1216 Beveiligingsbewustzijn -

blz 8 1.1 **Beveiligingsbewustzijn -**

BEWUST GEDRAG > wordt gekenmerkt door gedragingen waaraan wilsbeschikking ten grondslag ligt.

ONBEWUST GEDRAG > wordt gekenmerkt door gedragingen waaraan géén wilsbeschikking ten grondslag ligt en is vaak gebaseerd op gewoontes. Gewoontes in de vorm van AUTOMATISMEN zijn een gevaarlijke vorm van onbewust gedrag.

De motivatie van mensen kan worden beïnvloed door de perceptie (waarneming) en de attitude (houding) van mensen tov informatiebeveiliging.

Fouten in onbewust gedrag > ontstaan door gewoontes en automatismen.
Fouten in bewust gedrag > zijn vergissingen en overtredingen (bv naar het verkeerde nummer faxen).

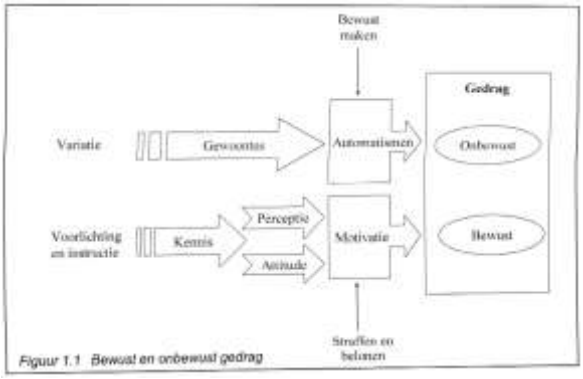
Overtredingen kunnen in goede en kwade trouw gebeuren.
Beveiligingsbewustzijn kan ook vergroot worden door instructie en voorlichting.
Om falen te voorkomen kan men functiescheiding toepassen.

461

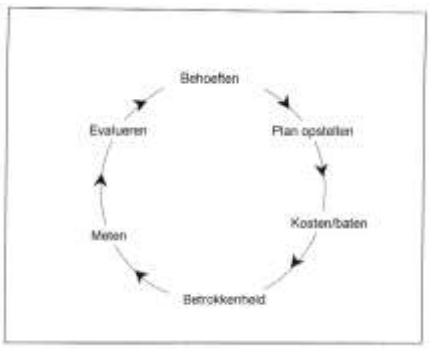
Soort gedrag	Kenmerken	Voorbeeld	Maatregelen
Bewust	wilsbeschikking	geen onbekende e-mail berichten openen	stimuleren door straffen en belonen
	gebaseerd op kennis en ervaring	vergissingen als het intoetsen van een verkeerd faxnummer	stimuleren door training en voorlichting
	aangeleerd	wachtwoord doorgeven aan collega	functiescheiding
			regels en voorschriften
Onbewust	geen wilsbeschikking	bureau niet opruimen	bewust maken door training en voorlichting
	gebaseerd op gewoontes en automatismen	niet uitloggen	bewust maken door aanwijzingen of variatie
	aanpassen aan de groep	vertrouwelijke informatie in printer achterlaten	afleren door straffen en belonen
		wachtwoord op beeldscherm plakken	aanpassen van de omgeving
			aanpassen van de werkomstandigheden

Figuur 1.2 Voorbeelden van bewust en onbewust gedrag

460



Figuur 1.1 Bewust en onbewust gedrag

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1217	**Beveiligingsbewustzijn -**		
blz 12 1.1	**Beveiligingsbewustzijn = Security Awareness -**		stappen voor een goed security awareness programma > 1. vaststellen vd behoeften 2. plan opstellen 3. kosten/baten analyse 4. betrokkenheid 5. meten - aantal beveiligings incidenten - beschikbaarheid Informatiesystemen - down-time vd centrale computersystemen - aantal virusinfecties - informatieaanvragen betreffende informatiebeveiliging bij servicedesk - aantal wijzigingen van wachtwoorden - opruimen van bureaus - automatisch uitloggen van schermen vd medewerkers 6. evalueren De doelgroepen zijn > - directie - lijnmanagement - IT-afdeling - administratie - personeelszaken - nieuw personeel - thuis- en mobiele werkers - servicedesk - gebruikers
462			 *Figuur 1.3 Security awareness programma*

1218 Beveiligingsbewustzijn -

blz 16 1.2 **taakverdeling -** de verantwoordig is als volgt verdeeld >
1- directie > uitzetten en uitdragen vh beveiligingsvbeleid; RICHTEN
2- lijnmanagement > voor implementatie en uitvoering vh beveligingsbeleid binnen eigen organisatorisch eenheid; INRICHTEN
3- leidinggevende > voor een adequate beveiliging vd eigen organisatorisch eenheid;
4- projectleiders > voor de beveiligingseisen binnen een project;
5- medewerkers > voor de beveiligingsaspecten binnen de eigen functie.

Richten > inrichten > verrichten
Zie figuur voor proces informatie beveiliging

	hoofdtaken	subtaken
beleid en organisatie	opstellen van het informatiebeveiligingsbeleid	leggen van relatie met de bedrijfsdoelstellingen
	inrichten van de beveiligingsorganisatie	formuleren van doelstellingen voor informatiebeveiliging
		uitdragen van het belang van informatiebeveiliging
		toekennen van personele, materiële en financiële middelen
		toewijzen van taken, verantwoordelijkheden en bevoegdheden
risicoanalyse	uitvoeren van risicoanalyses	vaststellen van de belangrijkste bedrijfsprocessen
		bepalen van de beveiligingseisen
		bepalen van de bedreigingen
		bepalen van de risico's (kans en schade)
maatregelen	selecteren van beveiligingsmaatregelen	kosten/batenanalyse van de maatregelen
		bepalen van de beveiligingsmaatregelen
		beschrijven van de maatregelen en implementatierichtlijnen
		opstellen van een informatiebeveiligingsplan
implementatie	implementeren van de beveiligingsmaatregelen	aanschaffen van beveiligingsmiddelen
		ontwikkelen van procedures
		invoeren van de geselecteerde maatregelen
		uitdragen van de maatregelen
bewaking	bewaken van de geïmplementeerde maatregelen	uitvoeren van onderhoud aan beveiligingsmiddelen en procedures
		controleren van de naleving van de geïmplementeerde maatregelen
		registreren van beveiligingsincidenten
		opstellen van een plan voor interne controle
		uitvoeren en initiëren van interne audits
evaluatie	evalueren van het gerealiseerde beveiligingsniveau	rapporteren over het aantal, het type en de gevolgen van beveiligingsincidenten
		evalueren van de realisatie van de geïmplementeerde maatregelen
		evalueren van het gerealiseerde beveiligingsniveau

Figuur 1.4 Beveiligingstaken

vrg:	trefwoord	trefwrd onderverdeling	omschrijving

1219 Beveiligingsbewustzijn -

blz 17	**beveiligingsfunctionar**	- security officer	(hoog)
1.2	**issen -**	- security specialist	..
		- beheerder informatiebeveiliging	..
		- adviseur interne controle en beveiliging	(laag)
		- IT-auditor	(deze heeft een onafhankelijke positie)

1220 Beveiligingsbewustzijn -

blz 22	**beveiligingseisen tav**	maatregelen kunnen zijn >
1.2.2	**personeel -**	- functieomschrijvingen
		- screening bij sollicitatie en deze bevat de volgende punten >
		- beschikbaarheid v positieve referenties
		- controle v volledigheid en nauwkeurigheid vd CV
		- controle en bevestiging v academische en professionele kwalificaties
		- identiteitsbewijs controle
		- controle op kredietwaardigheid bij gevoelige functies
		- geheimhoudingsverklaring
		- arbeidsvoorwaarden
		- opleiding/training
		- rapportage
		- disciplinaire maatregelen

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1221	**Juridische aspecten -**		*******
blz 24 1.3	**Wet Bescherming Persoongegevens (WPB) -**		Elke handeling of geheel v handelingen met betrekking tot persoongegevens, waarbij vooral van belang is de manier waarop gegevens kunnen worden verwerkt en met elkaar kunnen worden verbonden. De WBP is de opvolger van de WPR. De WBP handelt over de verwerking van persoonsgegevens. WPB gaat over 2 aspecten over hoe men om moet gaan met gegevens, namelijk > 1. registratie van gegevens 2. verwerken / manipuleren van gegevens Belangrijkste EISEN van de WPB zijn > - persoongegevens moeten op een legale zorgvuldige manier worden verkregen en verwerkt. - persoonsgegevens mogen uitsluitend worden verzameld voor duidelijk omschreven en gerechtvaardigde doelen. CBP = COLLEGE BESCHERMING PERSOONGEGEVENS > houdt toezicht op naleving. De FG rapporteert aan het CBP. PET = PRIVACY ENHANCING TECHNOLOGIES > vormen een geheel van ICT-maatregelen ter bescherming van de persoonlijke levenssfeer, door middel van het loskoppelen van de persoonsgegevens van de persoon. Dit is een belangrijke toepassing voor (semi-) overheden ed. om aan de WPB te kunnen voldoen. 2 domeinen > - identiteitsdomein > waar de identiteit van de persoon staat - pseudo-identiteitsdomein > waar de rest van de gegevens staan FG = FUNCTIONARIS VOOR DE GEGEVENSBESCHERMING > is onafhankelijk, houdt toezicht en oefent controle uit op de verwerking van persoonsgegevens binnen de organisatie, daarnaast rapporteert hij aan het CBP indien nodig. EISEN > betrouwbaar / diplomatiek / onafhankelijke positie in de org / kennis
1222	**Juridische aspecten -**		
blz 24 1.3			Bij ICT en informatiebeveiliging is de volgende wet- en regelgeving van belang > - Grondwet; - art 10 > eerbiediging vd persoonlijke levenssfeer (privacy) - art 13 > onschendbaarheid vd vertrouwelijk informatie; - Burgerlijk Wetboek (BW); - koopovereenkomst - rechten en plichten v burgers onderling ed - Wetboek van Strafrecht; - strafbepalingen bij overtredingen - Wet Gemeentelijke BasisAdministratle (GBA); - hoe gemeenten hun basisadministratie moeten inrichten - Auteurswet (AW) - hierin is vastgelegd dat auteursrecht toekomt aan de maker en geeft specifieke rechten op gebied van > - ongeoorloofd wijzigen - verveelvoudigen - openbaar maken - reverse enginering

