht is uitgevoerd in opdracht van <Naam opdrachtgever>, als onderdeel van *<de A&K-analyse op proces X, of de invoering van het VIR bij organisatieonderdeel Y>*.

Het rapport sluit aan op het rapport Beschrijving <Naam proces>. Het doel van de afhankelijkheidsanalyse is om vast te stellen in welke mate het proces <Naam proces> afhankelijk is van de systemen die dat proces ondersteunen.

De onderstaande tabel geeft een overzicht van de uitkomst van de afhankelijkheidsanalyse.

	Betrouwbaarheidseis		
Naam systeem	Beschikbaarheid	Exclusiviteit	Integriteit
Systeem A			
Systeem B			
Systeem C			
Etc.			

<Vul de matrix in door de gestelde waarderingsnorm per systeem per betrouwbaarheidsaspect te plaatsen. Deze matrix moet gelijkzijn aan de matrix in hoofdstuk 5 Vervolg>

Bijlage 1 bevat een toelichting op de waarderingsnormen per betrouwbaarheidsaspect.

<Geef aan wat de scope zal zijn voor de kwetsbaarheidsanalyse als gevolg van bovenstaande waardering. Vat hier voorts samen van welke functionarissen en overige hulpmiddelen het proces erg afhankelijk is.>

2 Inleiding

Doel rapport
Het doel van dit rapport is het beschrijven van het proces zoals dat ondersteund wordt door de bij de afhankelijkheidsanalyse betrokken systemen, alsmede de resultaten van de afhankelijkheidsanalyse voor het proces <Naam proces>.

Aanleiding
De afhankelijkheidsanalyse volgt op het rapport Beschrijving proces <Naam proces>. In die beschrijving is tevens het kader aangegeven voor het uitvoeren van de afhankelijkheidsanalyse.

Het rapport afhankelijkheidsanalyse schetst welke rol de geselecteerde informatiesystemen spelen bij de uitvoering van het proces. Daaruit vloeit voort de mate waarin het proces afhankelijk is van ieder van die systemen. De mate van afhankelijkheid is bepalend voor de betrouwbaarheidseisen die het proces stelt aan zo'n systeem stelt.

Opbouw rapport
Na deze inleiding vermeldt hoofdstuk 3 alle relevante informatie over de te beschouwen systemen in relatie met het proces.

Hoofdstuk 4 beschrijft hoe belangrijk ieder systeem is voor het functioneren van het proces. Dit wordt uitgedrukt in de betrouwbaarheidseisen (beschikbaarheid, exclusiviteit en integriteit) die aan ieder systeem worden gesteld.

In hoofdstuk 5 tot slot vermeldt welke systemen meegaan naar de kwetsbaarheidsanalyse en hoe de A&K analyse wordt voortgezet.

3 Proces en systemen

3.1 Procesbeschrijving

<Beschrijf hier het proces opnieuw, maar nu op zodanige wijze dat de rollen van de betrokken informatiesystemen in het proces goed tot uitdrukking komen. Consequentie zal zijn dat deze beschrijving verder in detail gaat dan de organisatie gerichte procesbeschrijving in het rapport Procesbeschrijving.

De betrokken systemen zijn algemeen beschreven in een apart document per systeem. Vermeld hier de verbijzondering, wanneer daar sprake van is. Bijvoorbeeld welk model men gebruikt door schematisatie van een raamwerksysteem als Simona of Sobek. Of welk deel van een systeem men gebruikt, bijvoorbeeld welke componenten van MFPS als onderdeel van MSW.

Maak hierbij ook duidelijk waar het informatiesysteem daadwerkelijk een deel van het proces uitvoert en waar het alleen het proces ondersteunt.. Verdeel, waar zinvol, het proces in processtappen (= fasen). Dit vooral als de ondersteuning door het systeem per fase sterk verschilt..>

3.2 Proces/systeem matrix

De onderstaande matrix geeft aan welke systemen welke processtappen ondersteunen. *<Deze matrix moet het overzicht geven van hetgeen beschreven is in paragraaf 3.2. Zorg voor onderlinge consistentie. Geef in de matrix ook aan of een processtap alleen gebruik maakt van de informatie, of dat hij tevens input levert aan het systeem.*

NB het heeft alleen zin deze matrix op te stellen wanneer meerdere processtappen zijn onderkend én sprake is van meer dan één systeem>

	Processtap 1	Processtap 2	Processtap n
Systeem A			
Systeem B			
Systeem C			
Systeem X			

4 Betrouwbaarheidseisen

De betrouwbaarheid van een informatiesysteem voor een proces wordt gemeten aan de hand van drie betrouwbaarheidsaspecten, te weten Beschikbaarheid, Exclusiviteit en Integriteit. Aan ieder van deze drie aspecten wordt per systeem een waardering gegeven. Deze waardering kent vier klassen (in aflopende volgorde): Essentieel, Belangrijk, Wenselijk en Geen criterium.

