Informatieclassificatie Vlaamse overheid (Vo-ICR)

Risicobeheer - methodiek

methodiek

Team Informatieveiligheid| Digitaal Vlaanderen

Dit is een document voor publiek gebruik

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

INHOUD VAN DIT DOCUMENT

Situering van het document

Dit document maakt deel uit van de begeleidende documentatie in context van het generieke informatieclassificatieraamwerk (ICR) van de Vlaamse overheid (Vo) op initiatief van het Stuurorgaan Vlaams Informatie- en ICT Beleid.

Doel van het document

Dit document beschrijft de methodiek die gebruikt kan worden in het kader van het uitvoeren van een risicoanalyse.

Verspreiding van het document

Dit document is voornamelijk voor intern gebruik en bevat informatie die mag gedeeld worden met personen verbonden aan de Vo en zijn diensten leveranciers.

Het document mag gedeeld worden met derden onder de richtlijnen openbaarheid van bestuur van de Vlaamse regering.

Vrijwaring

Dit document geeft de huidige status en daaraan gerelateerde informatie binnen het project weer. Gelieve de auteur of de bevoegde project begeleiders te contacteren om zich ervan te vergewissen dat u de laatst gevalideerde versie van dit document in handen heeft.

Eigenaar

Voorzitter werkgroep informatieveiligheid | Digitaal Vlaanderen

security@vlaanderen.be

Classificatie

Dit document valt onder de vertrouwelijkheidsklasse 1 (Publiek) en mag toegankelijk zijn voor iedereen.

Dit document valt onder integriteitsklasse 2. De organisatie heeft **geen directe hinder** indien de informatie gewijzigd wordt door onbevoegden en de **dienstverlening blijft gegarandeerd**. Maar bijsturing van de criteria en/of maatregelen is aangewezen.

Historiek

	Datum	**Auteur**	**Opmerkingen**
v.0.1	7 mei 2020	Guy KLERKX	Draft

v.0.2	12 mei 2020	Kristel VAN AKEN	Feedback
v.0.3	12 mei 2020	Guy KLERKX	Verwerken feedback 1
v.0.4	19 mei 2020	Guy KLERKX	Verwerken feedback 2
v.0.5	20 mei 2020	Guy KLERKX	Verwerken feedback Johan Smekens/Beau Janssens
v.0.6	16 juni 2020	Guy KLERKX	Verwerken feedback Kristel Van Aken
v.0.7	10 juli 2020	Guy KLERKX	Verwerken feedback taakgroep
v.0.8	2 september 2020	Guy KLERKX	Verwerken feedback leespanel
V1.0	8 september 2020	Kristel VAN AKEN	Publicatie
V2.0	29 augustus 2022	Kristel VAN AKEN	Verbeteren leesbaarheid Geen inhoudelijke wijzigingen

Bronnen en verwijzingen

De inhoud van dit document werd samengesteld op basis van volgende documenten:

Documentverwijzingen:

- *Vo Informatieclassificatie – Organisatie Informatieveiligheid* (PDF)
- *Vo Informatieclassificatie – Organisatie Informatieclassificatieraamwerk* (PDF)
- Vo Informatieclassificatie – Minimale maatregelen – (PDF)
  - *Vo Informatieclassificatie - Minimale maatregelen –Risicobeheer*
- Vo Informatieclassificatie – Overzicht baseline maatregelen (XLS)

INHOUDSOPGAVE

1. INLEIDING

1.1. Waarom werken volgens een methodiek?

Bij methodisch werken gaat het niet meer om intuïtief handelen, maar om een methodische en systematische aanpak waaraan voordelen zijn verbonden:

- de kans op fouten neemt af omdat er meer greep is op wat er gebeurt en men verder vooruit kan zien;
- zowel een ander als jijzelf weet wat er verwacht mag worden;
- het eigen handelen kan beter geëvalueerd worden om zo nodig het handelen te verbeteren;
- anderen krijgen een duidelijker beeld van de werkzaamheden en van datgene waarvoor men staat.
- nastreven van uniformiteit.

Methodisch handelen is dus werken volgens een weldoordachte manier om op een zo effectief en efficiënt mogelijke manier het doel te bereiken dat je voor ogen hebt. Methodisch werken heeft ook te maken met het streven naar verbetering van de kwaliteit.