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1223	**Europese richtlijn (95/46/EG) -**		
blz 31 1.3	**Europese richtlijn (95/46/EG) -**		De Europese richtlijn geeft aan op welke manier Europese wetgeving en nationale wetgeving samen gaan. Ze bevat > - toepasselijk nationaal recht; - beroep; - aansprakelijkheid; - sancties.
1224	**Wet op de Computer Criminaliteit (WCC) -**		*******
blz 32 1.3	**Wet op de Computer Criminaliteit (WCC) -**		De WCC heeft als doel de samenleving te beschermen tegen computermisbruik door het strafbaar stellen van computer-criminele handelingen. Beschikbaarheid, integriteit en exclusiviteit zijn daarbij de belangrijkste uitgangspunten. WCC-begrippen zijn: - computermisbruik; - computercriminaliteit; - computerfraude (als men zich in economisch opzicht probeert te verrijken); - computervredebreuk (door hacker).
1225	**Wet- en regelgeving voor de Rijksoverheid (VIR) -**		
blz 33 1.3	**Wet- en regelgeving voor de Rijksoverheid (VIR) -**		De VIR is een voorschrift voor de (rijks)overheid zelf. Stappen in het VIR-proces zijn; - opstellen informatiebeveiligingsbeleid; - inventarisatie; - afhankelijkheidsanalyse; - betrouwbaarheideisen; - kwetsbaarheidseisen; - beveiligingsmaatregelen; - opstellen infomatiebeveiligingsplan (IBP) met calamiteitenparagraaf en een keuze maken uit alle (informatie)beveiligingsmaatregelen die voortkomen uit de A&K-analyse; - opstellen implementatieplan (het IBP door het verantwoordelijke lijnmanagement laten Implementeren en onderhouden).

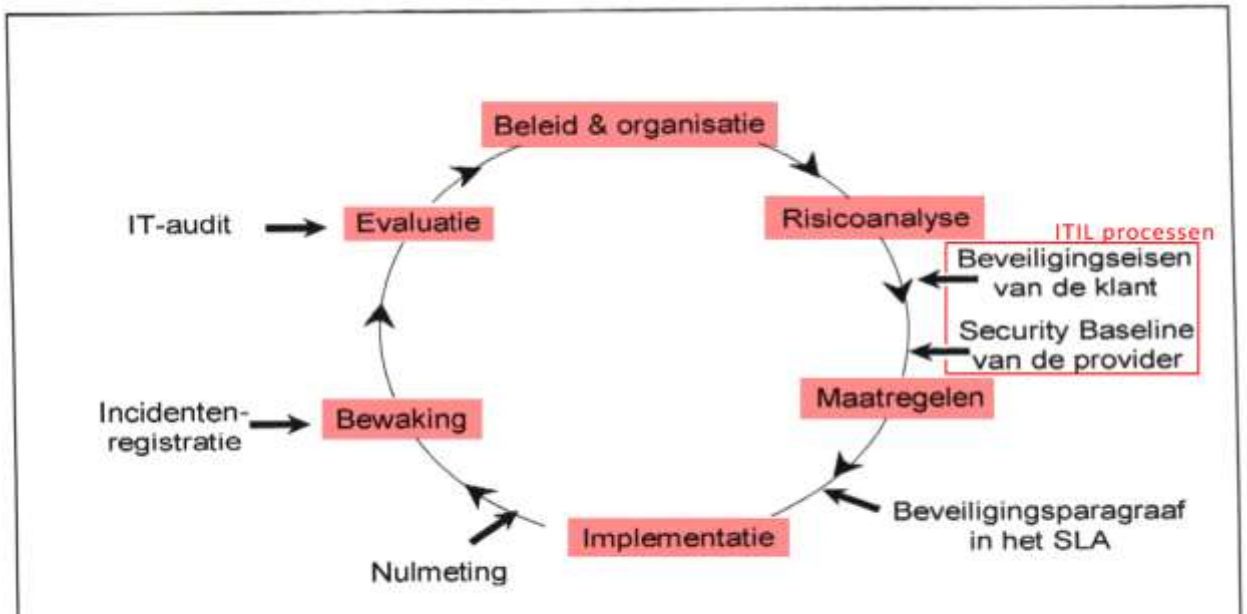
vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1226	**Contract of overeenkomst -**		

blz 38 1.3 **Contract of overeenkomst -**

SOORTEN contracten/overeenkomsten >
- Intentieverklaring / Letter of intent;
- Koopovereenkomst > hier is software benoemd en prijs vastgelegd
- Escrow (broncode+documentatie vd proggramatuur bij een derde partij bewaren)
  depotovereenkomst > is een 3-partijen overeenkomst tussen leverancier, afnemer en depothouder.
- Outsourcing;
- Lease-overeenkomst
  - operational > gaat vooral om het gebruik
  - financial > gaat vooral om de financiering
- SLA (Service Level Agreement);
- gedragscode voor e-commerce > principes zijn hier >
  - betrouwbaarheid
  - transperantie
  - vertrouwelijkheid en privacy
- Licentie overeenkomst > hier wordt toestemming verleend dat software gebruikt mag worden, men kent de volgende soorten >
  - ontwikkellicentie
  - eindgebruikerslicentie
  - shareware-licentie
  - freeware-licentie
  - beeldschermlicentie
  - shrink-wrap-licentie = krimfolieovereenkomst > uit USA, als je een programma opent verklaart de gebruiker zich al accoord met de licentievoorwaarden
  - registratiekaart
  - schriftelijke licentie
  - maatwerk

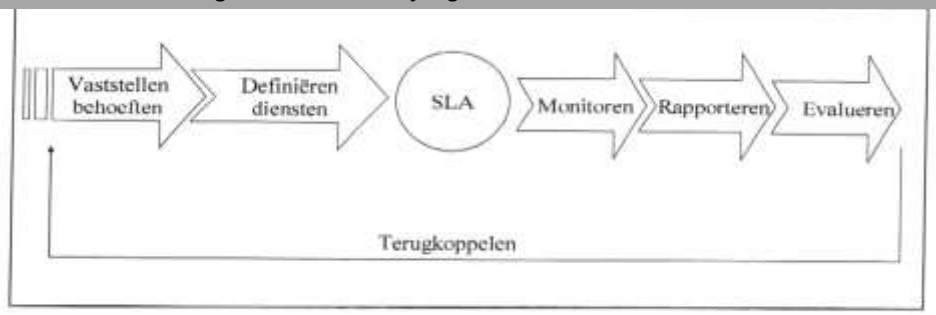
ad ESCROW > 4 manieren >
- bewaarneming door derden
- notarieel depot > bestaat weer uit 3 delen >
  - depotovereenkomst
  - depotakte
  - titelonderzoek
- auteursrecht-overdracht
- fiduciaire overdracht > als een leverancier de rechten op de drager en het gebruiksrecht op de broncode fiduciari overdraagt aan een speciaal daartoe in het leven geroepen rechtspersoon, meestal een stichting.