In bijlage 1 zijn de betrouwbaarheidseisen met waarderingsnormen weergegeven, zoals die bij deze afhankelijkheidsanalyse zijn gebruikt.

4.1 Eisen betrouwbaarheid systeem A

Aspect	Eis	Onderbouwing
Beschikbaarheid	<Essentieel of Belangrijk of Wenselijk of Geen Criterium	*<Geef hier een duidelijke, en op het proces toegesneden onderbouwing van de eis aan de beschikbaarheid>*
Exclusiviteit	<Essentieel of Belangrijk of Wenselijk of Geen Criterium	*<Geef hier een duidelijke, en op het proces toegesneden onderbouwing van de eis aan de exclusiviteit>*
Integriteit	<Essentieel of Belangrijk of Wenselijk of Geen Criterium	*<Geef hier een duidelijke, en op het proces toegesneden onderbouwing van de eis aan de integriteit>*

<Indien gewenst kan onder de tabellen nog een toelichting gegeven worden, bijvoorbeeld wat betreft verschillen in inzicht in de betrouwbaarheidseisen vanuit verschillende organisatiebelangen>.

4.2 Eisen betrouwbaarheid systeem B

<als bij A, en zo verder voor ieder systeem>

5 Vervolg

In de onderstaande tabel zijn de betrouwbaarheidseisen, zoals die per systeem in hoofdstuk 4 gegeven zijn, uitgezet tegen de processen, die door het systeem ondersteund worden. *<identieke tabel in de samenvatting>*

	Betrouwbaarheidseis		
Naam systeem	Beschikbaarheid	Exclusiviteit	Integriteit
Systeem A			
Systeem B			
Systeem C			
Etc.			

<Trek hier de conclusie welke systemen waarom meegenomen zullen worden naar de kwetsbaarheidsanalyse.

Geef hier, indien gewenst, een schets van de uitvoering van de kwetsbaarheidsanalyse.>

Bijlage 1 – Waarderingsnorm

De waarderingsnorm is overgenomen van het voormalige ACIB (Advies en Coördinatiepunt Informatiebeveiliging).

WAARDERINGSNORM		BETROUWBAARHEIDSASPECT		
		Beschikbaar-heid	**Exclusiviteit**	**Integriteit**
Essentieel Beveiliging is primair criterium en verplicht voor de organisatie		Onmisbaar Slechts in uitzonderlijke gevallen niet operationeel	Dwingend Bedrijfsbelangen worden ernstig geschaad als ongeautoriseerden toegang krijgen	Onontbeerlijk Bedrijfsproces eist foutloze informatie
Belangrijk Beveiliging is absoluut nodig gezien de belangen van de organisatie		Wezenlijk Nauwelijks uitval gedurende de openingstijd	Cruciaal Gegevens alleen toegankelijk voor direct betrokkenen	Detecteerbaar Een zeer beperkt aantal fouten is toegestaan
Wenselijk Een zekere mate van beveiliging wordt op prijs gesteld		Nodig Een enkele keer uitval is aanvaardbaar	Afgeschermd Gegevens alleen ter inzage voor een bepaalde groep	Actief Bedrijfsproces tolereert enkele fouten
Geen criterium Beveiliging is geen criterium voor de organisatie		Niet van belang Er hoeven geen garanties gehaald te worden	Openbaar Gegevens hoeven niet afgeschermd te worden	Passief Geen extra integriteitsbe-scherming

Toelichting waarderingsnormering per betrouwbaarheidsaspect

Bijlage 2 – Afkortingen en definities

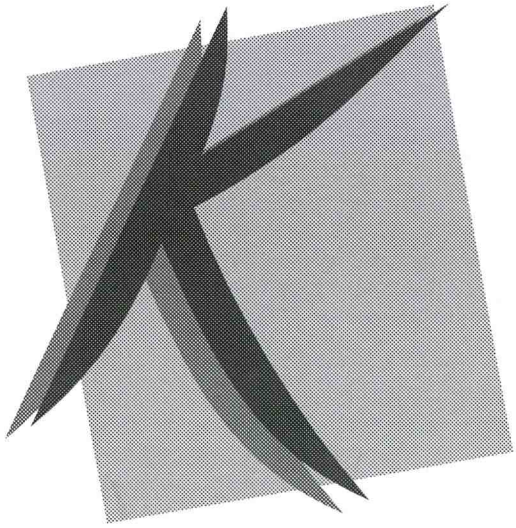
<Vermeld hier alle relevante afkortingen met hun verklaringen in alfabetische volgorde. Daarnaast eventueel ook definities van gehanteerde begrippen.>

Bijlage 12

Sjabloon "Rapport Kwetsbaarheidsanalyse"