Methodisch werken is een vorm van procesbesturing, zoals beschreven in het document ‘‘Vo informatieclassificatie – Minimale maatregelen – Proces Risicobeheer“. Het heeft als doel iets op een beheerste, gestructureerde en gecontroleerde wijze te laten verlopen. Methodisch werken heeft vier kenmerken:

- het handelen is doelgericht en bewust: De uitvoerder weet wat hij doet (bewust) en waarom (doel).
  - gericht op een concreet en vooropgesteld doel;
  - continu scherp op middel en doel;
  - doen wat bijdraagt aan doel, niet wat er niet aan bijdraagt;
  - aan anderen uit kunnen leggen wat je doet en waarom;
  - kritisch en structureel terugblikken op (eigen) handelen.
- het handelen is systematisch en dus repetitief: het verloopt volgens van te voren geplande stappen. Deze stappen zijn afgeleid van de doelstelling.
  - logische stappen;
  - gefaseerd werken;
  - niet ad hoc of te snel conclusies trekken.
- het handelen is procesmatig: de verschillende stappen sluiten op elkaar aan. Daarbij wordt rekening gehouden met het effect dat de ene stap op de andere heeft.
  - De ene actie schept voorwaarden voor de volgende actie(s);
  - Een ‘foute’ inschatting is onderdeel, geen einde; aan anderen uit kunnen leggen wat je doet en waarom;
  - kritisch en structureel terugblikken op (eigen) handelen.

2. RISICOMETHODIEK

2.1. Risicomethodiek in het kader van Vo informatieclassificatiemodel

Een programma voor informatiebeveiliging kan diverse grote en kleine doelen nastreven, maar de belangrijkste principes zijn te herleiden naar beschikbaarheid, integriteit en vertrouwelijkheid (BIV).

De definities van 'beschikbaarheid, 'vertrouwelijkheid' en 'integriteit' zijn al gegeven binnen het document 'Vo Informatieclassificatie – Minimale maatregelen - informatieveiligheid'. De controlemaatregelen die op grond van deze basisprincipes ingericht worden, variëren per organisatie, maar zijn steeds in lijn met het Vo informatieclassificatiemodel. Dit komt omdat elke organisatie haar eigen specifieke eisenpakket opstelt op basis van haar bedrijfs- en beveiligingsdoelen- en eisen.

Met behulp van de risicomethodiek wordt binnen de Vo een kader gegeven om te kunnen streven naar een uniformiteit tot het uitvoeren van risicoanalyses en het bepalen van maatregelen.

Alle beveiligingsmaatregelen worden geïmplementeerd om één of meer van deze BIV-principes in te vullen. Alle bedreigingen worden beoordeeld op hun vermogen om één of meer van de BIV-principes schade toe te brengen.

Beschikbaarheid, integriteit en vertrouwelijkheid zijn dus essentiële principes voor informatiebeveiliging. Ze helpen om bedreigingen te identificeren en deze op een gepaste manier aan te pakken.

Risicobeheer is pas effectief als het een integraal onderdeel is van de processen van de organisatie. Daarom moet een raamwerk gehanteerd worden dat bepaald welke de criteria rond risicoanalyses zijn, hoe het proces risicobeheer eruit ziet, de methodiek en welk instrumentarium kan aangewend worden.

Scope, doelgroep en voordelen

De risicomethodiek is bedoeld voor alle typen organisaties binnen de Vo, ongeacht grootte en aard van de activiteiten, en is vooral gericht op organisatie-brede risico's.

De doelgroep van dit document is heel divers: verantwoordelijken voor risicobeheer binnen organisaties als geheel of voor specifieke onderdelen of activiteiten, maar ook personen/organisaties die er op toe moeten zien dat een organisatie haar risico's goed beheert of de aanpak daarvan moet beoordelen, waaronder businessanalysten, toepassingsbeheerders en projectmanagers.

Rollen en verantwoordelijkheden

Binnen de uitvoering van een risicoanalyse zijn volgende actoren betrokken:

Rollen	Verantwoordelijkheden
CISO/ISO	• vastleggen risicoanalysemethodiek van de organisatie conform de wet- en regelgeving; • vastleggen van de nodige tools voor risicoanalyses; • uitvoeren, meewerken aan of initiëren van risicoanalyses inzake informatieveiligheid; • erover waken dat risicoanalyses worden uitgevoerd conform het beleid van de organisatie. • Erover waken dat de risicoanalyses conform de vastgelegde methodiek worden uitgevoerd.

DPO/PO	• meewerken aan of initiëren risicoanalyse inzake bescherming van persoonsgegevens; • erover waken dat DPIA's worden uitgevoerd conform de wet- en regelgeving en het beleid van de organisatie. • Erover waken dat de uitgevoerde DPIA's volgens de vastgelegde methodiek worden uitgevoerd.
Topmanagement	• De nodige budgetten en werkingsmiddelen aanreiken, ondersteunen van het uitvoeren van risicoanalyses; • goedkeuring risico-verslag; • goedkeuring toe te passen risico-strategie; • Acceptatie restrisico.
Lijn management	• Vastellen risico-verslag; • Beoordeling toe te passen risico-strategie.
Coördinator risicoanalyse	• Het begeleiden en faciliteren van de risicoanalyse; • Opstellen verslag risicoanalyse.
Proces-eigenaar / Informatie-eigenaar (inclusief projecteigenaar, business-analysten)	• Vaststellen van de processen in scope van de risicoanalyse; • Beoordelen prioriteit v/d processen; • Vaststellen van de gebruikte informatie; • Beoordelen van de relevante bedreigingen; • Beoordelen beveiligingsmaatregelen.
Systeem-eigenaar (inclusief toepassingsbeheerders)	• Vaststellen van de systemen in scope van de risicoanalyse; • Beoordelen prioriteit v/d systemen; • Beoordelen van de relevante bedreigingen; • Beoordelen beveiligingsmaatregelen.