467



Figuur 1.6 Beveiligingsparagraaf in relatie tot het proces informatiebeveiliging

466

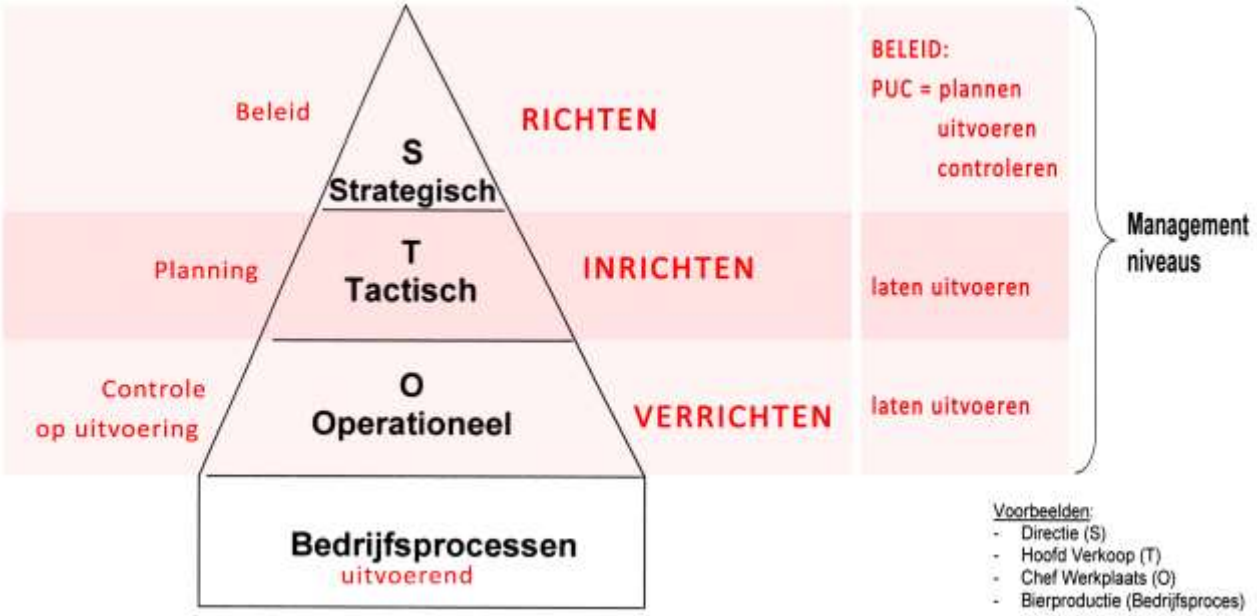


Figuur 1.5 Opstellen en aanpassen van een SLA

1227 Contract of overeenkomst -

blz 38 1.3 **Contract of overeenkomst -**

496



1228 Juridische aspecten -

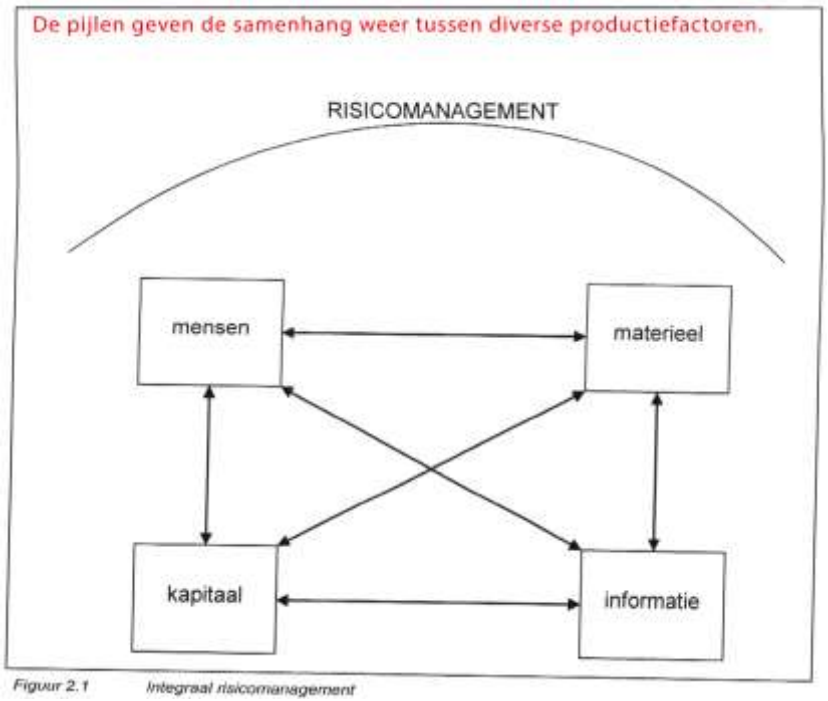
blz 33 1.3 **Telecommunicatiewet -** is iedere overdracht, uitzending of ontvangst van signalen door middel van telecommunicatie-infrastructuur.
In deze wet is geregeld hoe telecommunicatieaanbieders kunnen toetreden tot de telecommunicatiemarkt.

De volgende artikelen hebben betrekking op beveiliging >
- aanbieders zijn verplicht tot bescherming v persoonlijke levenssfeer vd gebruikers vd voorzieiningen.
- aanbieders zijn verplicht om aan politie ed. voorziening te bieden voor afluisteren en aftappen v telefoon- en data verkeer, hier is wel toestemming nodig voor van een rechter-commesaris.
- partijen die versleutelde info uitwisselen moeten op verzoek de sleutel kunnen geven aan politie e.d.

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1229	**Juridische aspecten -**		
blz 47 1.6	**E-commerce -**		hiermee wordt bedoel het gebruiken van openbare netwerken voor zakelijke toepassingen en er worden de volgende vormen onderscheiden > A = Overheidsinstantie B = Zakelijke partners C = Consumer cq consument bv: A2A > administration-to-administration > electronische transacties tussen overheidsinstellingen onderling De volgende combinaties zijn mogelijk: A2A, A2B, A2C, B2B, B2C, C2C over de grenzen van eigen bedrijf heen kijken en leveranciers en klanten direct toegang geven tot geautomatiseerde bedrijfsprocessen via internet. Voorbeelden E-Business en E-Commerce: E-ticketing E-trading E-learning E-entertainment E-games E-banking Teleshopping andere E-activiteiten: surfen en zoekmachinemarketing
1230	**Juridische aspecten -**		
blz 47 1.6	**gedragscode voor electronisch zakendoen -**		ECP - Electronic Commerce Platform > Doel > om in onderlinge samenwerking te komen tot de ontwikkeling en aanvaarding v electornisch zakendoen en op deze wijze de concurrentiekracht vh Nederlandse bedrijfsleven te bevorderen. Het biedt een rammwerk om het vertrouwen in het electronisch zakendoen te vergroten. Het bevat al regels die nog niet in de wetgeving zitten en loopt dus voor op de wetgeving. Is gebaseerd op de volgende principes > - betrouwbaarheid - transparantie - vertrouwelijkheid en privacy
ISMA		**Hoofdstuk: 2**	**Risicomanagement**

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1231	**risicomanagement -**		
blz 100 2	**integraal risicomanagement -**		Om juiste beslissingen te kunnen nemen moet informatie juist en betrouwbaar zijn (BIV) > - BESCHIKBAAR - INTEGRITEIT - VERTROUWELIJKHEID Risicomanagement > heeft als doel het beheersen v risico's. Integraal risicomanagement > houdt in dat de risico's voor alle producten in samenhang wordt beheerst en zal zich richten op > - de porductiefactoren > risisco's voor objecten - risico's voor de samenhang tussen de objecten

468



Figuur 2.1 Integraal risicomanagement

ISMA **Hoofdstuk: 3 Risicoanalyse**

vrg:	trefwoord	trefwrd onderverdeling	omschrijving

1232 Afbakening begrip risicoanalyse -

blz 110 3.1.1 **bedreigingen en risico's -**

Doel vd RISICOANALYSE is het in kaart brengen vd objecten die worden bedreigd en de risico's die verband houden met deze objecten. Daarna kan naar maatregelen worden gezocht om te proberen te voorkomen. Wordt voor ieder object apart uitgevoerd dat voor een bepaald risico in aanmerking komt.

INCIDENT > is een bedreiging die zich voordoet (betekenis wijkt hier af van ITIL).

Risico's kan men onderverdelen in >
- ORGANISATIE VERBONDEN categoriën >
  - bestuurlijk
  - economisch
  - informatie-gebonden
  - technisch
  - logistiek
  - sociaal
  - crimineel
  - financieel
  - juridisch
- naar BRON vd bedreiging >
  - omgeving
  - mens
  - techniek

469

inbreuk	opzettelijk	onopzettelijk
Op de beschikbaarheid	sabotage, vandalisme, diefstal van gegevens	brand, wateroverlast, computeruitval
op de integriteit	fraude	fouten, storingen
op de vertrouwelijkheid	spionage, diefstal van gegevens	regelovertreding

Figuur 3.1 Globale indeling van bedreigingen naar betrouwbaarheidsaspect

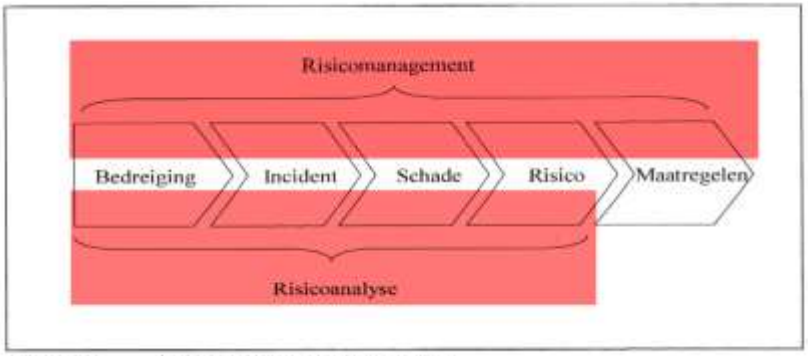
1233 Afbakening begrip risicoanalyse -

blz 110 3.1.2 **risicomangement -**

bestaat uit een combinatie van analyserende en sturende maatregelen met als doel de risico's te identificeren en maatregelen te ontwerpen en in te voeren, waardoor de kans dat een risico zich voor gaat doen, tot een acceptabel niveau teruggebracht wordt.

Er worden 5 stappen onderscheiden >
1. verkrijgen van inzicht in risico's;
2. vastellen van doelen, beleid en strategie;
3. realiseren van maatregelen;
4. toezicht houden op de status vd maatregelen dmv controle;
5. actueel houden en bijsturen van inzicht, beleid en maatregelen.

441



Figuur 1.6 Risicoanalyse en risicomanagement

vrg:	trefwoord	trefwrd onderverdeling	omschrijving

1234 Afbakening begrip risicoanalyse -

blz 111 3.1.3 **Risk Control Method (RCM) -**

Risicoanalyse als onderdeel van Risk Control Method. Risicoanalyse is een moment opname.
RCM = RISK CONTROL METHOD > is een methode voor het beheersen van relevante bedrijfsrisico's en bestaat uit de volgende stappen >

1. bewustwording;
2. richtringbepaling > nu wordt de risicoanalyse uitgevoerd,
   daarna kiest men voor de 4 mogelijke strategieën >
   - verminderen
   - vermijden
   - overdragen
   - accepteren

   Men houdt hier ook rekening met de beveiligingsaspecten BIV (beschikbaarheid, Integriteit en Vertrouwelijkheid).
   Hier dient ook de probleemstelling geformuleerd te worden en wordt het raamwerk voor later onderzoek gelegd.
3. prioriteiten bepalen > daarna komt er een beleidsplan uit en dit omvat een concrete en haalbare planning voor alle in te voeren maatregelen, evenals doelstellingen en beoogde resultaten per maatregel, betrokkenen, inschatting vd kosten en baten en een tijdplanning.
4. ontwerpen > belangrijk is hier betrokken zijn bij wijzigingsbeheer, de wijze waariop een wijziging wordt geïntieerd en doorgevoerd wordt, en de controle en rapportage daarover.
5. realiseren
6. implementeren
7. evalueren

In RCM wordt vanuit gegaan dat alle bestaande maatregelen een preventieve en/of representieve invloed hebben op mogelijk bedreigingen.

SLE = Single Loss Exposure = enkelvoudige schadeverwachting
ALE = Annual Loss Exposure = jaarlijkse schadeverwachting
(R= kans * schade) > Het is hier gebruikelijk om hier een onderscheid te maken tussen SLE en ALE.