Ministerie van Verkeer en Waterstaat
Directoraat-Generaal Rijkswaterstaat
Directie <Naam directie>

Rapport kwetsbaarheidsanalyse [Naam proces]



Colofon

Uitgegeven door: DG RWS / Directie [Klik hier voor naam directie]

Informatie: [Klik hier voor naam opsteller]
Telefoon: [Klik hier voor telefoonnummer opsteller]

Kenmerk: [Klik hier voor specifiek documentkenmerk]
Status: [Klik hier voor concept / definitief]
Versie: [Klik hier voor versie]

Datum: [Klik hier voor datum]

Document historie

Versie	Datum	Auteur	Omschrijving	Distributie
[Nr]	[Datum]	[Auteurnaam]	[Klik hier voor versiebeschrijving]	[Klik hier om doelgroep aan te geven]

Inhoudsopgave

Samenvatting

Doel van het rapport
Dit rapport beschrijft de kwetsbaarheidsheidsanalyse voor het proces <Naam proces> en is gericht op de systemen *<noem de systemen waar de K-analyse zich op richt>*. Het doel van de kwetsbaarheidsanalyse is om na te gaan hoe kwetsbaar het proces is voor wat betreft de systemen waarvan het proces sterk afhankelijk is.

Conclusies
<Vermeld hier de conclusies per systeem op hoofdlijnen uit de kwetsbaarheidsanalyse. Deze conclusie moet een waarde oordeel bevatten over de gesteldheid van de informatiebeveiliging van zo'n systeem. Als het systeem op punten onaanvaardbare risico's loopt, noem die dan expliciet.>

Aanbevelingen
<Geef hier op hoofdlijnen weer wat voor maatregelen getroffen zouden moeten worden om de informatiebeveiliging op het juiste peil te brengen. Benoem expliciet de maatregelen die met prioriteit getroffen moeten worden waar de risico's voor informatiebeveiliging erg groot zijn.>

Vervolg
De voorgestelde maatregelen worden overgenomen in het informatiebeveiligingsplan. Het management dient nader over het treffen van die maatregelen te besluiten op basis van de afweging tussen de grootte van het risico en de omvang van de maatregel. Het informatiebeveiligingsplan kan vervolgens dienen voor het plannen van de uit te voeren maatregelen en voor het bewaken op tijdige uitvoering.

1 Inleiding

Doel van het rapport
Dit rapport beschrijft de kwetsbaarheidsheidsanalyse voor het proces <Naam proces> en is gericht op de systemen *<noem de systemen waar de K-analyse zich op richt>*. Het doel van de kwetsbaarheidsanalyse is om na te gaan hoe kwetsbaar het proces is voor wat betreft de systemen waarvan het proces sterk afhankelijk is.

Aanleiding
Het rapport sluit aan op het Rapport afhankelijkheidsanalyse <Naam proces>. Onderstaande tabel geeft het overzicht van de uitkomst van de afhankelijkheidsanalyse.

	Betrouwbaarheidseis		
Naam systeem	Beschikbaarheid	Exclusiviteit	Integriteit
Systeem A			
Systeem B			
Systeem C			
Etc.			

Basis documenten
De volgende documenten zijn gehanteerd als basis voor het uitvoeren van de kwetsbaarheidsanalyse:

- Rapport Afhankelijkheidsanalyse <Naam proces>; opvraagbaar via FAKIR
- Code voor Informatiebeveiliging, versie 1, november 1994, Ministerie van Economische Zaken/NNI
- Handreiking Minimumeisen Informatiebeveiliging 2001; opvraagbaar via IB-site
- Minimumeisen Informatiebeveiliging *2001;* opvraagbaar via IB-site
- Werkinstructie bij checklists K-analyse; opvraagbaar via IB-site
- Rapport kwetsbaarheidsanalyse (sjabloon); opvraagbaar via IB-site.

Opbouw rapport
De kwetsbaarheidsanalyse is uitgevoerd per geselecteerd informatiesysteem uit de afhankelijkheidsanalyse. Voor ieder systeem is een hoofdstuk ingericht voor de kwetsbaarheidsanalyse. Zo'n hoofdstuk bevat alleen de bevindingen die het vermelden waard zijn bij het uitvoeren van de kwetsbaarheidsanalyse. Waar deze bevindingen een risico voor de informatiebeveiliging inhouden, staat tevens de aanbevolen maatregel om het risico af te dekken.

De conclusies op hoofdlijnen uit de kwetsbaarheidsanalyse zijn opgenomen in de Samenvatting.

In de bijlage treft men respectievelijk de Waarderingsnormtabel van het voormalige ACIB en de begrippenlijst.