1235 Afbakening begrip risicoanalyse - Risk Control Method (RCM) -

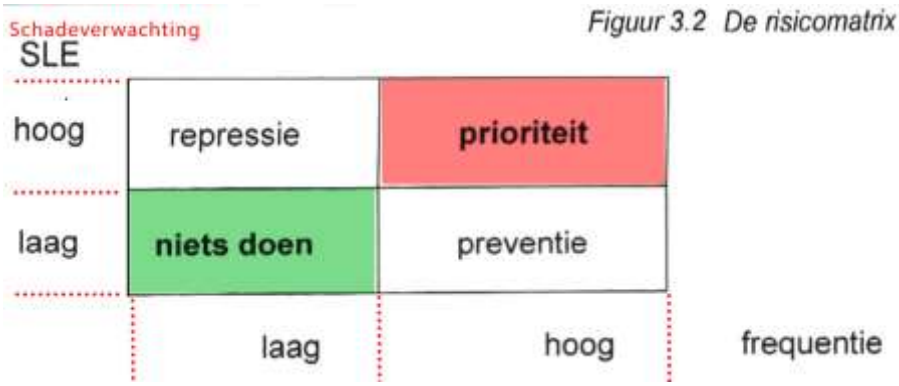
blz 113 3.1.3 **risicomatrix -**

is een hulpmiddel bij de interpretatie van de uitkomsten vd risicoanalyse. Hier worden de enkelvoudige schadeverwachting van bedreigingen en de frequentie waarmee de bedreigingen verwacht worden op te treden gecombineerd.
De risicomatrix kan gebruikt worden bij simuleren van verbeteringen, de keuze van verbeteringen moeten economisch verantwoord zijn (kosten en baten tegen elkaar afwegen).

Risicostrategiën zijn -
- VERMINDEREN > inzet van preventieve en/of representatieve maatregelen;
- VERMIJDEN > of opheffen vd risisco's door aanpassen v activiteiten, hulpmiddelen en/of methoden;
- OVERDRAGEN > outsourcing;
- ACCEPTEREN

SLE = Single Loss Exposure

470



Figuur 3.2 De risicomatrix

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1236	**Risicoanalyse methoden -**		

blz 115 3.2 **Quickscan en checklist -**

STANDAARD VRAGENLIJST > is een eenvoudige aanpak met 2 vormen >

- QUICK SCAN > is een standaard vragenlijst van buiten de organisatie. Wordt meestal in vorm van een enquetelijst gedaan zonder onderzoeker erbij, dus via een beeldscherm. Is eenmalig en levert geen pasklare oplossingen aan, het vormt geen volwaardige vervanger voor meer uitgebreide analysetools.
- BASELINE CHECKLIST > Een baseline is een basisniveau van beveiliging dat uit een stelsel van interne maatregelen betreft die binnen de hele organisatie doorgevoerd worden. Op basis vd Code voor Informatievbeveiliging zijn er vragenlijsten samengesteld om tot een basis niveau te komen.

Bij een checklist zijn de vragen afgestemd op wat relevant is voor de deelnemer.

Voordelen >

- goedkoop, snel in te voeren, normeerbaar, inzichtelijk, bewustwording.

Nadelen >

- standaard, statisch.

471

+ quick scan / checklist -	
• eenvoudig toe te passen • snel resultaat • weinig mankracht vereist (1 onderzoeker meestal	• weing diepgang • vaak organisatiegebonden (geen vergelijk mogelijk) • statisch (regelmatige actualisatie noodzakelijk)

Figuur 3.3 Voor- en nadelen van een quick scan/ checklist

vrg:	trefwoord	trefwrd onderverdeling	omschrijving	
1237	**Risicoanalyse methoden -**			***

blz 116 3.2.2 **kwalitatieve risicoanalyse -**

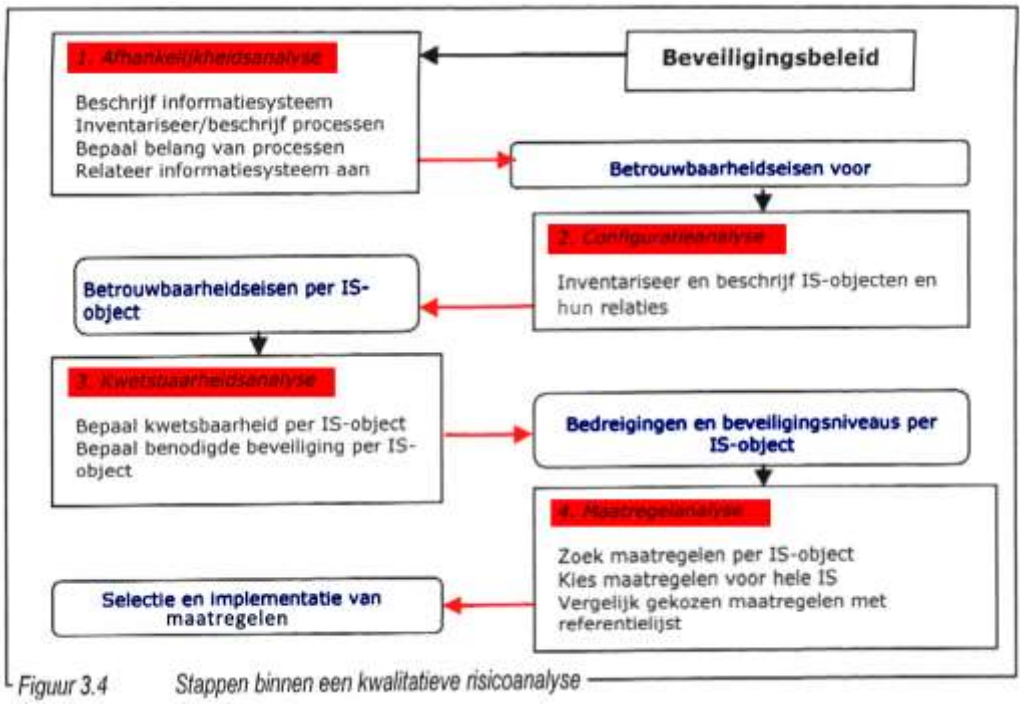
probeert een inschatting te maken vd de te lopen risico's die gelden voor verschillende analyseobjecten, waarbij de omvang v die risico's en de relatieve zwaarte ervan wordt begroot. We gaan hiervan uit van het bedrijfsproces dat ondersteund wordt door een enkel IS of door een combinatie van diverse informatiesystemen.

RISOCONEUTRAAL > wanneer kosten v beveiliging in evenwicht zijn met de potentiële schade die kan ontstaan.
RISICODRAGEND > hier accepteerd men de kans op grote schade.
RISICOMIJDEND > hier gaat men heel voorzichtg te werk

4 deelanalyses bij kwalitatieve risicoanalyse zijn >
- afhankelijksheidsanalyse;
- configuratieanalyse;
- kwetsbaarheidsanalyse;
- maatregelanalyse.

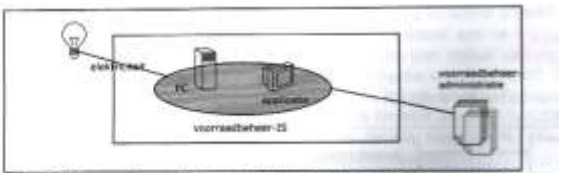
INFORMATIESYSTEEM (IS) > bestaat uit een aantal onderling gerelateerde fysieke en logische objecten en kan voor het uitvoeren van verschillende ondersteuningen ook verschillende combinaties van objecten gebruiken.
EEN ENKEL OBJECT > Wanneer bepaalde objecten samen onder een verantwoordelijkheidsgebeid zijn gebracht.
BASISVOORZIENINGEN > zijn objecten die geen deel uit maken van de informatievoorziening.

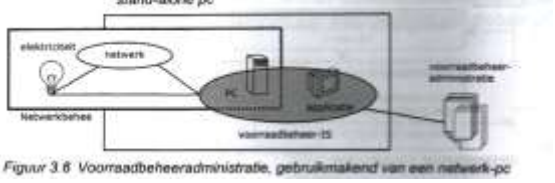
472



Figuur 3.4 Stappen binnen een kwalitatieve risicoanalyse

473


Figuur 3.5 Voorraadbeheeradministratie, gebruik makend van een IS op een stand-alone pc


Figuur 3.6 Voorraadbeheeradministratie, gebruikmakend van een netwerk-pc

vrg:	trefwoord	trefwrd onderverdeling	omschrijving

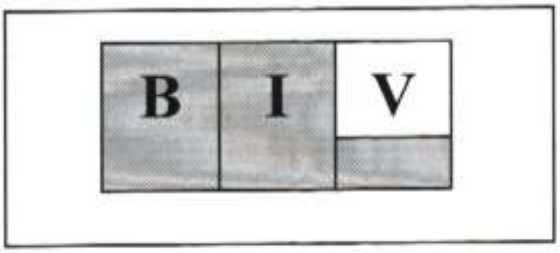
1238 Risicoanalyse methoden - kwalitatieve risicoanalyse -

blz 118 3.2.2 **afhankelijkheidsanalyse -** heeft tot doel om vast te stellen in hoeverre bedrijfsprocessen die door IS-en worden ondersteund, afhankelijk zijn van deze systemen. Om dit te bepalen neemt men de volgende stappen >

1. beschrijven vh IS
2. inventariseren en beschrijven van processen
3. bepalen vh belang van ieder proces > wordt uitgedrukt in (BIV) >
   - Beschikbaarheid
   - Integriteit
   - Vertrouwelijkheid
4. relateren vh IS aan processen
5. definiëren vd betrouwbaarheidseisen wordt uitgedrukt in (BIV) >
   - Beschikbaarheid
   - Integriteit
   - Vertrouwelijkheid

Het beveiligingsbeleid vormt het uitgangspunt voor de stappen, het resultaat is een lijst met betrouwbaarheidseisen voor het IS.

474



B = Beschikbaarheid > essentieel
I = Integriteit > essentieel
V = Vertrouwelijkheid > wenselijk

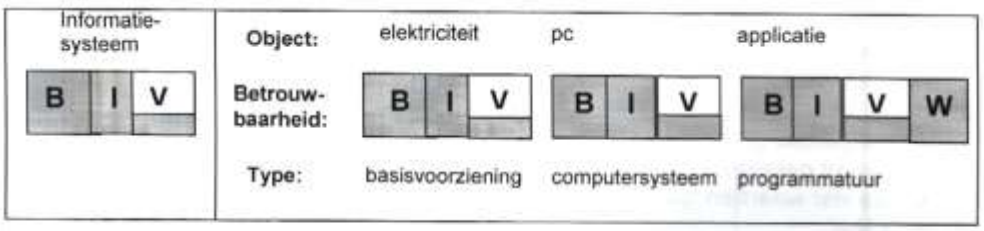
Figuur 3.7 Betrouwbaarheidseisen voor het voorraadbeheerinformatiesysteem

1239 Risicoanalyse methoden - kwalitatieve risicoanalyse -

blz 119 3.2.2 **configuratienanalyse -** heeft als doel om vast te stellen hoe een IS is opgebouwd. De stappen zijn hier >

1. inventariseren en beschrijven vd IS-objecten en de relaties
2. bepalen vd betrouwbaarheidseisen per IS-object

475



B = Beschikbaarheid
I = Intergriteit
V = Vertrouwelijkheid

W = Waarde

Figuur 3.8 Betrouwbaarheidseisen voor het voorraadbeheerinformatiesysteem en de objecten daarvan

vrg:	trefwoord	trefwrd onderverdeling	omschrijving

1240 Risicoanalyse methoden - kwalitatieve risicoanalyse - **

blz 120 3.2.2 **kwetsbaarheidsanalyse -** heeft als doel om voor ieder IS te bepalen wat de relevante bedreigingen zijn en omvat de volgende stappen >
1. bepalen vd kwetsbaarheid per IS-object;
2. bepalen vd benodigde beveiliging per IS-object.

476

Object	Type object	Bedreiging	Kwetsbaarheid	Beveiligingsniveau
Applicatie	Programmatuur	Virus	✦✦	Hoog
		Diefstal	✦✦✦	Hoog
PC	Computersysteem	Invloeden van buitenaf	✦✦✦	Laag
		Storing	✦✦✦	Laag
Elektriciteit	Basisvoorziening	Invloeden van buitenaf	✦✦	Nihil
		Sabotage	✦✦	Nihil

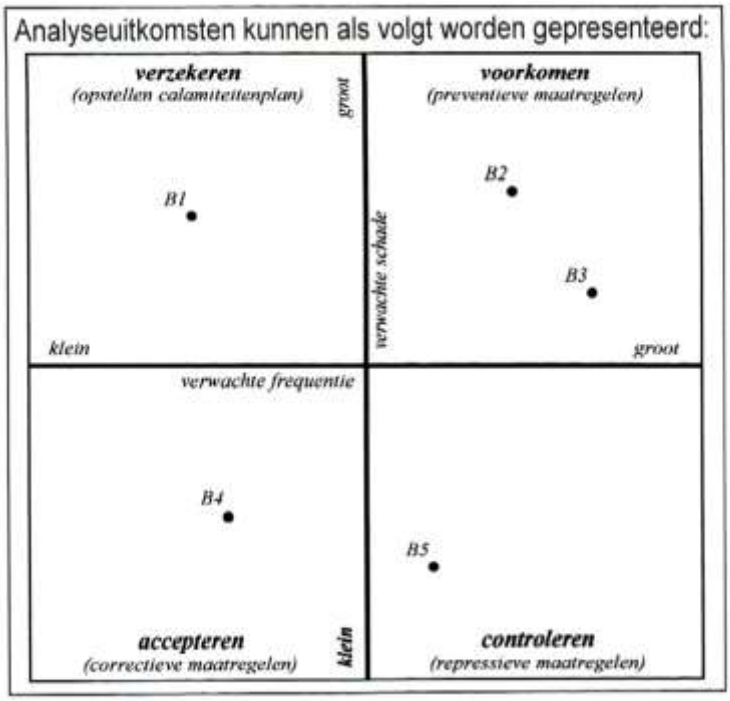
Figuur 3.9 Kwetsbaarheid en beveiligingsniveau voor bedreigingen per IS-object

1241 Risicoanalyse methoden - kwalitatieve risicoanalyse - **

blz 121 3.2.2 **maatregelanalyse -** heeft tot doel om tot een set beveiligingsmaatregelen te komen die het onderhavige IS zodanig beveiligen dat de risico's die overblijven acceptabel zijn.
Ook hier zijn weer een aantal stappen te onderscheiden >
1. bepalen vd maatregelen per IS-object;
2. bepalen vd maatregelen voor het gehele IS;
3. vergelijken vd set geselecteerde maatregelen met een referentielijst;
4. bepalen vd benodigde middelen en vaardigheden.

In het volgende figuur zijn verzekeren, voorkomen, accepteren en controleren de strategiën.

477



PREVENTIEF en KANS horen bij elkaar.

én

REPRESSIE en SCHADE horen ook bij elkaar.

Figuur 3.10
Verwachte frequentie en schade per bedreiging

vrg:	trefwoord	trefwrd onderverdeling	omschrijving	
1242	**Risicoanalyse methoden -**			****
blz 122 3.2.3	**kwantitatieve risicoanalyse -**		Deze gaat een stapje verder dan de Kwalitatieve, hier worden aan alle risico's een waarde verbonden dmv R = S*% en heeft minder beperkingen.	

478

Figuur 3.11 Voor- en nadelen van de kwalitatieve en kwantitatieve risicoanalyse

Risico = Kans * Schade

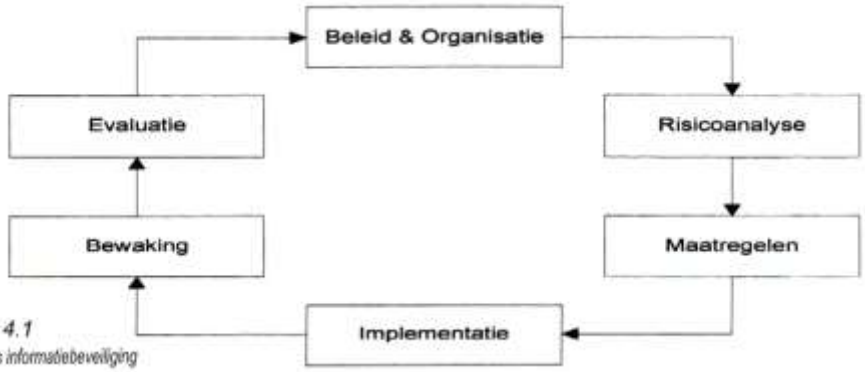
 = % * €

1243	**betrokken objecten en partijen -**			
blz 124 3.3			Bij ontwerp ve risicoanalyse zijn techniekgeörienteerde analyses te verdelen naar > - applicatiegericht en - infrastructuur gericht. Bij een bedrijfsgeorienteerde risicoanalyse dient met de volgende karisterieken in ogenschouw te nemen > - het aantal processen en hun onderlinge afhankelijkheid - de beheersbaarheid en voorspelbaarheid v processen - de gevoeligheid en stabiliteit vh proces - het reactiepatroon vh proces. Er zijn ook altijd 3 partijen betrokken bij een risicoanalyse (OUD) > 1. Opdrachtgever 2. Uitvoerder 3. Deelnemers	

ISMA	Hoofdstuk: 4	Informatiebeveiligingsbeleid

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1244	**Proces informatiebeveiliging -**		
blz 154 4.1	**proces informatiebeveiliging -**		heeft als uitgangspunt de beveiligingseisen ve organisatie. Vervolgende moet de organisatie dusdanig worden ingericht dat duidelijk is wie verantwoordelijk is voor de verschillende aspecten vd informatiebeveiliging. Nadat de risico's zijn geinventariseerd, kan een pakket maatregelen worden samengesteld om risico's te beperken, daarna worden ze geimplementeerd, bewaakt en geevalueerd. In dit boek wordt stap 1 Beleid en organisatie en stap 6 evaluatie verder behandeld (zie figuur).

479



Figuur 4.1
Het proces informatiebeveiliging

vrg:	trefwoord	trefwrd onderverdeling	omschrijving	
1245	**Informatiebeveiligingsbeleid -**			**

blz 155 4.2 **informatiebeveiligingsbeleid -**

CIO = Chief Information Officers

Als een organisatie bepaalde normen en waarden uitdraagt, dan zullen de uiteindelijk de te implementeren maatregelen niet strijdig zijn met deze normen en waarden.
Het informatiebeleid moet afgestemd zijn op het algehele organisatiebeleid en het informatiebeleid. Een goede afstemming geldt natuurlijk niet alleen tussen de verschillende soorten beleid onderling maar ook tussen de verschillende informatiebeveiligingsbeleidsdocumenten binnen de organisatie.

Het topmanagement vh informatiebeveiligingsbeleid kan het beste worden uitgevoerd door een groep lijnmanagers. Dat geeft de volgende voordelen >
- beleid wordt geschreven door mensen die het ook zelf actief zullen dragen, implementeren en uitvoeren binnen de organisatie.
- het beleid sluit dan goed aan bij >
  - gehanteerde terminologie in de organisatie
  - organisatiestructuur
  - bedrijfsprocessen
  - organisatiecultuur

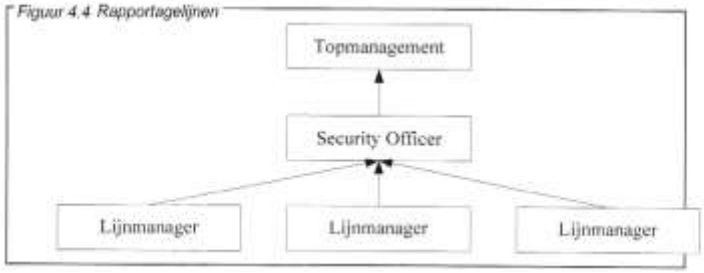
Maatregelen zijn nodig om de risisco's die de organisatie loopt en die de betrouwbaarheidsaspecten (BIV= beschikbaarheid, integriteit, vertoruwelijkheid) van de info en informatiesystemen in gevaar kunnen brengen, te voorkomen of beperken.
Om eenduidigheid te creeen zullen organisatie definities moeten formuleren.