2 Kwetsbaarheidsanalyse <systeem 1>

ID-nummer	1.<IDnummer uit checklist>
Eis	*<Maak duidelijk wat de minimumeis of de aanvullende eis inhoudt. >*
Bevinding	*<Vermeld hier in hoeverre en op welke wijze aan de eis is voldaan. Geef aan, voor zover niet aan de eis is voldaan, welk risico dit inhoudt voor de informatiebeveiliging.>*
Conclusie	*<Neem de conclusie uit checklist over>*
Maatregel (aanbeveling 1)	*<Vermeld hier de aanbevolen maatregel. Als de maatregel bestaat uit verschillende aanbevelingen, geef dan in de linkerkolom een volgnummer per aanbeveling>*
Opmerkingen	*<Plaats hier eventuele opmerkingen. Streef er naar de eis, bevinding en maatregel kort en bondig te vermelden. Gebruik deze rubriek daarbij voor nadere toelichting waar dit nodig is.>*

<Kopieer bovenstaand kader zo vaak als nodig voor dit systeem. Dit aantal wordt bepaald door het aantal conclusies uit de kwetsbaarheidsanalyse dat sprake is van een vermeldenswaardige bevinding. Vul het ID-nummer voor ieder kader aan met het IDnummer van de eis in de checklist. De reeds ingevulde "1" in het ID-nummer is het systeemvolgnummer. Houd hierbij dezelfde volgorde aan als de eisen in de checklists. Zie hiervoor de Werkinstructie bij checklists K-analyse.>

3 Kwetsbaarheidsanalyse <systeem n>

ID-nummer	n.<IDnummer uit checklist>
Eis	*<Maak duidelijk wat de minimumeis of de aanvullende eis inhoudt. >*
Bevinding	*<Vermeld hier in hoeverre en op welke wijze aan de eis is voldaan. Geef aan, voor zover niet aan de eis is voldaan, welk risico dit inhoudt voor de informatiebeveiliging.>*
Conclusie	*<Neem de conclusie uit checklist over>*
Maatregel (aanbeveling 1)	*<Vermeld hier de aanbevolen maatregel. Als de maatregel bestaat uit verschillende aanbevelingen, geef dan in de linkerkolom een volgnummer per aanbeveling>*
Opmerkingen	*<Plaats hier eventuele opmerkingen. Streef er naar de eis, bevinding en maatregel kort en bondig te vermelden. Gebruik deze rubriek daarbij voor nadere toelichting waar dit nodig is.>*

<Kopieer bovenstaand kader zo vaak als nodig voor dit systeem. Dit aantal wordt bepaald door het aantal conclusies uit de kwetsbaarheidsanalyse dat sprake is van een vermeldenswaardige bevinding. Vul het ID-nummer voor ieder kader aan met het IDnummer van de eis in de checklist. De reeds ingevulde "n" in het ID-nummer is het systeemvolgnummer. Houd hierbij dezelfde volgorde aan als de eisen in de checklists. Zie hiervoor de Werkinstructie bij checklists K-analyse.>

Bijlage 1 – Waarderingsnormtabel

De waarderingsnorm is overgenomen van het voormalige ACIB.

WAARDERINGSNORM		BETROUWBAARHEIDSASPECT		
		Beschikbaarheid	**Exclusiviteit**	**Integriteit**
Essentieel Beveiliging is primair criterium en verplicht voor de organisatie.		Onmisbaar Slechts in uitzonderlijke gevallen niet operationeel.	Dwingend Bedrijfsbelangen worden ernstig geschaad als ongeautoriseerde toegang krijgen.	Onontbeerlijk Bedrijfsprocessen eist foutloze informatie.
Belangrijk Beveiliging is absoluut nodig gezien de belangen van de organisatie.		Wezenlijk Nauwelijks uitval gedurende de openingstijd.	Cruciaal Gegevens alleen toegankelijk voor direct betrokkenen	Detecteerbaar Een zeer beperkt aantal fouten is toegestaan
Wenselijk Een zekere mate van beveiliging wordt op prijs gesteld.		Nodig Een enkele keer uitval is aanvaardbaar.	Afgeschermd Gegevens alleen ter inzage voor een bepaalde groep.	Actief Bedrijfsproces tolereert enkele fouten.
Geen criterium Beveiliging is geen criterium voor de organisatie.		Niet van belang Er hoeven geen garanties gehaald te worden.	Openbaar Gegevens hoeven niet afgeschermd te worden.	Passief Geen extra integriteits-bescherming

Bijlage 2 – Begrippenlijst

<Hieronder een eerste aanzet. Aan te vullen met relevante begrippen uit het rapport>.