481

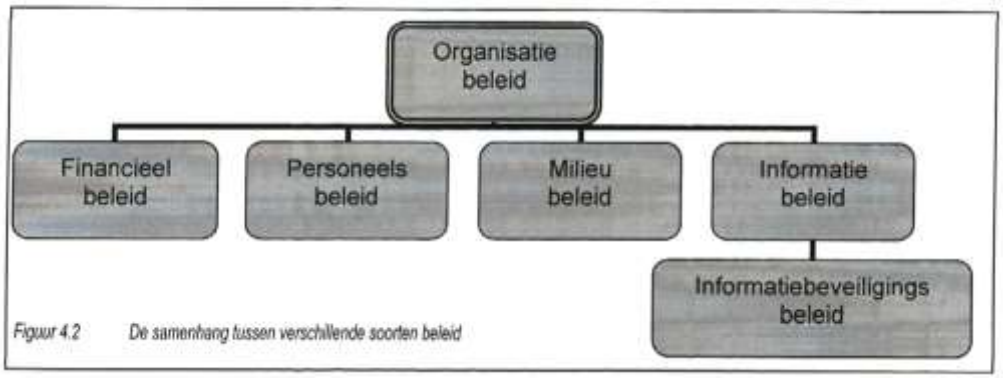
Inhoudsopgave

Figuur 4.3 Globale inhoudsopgave

Figuur 4.4 Rapportagelijnen



480



Figuur 4.2 De samenhang tussen verschillende soorten beleid

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1246	**Standaarden in het informatiebeveiligingsbeleid -**		
blz 163 4.3	**Standaarden in het informatiebeveiligingsbeleid -**		De VIR= Voorschrift Informatiebeveiliging Rijksoverheid is een voorschrift voor de (rijks)overheid zelf (1994). Stappen in het VIR-proces zijn; - opstellen informatiebeveiligingsbeleid; - inventarisatie; - afhankelijkheidsanalyse; - betrouwbaarheideisen; - kwetsbaarheidseisen; - beveiligingsmaatregelen; - opstellen infomatiebeveiligingsplan (IBP) met calamiteitenparagraaf en een keuze maken uit alle (informatie)beveiligingsmaatregelen die voortkomen uit de A&K-analyse; - opstellen implementatieplan (het IBP door het verantwoordelijke lijnmanagement laten Implementeren en onderhouden). Code voor informatiebeveiliging > hier wordt in hoofdlijnen aangegeven wat er in het informatiebeveiligingsbeleid opgenomen dient te worden. Doelstelling vh informatiebeveiligingsbeleid > is het bieden v sturing en ondersteuning aan het management ten behoeve van informatiebeveiliging.
1247	**Evaluatie -**		
blz 165 4.4	**Evaluatie - NOREA 6 domeinen -**		Evaluatie kan intern en extern worden uitgevoerd. INTERNE AUDIT = Interne evaluatie > evaluatie wordt door eigen medewerkers uitgevoerd EXTERNE AUDIT = Externe evaluatie > evaluatie wordt door een onafhankelijke partij uitgevoerd. De autdit heeft betrekking op (door de opdrachtgever) vooraf gespecificeerde bedrijfsprocessen, informatiesystemen en de hierbij behorende objecten. Deze kunnen ondergebracht worden bij een van de door NOREA (=Nederlandse Orde van Register EDP-Auditeurs) gedefinieerde DOMEINEN. De 6 NOREA-domeinen > 1.INFORMATIESTRATEGIE > hieronder valt het geheel van doelstellingen, uitgangspunten en randvoorwaarden voor het omgaan met informatie binnen een ondernemeing en voor het organiseren vd informatievoorziening. 2. INFORMATIE EN IT-MANAGEMENT (IM/IT-management) > slaat op de voorwaarden die leiding dienst te scheppen om geautomatiseerde systemen te ontwikkelen, te beheren en te gebruiken, alsmede op de voorwaarden om deze processen te besturen. 3. INFORMATIESYSTEMEN > omvat geautomatiseerde processen die primair ontworpen zijn om gegevens te genereren of manipuleren. 4. TECHNISCHE SYSTMEN > bestaat uit de technische systemen, geïmplementeerd in hardware en systeemware om die aan te sturen. 5. PROCESSYSTEMEN > zijn ontworpen om elektronische interface en daarmee apparaten (robots)aan te sturen. (ze zijn niet ontworpen om de mens te ondersteunen). 6. OPERATIONELE AUTOMATISERINGSONDERSTEUNING > omvat alle activiteiten ve organisatie die gericht zijn op het beheren en beschikbaar maken en houden vd technische infrastructuur en de onder beheer zijnde IT-systemen.

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1248	**Evaluatie -**		
blz 166 4.4	**NOREA 7** **kwaliteitsaspecten -**		1. EFFECTIVITEIT > de mate waarin een object in overeenstemming is met de eisen en doelstellingen vd gebruikers en of een object bijdraagt aan de organisatiedoelstellingen zoals die in de informatiestrategie zijn vastgelegd. 2. EFFICIËNTIE > is de verhouding tussen de gerealiseerde en begrote kosten ve object. Hieronder vallen 3 deelaspecten > - zuinigheid - herbruikbaarheid - de mate waarin productiviteit v gebruikers toeneemt 3. EXCLUSITIVITEIT > in hoeverre maken personen of apparatuur via procedures en beperkte bevoegdheden gebruik van IT-processen. Deelaspecten zijn hier > - authenticiteit - identificatie - controle op beveogdheden 4. INTEGRITEIT > is de mate waarop het object in overeenstemming is met de afgebeelde werkelijkheid. Hieronder vallen 3 deelaspecten > - nauwkeurigheid - volledigheid - waarborging 5. CONTROLEERBAARHEID > de mogelijkheid om kennis te verkrijgen over de structurering en werking ve object. Heeft 3 deelfactoren > - testbaarheid - meetbaarheid - verirfieerbaarheid 6. CONTINUÏTEIT > is de mate van continue beschikbaarheid ve object en de ongestoorde voortgang vd gegevensverwerking. Ook hier weer 3 delen > - beschikbaarheid - portabiliteit - herstelbaarheid 7. BEHEERSBAARHEID > de mate waartin het object kan worden aangestuurd en bijgestuurd. Is teverdelen in > - onderhoudbaarheid - effectiviteit (efficiency en tijdigheid vd correctieve maatregelen) - beveiliging

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1249	**Certificering -**		

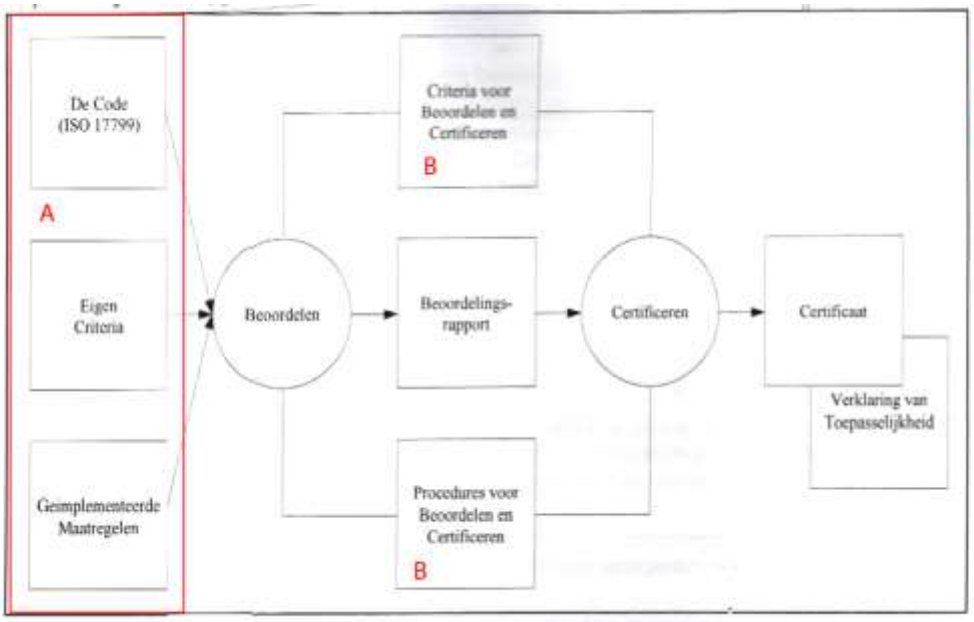
blz 168 4.5 **code voor informatiebeveiliging -**

Het boek bestaat uit 2 delen >
- 1. Code voor informatiebeveiliging > beschrijft het managementraamwerk en de te treffen beveiligingsmaatregelen.
- 2. is een specificatie voor managementsystemen voor Informatiebeveiliging.

Meestal 2 redenen om zich te laten certificeren >
1. INTERN > organisatie wil weten of voldaan is aan de Code voor informatiebeveiliging.
2. EXTERN > de organisatie wil de klanten/partners laten weten dat er of voldaan is aan de Code voor informatiebeveiliging.

Zie figuur 4.5 > schema is opgesteld met volgende oogmerken >
- moet inspelen op de behoefte ve breed scala aan bedrijvigheid in handel en industrie en bij overheid.
- de toepassing ervan moet een positieve afweging opleveren tussen baten en benodigde middelen.

484



Blok A > is de organisatie die het certificaat wil krijgen

B > dit zijn hulp-middelen om te kunnen beoordelen en te kunnen certificeren

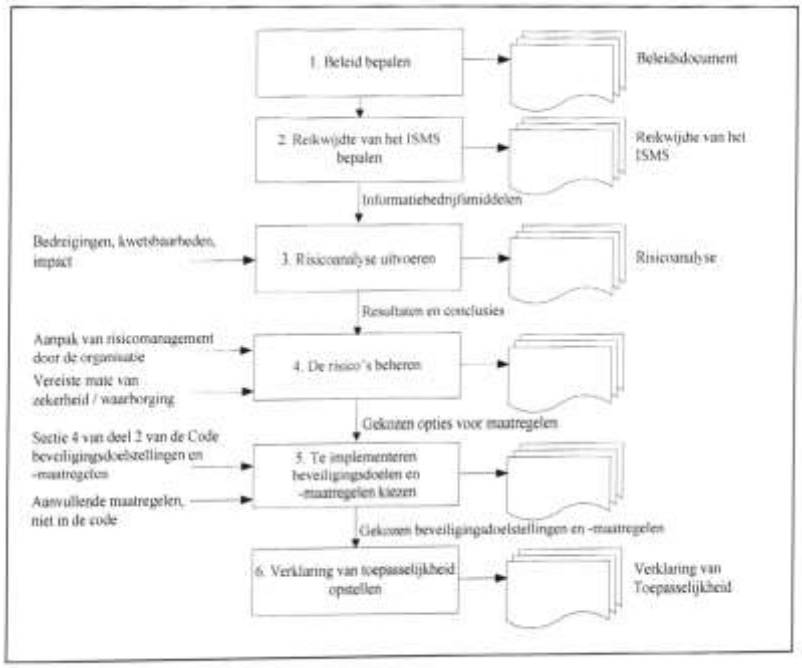
Figuur 4.5 *Het schema voor Certificatie van Informatiebeveiliging op basis van BS7799-2*

483

Voorbeeld:

Bedrijfsprocessen (Managementsystemen)	Producten	Personen
- ISO9000 - Code voor informatiebeveiling - ITIL - Prince 2 - CMM	- KEMA-keur - Common Criteria	- Microsoft Certified System Engineer - IT Auditor - HAVO diploma - Zwemdiploma's

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1250	**Certificering -**		
blz 169 4.5	**ISMS = Maangementsysteem voor informatiebeveiliging -** 485		Stappen zoals in de figuur 4,6 staan doorlopen om de beveiligingsdoelstellingen en -maatregelen te bepalen. Deze ook regelmatig evalueren.



Figuur 4.6 Het opzetten van een managementstructuur (komt voor figuur 4.5)

1251	**Certificering -**		
blz 170 4.5	**certificatieproces -**		beschrijft de algemen procedures die gevolgd moeten worden als > - een organisatie zich wil laten certificeren - de organisaties die deze audits uitvoeren. Certificatieproces bestaat uit > 1. AANVRAAG > men moet beschikken over een Verklaring v Toepasselijkheid (conformrmiteitsverklaring), dit bestaat uit minimaal > - naam vd organisatie - toepassinggebied - datum - versienummer - selectie v de voor deze organisatie relevante beveiligingsmaatregelen uit de Code - eventuale additionele beveilignsmaatregelen - ondertekening vh hoogste mangement vd organisatie of afdeling 2. PROEFBEOORDELING (optioneel) 3. DOCUMENTATIEONDERZOEK 4. IMPLEMENTATIEBEOORDELING > de te certificeren organisatie heeft nu ook tijd om weerwoord te geven. 5. BESLISSING TOT CERTIFICATIE > certificaat is meestal 3 jaar geldig. 6. PERIODIEKE CONTROLE > heeft vaste elementen > - intern audits uitgevoerd door te certificeren organisatie - aantoonbare werking vh mangementsysteem - behndeling v beveilingingsincidenten door de organisatie - beoordeling v eventuele wijzigingen in de IT-infrastructuur 7. HERBEOORDELING

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1252	**Informatiebeveiligingsplan -**		
blz 194 5	**informatiebeveiliging splan -**		geeft invulling aan het informatiebeveiligingsbeleid. In dit plan zijn oa opgenomen > - de concrete beveiligingsmaatregelen, - de beveiligingsmiddelen, - een verantwoording van de keuze voor de beveiligingsmaatregelen en - middelen, - de verantwoordelijkheden en richtlijnen voor de implementatie vd maatregelen. Onderdelen van een informatiebeveillgingsplan: 1. de doelstellingen en de reikwijdte van het plan; 2. de te beveiligen objecten en hun eigenaar; 3. organisatie van de informatiebeveiliging; taken, verantwoordelijkheden en bevoegdheden; 4. beveiligingseisen en -randvoorwaarden; 5. objecten, risico's en maatregelen; 6. nieuwe systemen; 7. toetsing en evaluatie van de maatregelen; 8. registratie en afhandeling van beveiligingsincidenten; 9. calamiteitenplan met uitwijk- en herstelprocedures; 10. opleidingsplan met betrekking tot informatiebeveiliging; 11. plannen voor de bevordering van het beveiligingsbewustzijn; 12. planning; 13. kosten. Consequenties > - restrisico's; - naleving; - aanpassing; - kosten. Beveiligingsmaatregelen zijn in te delen naar > - werkwijze (fysiek / technisch / organisatorisch); - effect (preventief / dedectief / repressief / correctief) ; - betrouwbaarheidsaspect (Beschikbaarheid / Integriteit / Vertrouwelijkheid).

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1253	**Standaardisatie v informatiebeveiliging -**		

procesgerichte standaardisatie - 6.1.1

voordelen >
- eenzelfde informatiebeveilingscode kan informatieuitwisseling optimaal laten verlopen;
- door grotere uniformiteit in werkwijzen minder fouten worden gemaakt.

Standaardisatie volgens ISO-normen >
- ISO 13335 > Guidelines for the Management of IT Security (GMITS) > 5 delen report t.b.v. beveiligingsmanagement >
  1. overzicht v fundamentele concepten en modellen die bedoeld zijn om het management v informatiebeveiling te beschrijven;
  2. richt zich op invoering en handhaving en de mangements- en planningsaspecten daarvan;
  3. spitst zich toe op bestaan beveiligheidstechnieken, doelgroep medewewrkers met bepaalde verantwoording voor bepaalde fase.
  4. geeft richtlijnen om een selectie v beschermingsmaatregelen te maken en hoe deze te ondersteunen.
  5. behandelt de aspecten waarmee te maken krijgt bij het aansluiten v IS aan externe netwerken.
- ISO 14516 > Guidelines for the Use and Management of TTP (Trusted Third Parties). Technical report voor partijen die TTP willen opzetten
- ISO 17799 > Information Technology - Code of practice for information security. Wereldwijd geaccepteerde, gedetailleerde standaard in informatiebeveiliging, gebaseerd op de Britse Code of Practice. De standaar bestaat ui 10 secties >
  1. beveiligingsbeleid
  2. organisatie vd beveiliging
  3. classificatie en beheer vd bedrijfsmiddelen
  4. personeel
  5. fysieke beveiliging en omgeving
  6. computer- en netwerkbeheer
  7. toegangsbeveiliging
  8. ontwikkeling en onderhoud van systemen
  9. continuïteitsplanning
  10. toezicht

  De te ondernemen maatregelen kunnen zijn > training, viruscontrole e.d.
- ISO 15408 > Common Criteria for Information Technology Security Evaluation; CC is gebaseerd op Orange Bock en ITSEC. Kernbegrip: Target Of Evaluation (TOE), dit heeft 3 basisvoorwaarden >
  a. verzameling beveiligingseisen en -specificaties die bij TOE horen;
  b. De TOE waarvoor de evaluatie is vereist;
  c. de evaluatiecriteria en methodologie.

  CC aandachtsgebeiden voor TOE >
  - beveiligingsomgeving > rekening houden met >
    - fysieke omgeving van de TOE;
    - bedrijfsmiddelen
    - rol vd specifieke TOE en bijbehorende gebruikersmogelijkheden.
  - beveiligingsdoelstellingen;
  - beveiligingsvoorwaarden.

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1254	**Standaardisatie v informatiebeveiliging - procesgerichte standaardisatie -**		
blz 221 6.1.1	**Orange Book -**		Evaluatie van de geschiktheid van beveiligingsmethoden; biedt een certificatie met betrekking tot > - beveiligingsbeleid, - verantwoordelijkheden, - zekerstelling en - documentatie. Drie-delig doel: - geeft gebruikers een handvat voor in hoe verre mate het systeem gevoelige informatie kan worden toevertrouwd; - voorziet systeembouwers van een standaard v beveiligingsmethoden; - schept een basis voor specificeren v beveiligingseisen bij aanschaf en implmentatie van nieuwe systemen. Orange Book onderschei 4 niveau's > - D > minimal protection > gebeurt zelden - C > discretiony protection - B > mandotory protection - A > verified protection
1255	**Standaardisatie v informatiebeveiliging -**		
blz 222 6.1.2	**technische standaardisatie = productstandaardisatie -**		technische standaardisatie = productstandaardisatie = op techniek gericht. Heeft betrekking op het standadiseren van producten, systemen of delen daarvan. Voorbeelden zijn algoritmen voor encrypties, besturingssystemen voor UNIX of Windows of GSM, toegangsbeheersing zoals pinpassen, TCP/IP protocollen e.d. - ISO 10181 > Security frameworks for open systems. Gebaseerd op het OSI-model, beschreven in de 7 te onderscheiden lagen. - ITSEC > Maakt onderscheid tussen systemen en producten; biedt een set evaluatiecriteria met het security target als centraal document (beveiligingsfunctionaliteit van de TOE, evenals de omgeving en het na te streven doel); evaluatieniveaus van E0 tot en met E6, waarbij 6 het hoogste is. Kan gezien worden als een verder ontwikkeling op basis van Orange Book, hier wordt ook aandacht besteed aan integriteit en beschikbaarheid.