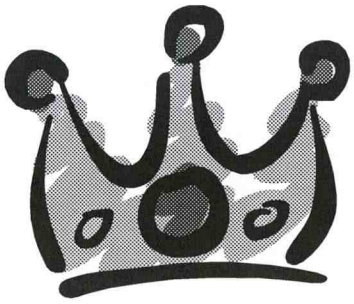
	Begrippen
Afhankelijkheidsanalyse	Het vaststellen van de mate waarin een proces afhankelijk is van de ondersteunende systemen.
Bedreiging	Het boven het hoofd hangen van een ongewenste gebeurtenis.
Beschikbaarheid	De mate waarin de ongestoorde voortgang van de informatievoorziening is verzekerd.
Exclusiviteit	De mate waarin de bevoegdheid en de mogelijkheid tot uitlezen, kopiëren of kennisnemen tot een gedefinieerde groep van gerechtigden is beperkt.
Informatiebeveiliging	Het treffen van een samenhangend pakket van maatregelen ter borging van de betrouwbaarheid van de informatievoorziening, met daarbij inbegrepen informatiesystemen en de informatie daarin.
Informatiebeveiligings-plan	Opsomming van alle beveiligingsmaatregelen en/of de vindplaatsen daarvan, welke voor een informatiesysteem of een verantwoordelijkheidsgebied van kracht is. Tevens een opsomming van de acties die gepland zijn om bepaalde maatregelen door te voeren dan wel te borgen.
Integriteit	De mate waarin gegevens of informatie in overeenstemming is met de realiteit en de mate waarin niets ten onrechte wordt achtergehouden. Hierbij gaat het om juistheid, volledigheid, actualiteit, consistentie en betrouwbaarheid.
Kwetsbaarheidanalyse	Het vaststellen van bedreigingen die de vereiste betrouwbaarheid van een proces of systeem kunnen verstoren en het bepalen van een adequate set maatregelen om de bedreigingen weg te nemen of de gevolgen bij het manifest worden van een bedreiging te ondervangen (preventief en curatief).
Maatregel	Schikking en ordening waardoor een zaak geregeld wordt.

Bijlage 13

Sjabloon "Informatiebeveiligingsplan"

Ministerie van Verkeer en Waterstaat
Directoraat-Generaal Rijkswaterstaat
Directie <Naam directie>

Informatiebeveiligingsplan [Naam Proces]



Colofon

Uitgegeven door: DG RWS / Directie <Naam directie>

Informatie: [Klik hier voor naam opsteller]
Telefoon: [Klik hier voor telefoonnummer opsteller]

Kenmerk: [Klik hier voor specifiek documentkenmerk]
Status: [Klik hier voor Concept / definitief]
Versie: [Klik hier voor versie]

Datum: [Klik hier voor datum]

Document historie

Versie	Datum	Auteur	Omschrijving	Distributie
[Nr]	[Datum]	[Auteurnaam]	[Klik hier voor versiebeschrijving]	[Klik hier om doelgroep aan te geven]

Inhoudsopgave

1 Inleiding

Doel rapport
In dit rapport staat het informatiebeveiligingsplan voor het proces <Naam proces> gericht op de systemen *<noem de systemen uit de K-analyse>*, zoals dat is ingevuld bij de directie <Naam directie>. Dit Informatiebeveiligingsplan dient in eerste instantie als basis voor besluitvorming over te treffen maatregelen informatiebeveiliging, waarna het als verantwoording dient over de genomen besluiten. Vervolgens dient als actieplanning voor de uit te voeren maatregelen, waar tegen tevens de voortgang van de uitvoering kan worden bewaakt.

Aanleiding
Het rapport sluit aan op het Rapport kwetsbaarheidsanalyse <Naam proces>. In dat rapport staan onder meer de niet afgedekte risico's voor informatiebeveiliging per systeem vermeld met de aanbevolen maatregelen om deze risico's af te dekken. Deze aanbevolen maatregelen zijn overgenomen in dit plan om daar verder follow-up aan te geven.

Basis documenten
De volgende documenten zijn gehanteerd als basis voor het opstellen van het Informatiebeveiligingsplan:
- Werkinstructie bij checklists K-analyse; opvraagbaar via IB-site
- Rapport kwetsbaarheidsanalyse <naam proces>
- Informatiebeveiligingsplan (sjabloon); opvraagbaar via IB-site.

Opbouw rapport
Het informatiebeveiligingsplan is opgesteld per informatiesysteem uit de kwetsbaarheidsanalyse. Voor ieder systeem is een hoofdstuk ingericht. Zo'n hoofdstuk bevat alle aanbevolen maatregelen uit de kwetsbaarheidsanalyse. Door hetzelfde ID-nummer te hanteren wordt de relatie gelegd met de eis en de bevinding waarop de maatregel is gebaseerd.

De Actielijst vormt het laatste hoofdstuk.

Fasering
Het informatiebeveiligingsplan is een werkdocument, dat gefaseerd wordt opgebouwd. Aan de invulling is af te lezen in welke fase het informatieplan zich bevindt.

Fase 1
In de eerste fase worden de voorgestelde maatregelen overgenomen uit de kwetsbaarheidsanalyse. Aan deze maatregel wordt een inschatting verbonden van de grootte van het risico en van de grootte van de inspanning voor het uitvoeren van de maatregel. Daarmee is de basis voor besluitvorming gelegd.

Fase 2
In de tweede fase neemt het management de besluiten over het uitvoeren van de maatregelen. Bij een negatief besluit geeft het management een heldere

	argumentatie. Bij een positief besluit geeft het management tevens een indicatie van prioriteit af.
Fase 3	Fase 3 houdt het opstellen van de actielijst in op basis van de besluitvorming. Hierbij moet met de verantwoordelijke voor de uitvoering een planning worden afgesproken. Deze fase wordt afgesloten met het accorderen van de actielijst door het management en de afspraak waar de voortgangsbewaking wordt belegd.
Fase 4	Fase 4 betreft het daadwerkelijk uitvoeren van de actielijst. En de bewaking daarop. Deze fase is pas afgesloten, wanneer is vastgesteld dat alle geplande acties zijn uitgevoerd.
Fase 5	Fase 5 in de verantwoordingsfase. Het informatieplan moet bewaard blijven om op ieder moment te kunnen aantonen waarom bepaalde maatregelen niet zijn uitgevoerd ("bewust risico nemen") en wanneer welke maatregelen zijn uitgevoerd.

2 Systeem <systeem 1>

ID-nummer	1.<IDnummer uit checklist>
Maatregel uit K-analyse (aanbeveling 1)	*<Kopieer hier de maatregel uit het rapport kwetsbaarheidsanalyse. Noem in de linkerkolom ook de aanbeveling volgnummers waarop de maatregel is gebaseerd als daar sprake van is>*
Indicatie inspanning	*<Geef hier een indicatie van de inspanning die het vergt om de genoemde maatregel door te voeren. Dit kan een absolute aanduiding zijn (in mensuren) of een minder meetbare aanduiding (bijvoorbeeld maatregelen indiceren naar veel/weinig/geen inspanning). Dit vak kan ingevuld worden door A&K analist i.o.m. medewerkers uit de organisatie.>*
Omvang mogelijke gevolgen van de bedreiging(en)	*<Geef hier aan welk risico je neemt als de maatregel niet wordt doorgevoerd. Ook hierbij is de inbreng van medewerkers uit de o rganisatie onmisbaar!>*
Besluit	De maatregel wordt (niet) uitgevoerd. *<Geef hier aan of de organisatie de maatregel wel of niet gaat uitvoeren. Geef, in geval gekozen wordt voor niet uitvoeren, een onderbouwing voor die keuze en bij wel uitvoeren een indicatie van prioriteit>.*
Opmerkingen	*<Plaats hier eventuele opmerkingen m.b.t. de maatregel. In dit vak kan ook aangegeven worden op welke wijze men denkt de maatregel te effectueren. Bijvoorbeeld:* *Deze maatregel maakt deel uit van de maatregelen die in het kader van de Minimumeisen Informatiebeveiliging genomen moeten worden. Deze maatregel wordt opgepakt met de invoering van de minimumeisen. De coördinatie voor de invoering van de minimumeisen is in handen van de V.I.R. Coördinator.*

<Kopieer bovenstaand kader zo vaak als nodig voor dit systeem. Dit aantal wordt bepaald door het aantal aanbevolen maatregelen in het rapport kwetsbaarheidsanalyse. Neem hierbij het volledige ID-nummer over,want dit legt de relatie naar de K-analyse. Houd hierbij dezelfde volgorde aan als in het rapport kwetsbaarheidsanalyse. Zie ook de Werkinstructie bij checklists K-analyse. Begin per maatregel op een nieuwe pagina. In de regel passen geen twee tabellen op één pagina, en spreiding van één tabel over meer dan één pagina is onoverzichtelijk>

3 Systeem <systeem n>

Kenmerk	n.1
Component	Mens *<Geef hier een MAPGOODcomponent>*
Maatregel uit K-analyse (aanbeveling 1)	*<Kopieer hier de maatregel uit het rapport kwetsbaarheidsanalyse. Noem in de linkerkolom ook de aanbeveling(en) waarop de maatregel is gebaseerd>*
Indicatie inspanning	*<Geef hier een indicatie van de inspanning die het vergt om de genoemde maatregel door te voeren. Dit kan een absolute aanduiding zijn (in mensuren) of een minder meetbare aandudiding (bijvoorbeeld maatregelen indiceren naar veel/weinig/geen inspanning). Dit vak kan ingevuld worden door A&K analist i.o.m. medewerkers uit de organisatie.>*
Omvang mogelijke gevolgen van de bedreiging(en)	*<Geef hier aan welk risico je neemt als de maatregel niet wordt doorgevoerd.Dit vak kan enkel goed ingevuld worden door medewerkers uit de o rganisatie!>*
Besluit	De maatregel wordt (niet) uitgevoerd. *<Geef hier aan of de organisatie de maatregel wel of niet gaat uitvoeren. Geef, in geval gekozen wordt voor niet uitvoeren, een onderbouwing voor die keuze>.*
Opmerkingen	*<Plaats hier eventuele opmerkingen m.b.t. de maatregel. In dit vak kan ook aangegeven worden op welke wijze men denkt de maatregel te effectueren. Bijvoorbeeld:* *Deze maatregel maakt deel uit van de maatregelen die in het kader van de Minimumeisen Informatiebeveiliging genomen moeten worden. Deze maatregel wordt opgepakt met de invoering van de minimumeisen bij de directie XXY. De coördinatie voor de invoering van de minimumeisen is in handen van V.I.R. Coördinator.*