90

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY		Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

vrg:	trefwoord	trefwrd onderverdeling	omschrijving
1256	**methoden en hulpmiddelen -**		
blz 225 6.2.1	**risicoanalyse -**		Methoden en hulpmiddelen op het gebied van de informatiebeveiliging zijn in dit hoofdstuk als volgt ingedeeld: - Risicoanalyse - Standaard: Quickscan en checklist Het betreft in feite eenvoudige vragenlijsten of afvinklijsten, om na te gaan in hoeverre een bedrijf of organisatie de informatiebeveiliging op orde heeft. - Quick scan Bescherming Persoonsgegevens Vragen zijn als volgt ingedeeld > - privacy bewustzijn in de organisatie; - uitvoering wettelijke bepalingen - beveiliging - Quickscan met behulp van Vragenlijst Fysieke Beveiliging > onderwerpen > - gebouwen en omgeving - fysiek toegangsbeheer - organisatorische aspecten - veiligheid v personeel en bezoekers - kritische ruimten - continuïteitsvoorzieningen - Checklist Informatiebeveiliging 1. beveiligingsbeleid 2. beveiligingsorganisatie 3. classificatie en beheer v bedrijfsmiddelen 4. beveiligingseisen tav personeel 5. fysieke beveiliging en beveiliging omgeving 6. beheer v communicatie- en beslissingsprovessen 7. toegangsbeveiliging 8. ontwikkeling en onderhoud v systemen 9. continuïteitsmangement 10. naleving

1257 methoden en hulpmiddelen - risicoanalyse - overige analyses -

blz 231 **CRAMM -**

6.2.1

Maatwerk: overige analyses

Minder standaard, meer bedrijfspecifiek georiënteerde analyses op het gebied van de informatiebeveiliging.

CRAMM = CCTA Risk Analysis and Management Method >

vormt een volledige voor de bij de meeste bedrijven welbekende ISO-norm 17799. Hanteert een systematische aanpak die verdeeld is in drie stappen: in beeld brengen van de organisatie, definiëren van het risicoprofiel en selecteren van de noodzakelijke beveiligingsmaatregelen en opstellen van een lijst van aanbevelingen.

Methodiek CRAMM >

1. in beeld brengen vd organisatie
2. definieren risicoprofiel
3. selecteren vd noodzakelijke beveiligingsmaateregelen en opstellen ve lijst v aanbevelingen.

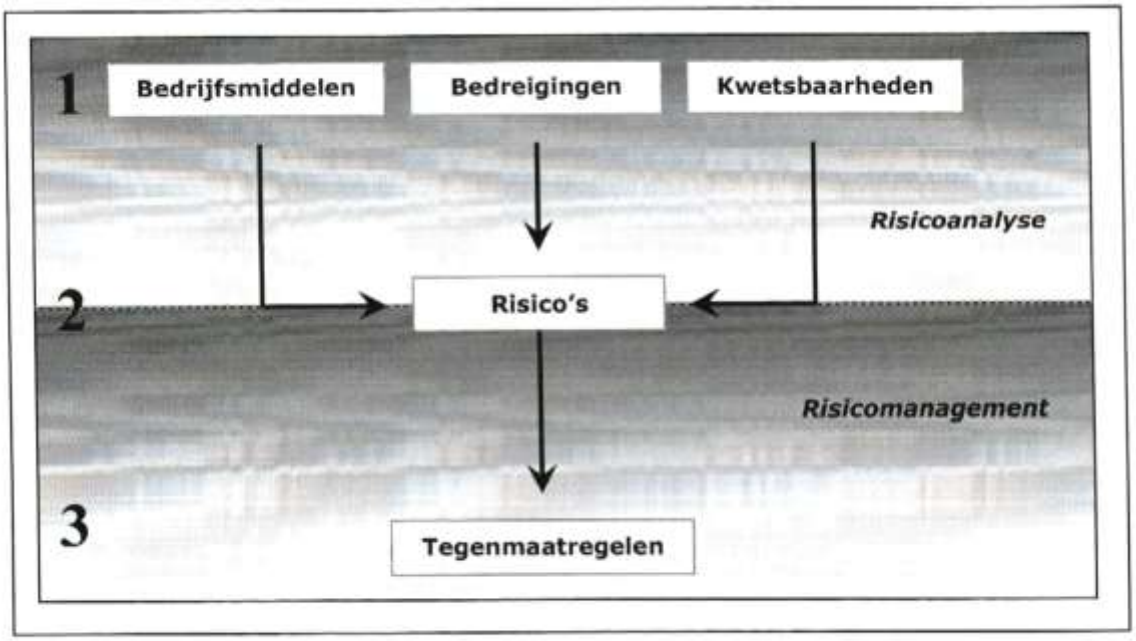
Per maatregelgroep worden maatregelen op drie niveau's gedefinieerd >

1. beveiligingsdoelstellingen
2. functies
2. opties/voorbeelden

CRAMM vereist een hoge mate v kundigheid en ervaring vd uitvoerders.

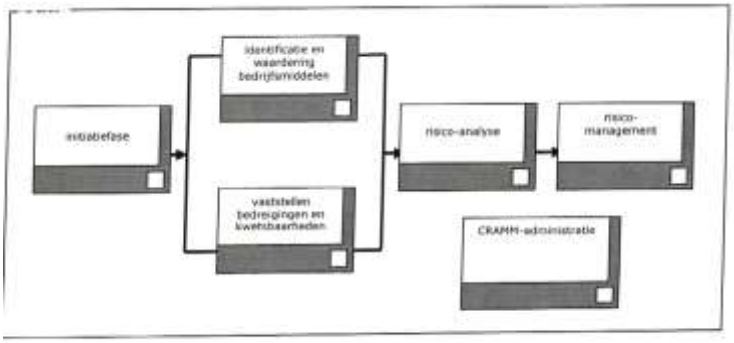
De CRAMM-tool is niet flexibel.

486



Figuur 6.1 Aanpak van CRAMM

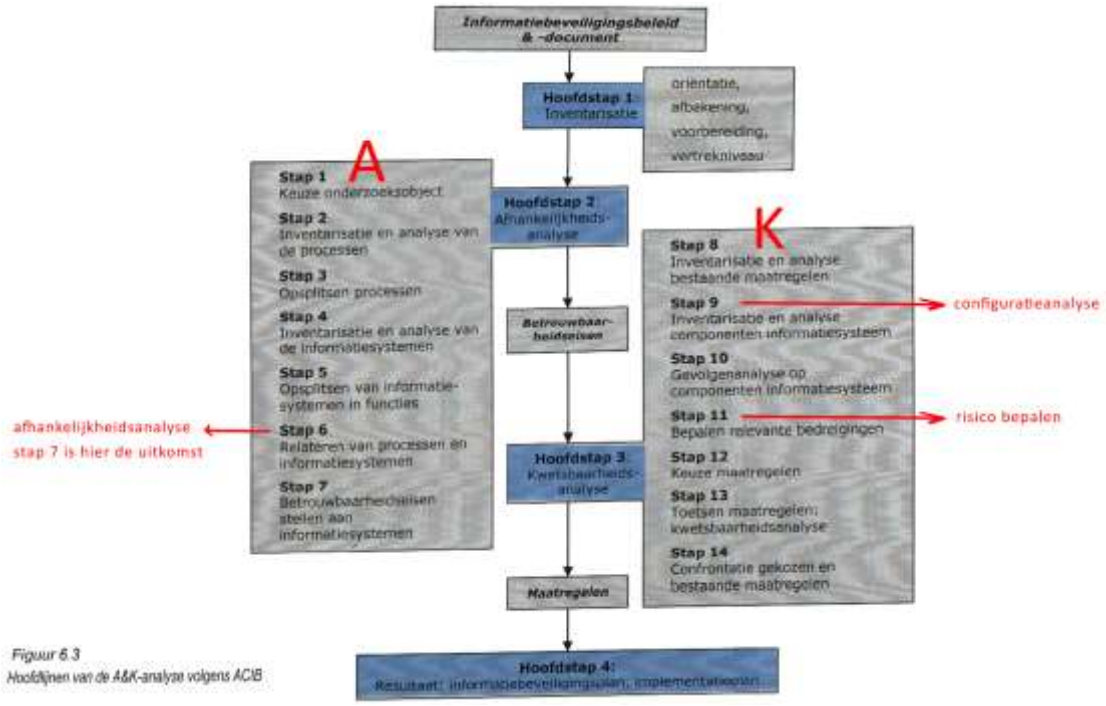
487



Figuur 6.2 Processtroom in CRAMM-tool

vrg:	trefwoord	trefwrd onderverdeling	omschrijving	
1258	**methoden en hulpmiddelen - risicoanalyse - overige analyses -**			**
blz 234 6.2.1	**A&K-analyse -**		A&K-analyse (ACIB) > Bedoeld om de afhankelijkheid van het bedrijfsproces van informatiesystemen en de kwetsbaarheid van informatiesystemen voor bedreigingen in kaart te brengen. De 4 hoofdstappen zijn 1. inventarisatie 2. afhankelijkheidsanalyse 2a. vastellen v afhankelijheden 2b. opstellen v betrouwbaarheidseisen 3. kwetsbaarheidsanalyse 3a. vastellen van kwetsbaarheden 3b. opstellen v informatiebeveiliginsplan 4. implementatie 4a. implementeren v informatiebeveiliginsmaatregelen 4b. opstellen vh definitieve informatiebeveiligingsplan 4c. Beheer en naleving vh informatiebeveilingsplan	

488



Figuur 6.3
Hoofdlijnen van de A&K-analyse volgens ACIB

1259	**methoden en hulpmiddelen - risicoanalyse - overige analyses -**			
blz 237 6.2.1	**Trusted Third Party (TTP) -**		Wordt ingezet wanneer elke vorm van wantrouwen tussen twee partijen bij uitwisseling moet worden weggenomen/voorkómen. Middelen zijn hier > - sleutelbeheer - certificatenbeheer - integriteitsgarantie - data recovery - ondersteuning bij identificatie - authenticatie en autorisatie - non-repudiation > voorkomt dat de ontvanger of zender, het verzenden vh bericht ontkent. - time stamping > vastellen wanneer een bericht is verzonden en/of is ontvangen - elektronisch notariaat > vasteleggen v gepleegde transacties en verzonden en ontvangen berichten - directory diensten > bijhouden register v gebruikers met adressen, sleutels, certificaten ed.	informatie