< Kopieer bovenstaand kader zo vaak als nodig voor dit systeem. Dit aantal wordt bepaald door het aantal aanbevolen maatregelen in het rapport kwetsbaarheidsanalyse. Neem hierbij het volledige ID-nummer over,want dit legt de relatie naar de K-analyse. Houd hierbij dezelfde volgorde aan als in het rapport kwetsbaarheidsanalyse. Zie ook de Werkinstructie bij checklists K-analyse. Begin per maatregel op een nieuwe pagina. In de regel passen geen twee tabellen op één pagina, en spreiding van één tabel over meer dan één pagina is onoverzichtelijk>

4 Actielijst

In het onderstaande overzicht zijn de acties opgenomen om de maatregelen te realiseren.

ID-nummer	Verantwoordelijke uitvoering	Inspanning	Startdatum	Plan gereed	Einddatum

<Het ID-nummer bij de genomen maatregel overnemen. Vul daarbij degene die verantwoordelijk is voor de uitvoering. Bij de inspanning wordt aangegeven de geschatte tijd benodigd voor de realisatie. Bij maatregelen van grotere omvang zal de verantwoordelijke een eigen planning opstellen. Houd hier echter de planning op hoofdlijnen vast. De startdatum moet eerst met de geplande startdatum worden ingevuld, samen met de geplande datum gereed. Wanneer de actie werkelijk is gestart vul je de werkelijke startdatum in. Ten behoeve van het bewaken van de voortgang dient de einddatum alleen ingevuld te worden wanneer de actie ook werkelijk is afgerond.>

Bijlage 14

Schematisch overzicht betrouwbaarheidsaspecten en waarderingsnormen

WAARDERINGSNORM	BETROUWBAARHEIDSASPECT		
	Beschikbaarheid	**Exclusiviteit**	**Integriteit**
Essentieel Beveiliging is primair criterium en verplicht voor de organisatie	Onmisbaar Slechts in uitzonderlijke gevallen niet operationeel	Dwingend Bedrijfsbelang en worden ernstig geschaad als on-geautoriseer-den toegang krijgen	Onontbeerlijk Bedrijfsproces eist foutloze informatie
Belangrijk Beveiliging is absoluut nodig gezien de belangen van de organisatie	Wezenlijk Nauwelijks uitval gedurende de openingstijd	Cruciaal Gegevens alleen toegankelijk voor direct betrokkenen	Detecteerbaar Een zeer beperkt aantal fouten is toegestaan
Wenselijk Een zekere mate van beveiliging wordt op prijs gesteld	Nodig Een enkele keer uitval is aanvaardbaar	Afgeschermd Gegevens alleen ter inzage voor een bepaalde groep	Actief Bedrijfsproces tolereert enkele fouten
Geen criterium Beveiliging is geen criterium voor de organisatie	Niet van belang Er hoeven geen garanties gehaald te worden	Openbaar Gegevens hoeven niet afgeschermd te worden	Passief Geen extra integriteitsbe-scherming

Bijlage 15

Minimummaatregel:

Beleidsdocument voor informatiebeveiliging:
- Stel informatiebeveiligingsbeleid op en leg dit vast in een beleidsdocument
- Draag het informatiebeveiligingsbeleid uit in de organisatie

Beoordeling en evaluatie van het beleid:
- Laat minimaal eens per drie jaar een onafhankelijke evaluatie van het informatie-beveiligingsbeleid uitvoeren

Beleggen van verantwoordelijkheden voor informatiebeveiliging:
- Stel verantwoordelijkheden op het gebied van informatiebeveiliging vast en wijs ze toe aan functionarissen

Beveiligingseisen in contracten met derden:
- Leg afspraken over toegang tot IT-voorzieningen en informatie door derden schriftelijk vast

Beveiligingseisen in uitbestedingscontracten
- Neem bij uitbesteding van het management, de ontwikkeling of het beheer van informatie of informatiesystemen, of inhuur van tijdelijk personeel beveiligingseisen op in het contract tussen partijen

Richtlijnen voor het classificeren:
- Voldoe aan de richtlijnen vermeld in de Leidraad bescherming persoonsgegevens

Beveiligingseisen per functie:
- Stel algemene huisregels (gedragscodes) op inzake het omgaan met IT-voorzieningen
- Beschrijf voor kritische functies en taken apart de beveiligingseisen

Screening en personeelsbeleid:
- De identiteit van medewerkers, uitzendkrachten en personeel van derden wordt vastgesteld aan de hand van een geldig officieel identiteitsbewijs
- Bij de aanstelling of benoeming in een functie die bijzondere eisen stelt aan de integriteit of verantwoordelijkheid van de betrokkene, wordt een antecedentenonderzoek ingesteld
- Bij aanstelling of benoeming in een vertrouwensfunctie wordt een veiligheidsonderzoek ingesteld
- Geadviseerd wordt tijdelijk personeel, stagiaires en personeel van derden een geheimhoudingsverklaring te laten tekenen

Opleiding en training voor informatiebeveiliging:
- Alle medewerkers worden geïnformeerd over hun verantwoordelijkheden voortvloeiend uit wettelijke verplichtingen of geldende huisregels

Het rapporteren van beveiligingsincidenten:
- Voer een procedure in voor het melden en afhandelen van (vermoede) informatiebeveiligingsincidenten en maak deze bekend

Benoem kritieke ruimten:
- Benoem kritieke ruimten

Fysieke toegangsbeveiliging:
- Omhein de gehele locatie met een hek
- Installeer een alarmsysteem waarmee een extern alarmsignaal wordt gegeven
- Reguleer de toegang tot het gebouw

Veilig afvoeren en hergebruiken van apparatuur en informatiedragers:
- Verwijder, overschrijf of vernietig alle gegevens en vertrouwelijke applicatiesoftware als ze niet langer nodig zijn, met name voor reparatie of het afstoten van de media

Algemene beveiligingsmaatregelen:
- Tref maatregelen om de diefstal van componenten te signaleren en te voorkomen
- Tref maatregelen tegen brand
- Tref maatregelen tegen ongewenst binnenstromend water
- Tref maatregelen tegen stroomstoringen

Het beheer van wijzigingen:
- Zorg dat wijzigingen in de IT-voorzieningen gecontroleerd worden doorgevoerd

Netwerkbeheer:
- Beheer de configuratie van het netwerk actief

Bescherming tegen virussen en andere schadelijke software:
- Tref maatregelen tegen de introductie van schadelijke software

Wettelijke verplichtingen voor het uitwisselen van informatie:
- Besteed in de huisregels ten aanzien van het uitwisselen van informatie aandacht aan wettelijke aspecten waarmee rekening gehouden moet worden

Auteursrecht en licentiebeheer:
- Publiceer het beleid ten aanzien van de naleving van auteursrecht op software

Het proces van continuïteitsmanagement:
- Stel een continuïteitsplan op

Reserve kopieën maken (back-ups)
- Maak reservekopieën van alle essentiële bedrijfsgegevens

Eisen ten aanzien van logische beveiliging
- Wijs aan iedere gebruiker een gebruikersnaam (user-ID) toe
- Gebruik wachtwoorden die zo lang zijn dat ze moeilijk kunnen worden geraden of afgeleid uit de vercijferde vorm
- Wijzig wachtwoorden wanneer ze gecompromitteerd zijn
- Waarborg de vertrouwelijkheid van wachtwoorden bij uitgifte
- Werkstations in een netwerk moeten herkenbaar zijn
- Reguleer de toegang tot identificatievoorzieningen
- Biedt de eigenaar van een bestand de mogelijkheid zijn gegevens te beschermen tegen toegang door derden
- Beveilig onbeheerde werkstations tegen mogelijk gebruik door een ongeautoriseerd persoon

- Regel de toegang tot gegevens in overeenstemming met het toegangsbeleid van de organisatie
- Voorkom ongeautoriseerde toegang tot remote access ports
- Voorkom volledige toegang van en naar externe netwerken
- Beperk de toegang tot de systeembeheerderaccounts strikt

Specificatie van beveiligingseisen:
- In alle fasen van systeemontwikkeling, -beheer en -exploitatie dienen de informatiebeveiligingsaspecten te worden beoordeeld en bewaakt

Beveiliging van gegevens voor testdoeleinden:
- Toegang tot gegevens in testsystemen moet worden toegestaan in overeenstemming met het toegangsbeleid van de organisatie

Acceptatieprocedure:
- Specificeer acceptatiecriteria voor het testen van de beveiliging
- Autoriseer wijzigingen in het operating system
- Voer aanpassingen in standaardsoftware zo uit dat geen nieuwe problemen worden geïntroduceerd
- Controleer de kwaliteit van al het softwareonderhoudswerk