Overzicht per RACI-model:

		verantwoordelijke	aansprakelijke	raadpleging	informeren
Analyse van de zakelijke omgeving	**vaststellen context**	coördinator risicoanalyse	topmanagement / lijnmanagement	proces-eigenaar / informatie-eigenaar / systeem-eigenaar	DPO/PO/ ISO/ISO
	vaststellen scope	coördinator risicoanalyse	topmanagement / lijnmanagement	proces-eigenaar / informatie-eigenaar / systeem-eigenaar	DPO/PO/ ISO/ISO
Risicobeoordeling	**risico-identificatie**	coördinator risicoanalyse	topmanagement / lijnmanagement	proces-eigenaar / informatie-eigenaar / systeem-eigenaar / CISO / DPO	
	risicoanalyse	coördinator risicoanalyse	topmanagement / lijnmanagement	proces-eigenaar / informatie-eigenaar / systeem-eigenaar / CISO / DPO	
	risico-evaluatie	coördinator risicoanalyse	topmanagement / lijnmanagement	proces-eigenaar / informatie-eigenaar / systeem-eigenaar / CISO / DPO	
	bepalen risicostrategie	coördinator risicoanalyse	topmanagement / lijnmanagement	proces-eigenaar / informatie-eigenaar / systeem-eigenaar / CISO / DPO	
Risicobehandeling		coördinator risicoanalyse	topmanagement / lijnmanagement	proces-eigenaar / informatie-eigenaar / systeem-eigenaar	DPO/PO/ ISO/ISO
Communicatie en -overleg		coördinator risicoanalyse	topmanagement / lijnmanagement	proces-eigenaar / informatie-eigenaar / systeem-eigenaar	DPO/PO/ ISO/ISO
Monitoring en beoordeling		coördinator risicoanalyse	topmanagement / lijnmanagement	proces-eigenaar / informatie-eigenaar / systeem-eigenaar	DPO/PO/ ISO/ISO

2.2. De methodiek binnen de bouwstenen van het proces risicobeheer

Het risicobeheersproces kent volgende activiteiten:

- Analyse van de zakelijke omgeving
  - vaststellen context en scope
  - validatie minimale maatregelen IC
- Risicobeoordeling
  - risico-identificatie
  - risicoanalyse
  - bepalen risicostrategie
  - risico-evaluatie
- Risicobehandeling
- Communicatie en -overleg
- Monitoring en beoordeling

Deze activiteiten worden in detail besproken in het document '[Vo informatieclassificatie – Minimale maatregelen –risicobeheer]'.

2.3. Analyse van de zakelijke omgeving

Vaststellen context

Het is van cruciaal belang dat de aanleiding om juist nu een risicoanalyse uit te voeren goed bekend is.

- beschrijven van de context:

  hierbij moet men zich richten op de reden waarom de gegevens in scope van de risicoanalyse worden verwerkt, meer bepaald de doelstelling van de verwerking, en welke categorieën gegevens hierbij betrokken zijn. Op basis van de betrokken businessprocessen kunnen deze gegevens in beeld gebracht worden. Dit alles om zo de context van de risicoanalyse beter te kunnen beschrijven.

Rollen	Werkwijze	Middelen
• coördinator • proces-eigenaar • systeem-eigenaar	• nagaan welke categorieën gegevens verwerkt worden • nagaan om welke reden deze gegevens verwerkt worden, waarbij de doelstelling van de verwerking gedocumenteerd wordt • omschrijven van de context van de risicoanalyse	• interview met applicatie-eigenaar, workshop • sjabloon rapport risicoanalyse

Resultaat

- een omschrijving van de context tot de gevraagde risicoanalyse, met een inzicht in de betrokken categorieën gegevens die verwerkt wordt
- dit wordt binnen het rapport van de risicoanalyse genoteerd

Vaststellen scope

Dit houdt in eerste instantie in dat de betrokken zakelijke **processen** in beeld worden gebracht om zo een beeld te krijgen over welke **informatie** er verwerkt wordt, en welke relevante **systemen** hierbij betrokken zijn. Deze elementen vormen de scope van de risicoanalyse.

Informatie

Alle informatie die aangesproken worden binnen het betrokken zakelijke proces, dienen in beeld gebracht te worden.

- in kaart brengen van informatie:
  - oplijsten van de betrokken zakelijke processen binnen de scope van de risicoanalyse;
  - oplijsten van de informatie verwerkende systemen die de betrokken zakelijke processen ondersteunen – deze oplijsting dient beperkt te blijven tot direct gerelateerde toepassingen en infrastructuur gebruikt binnen het zakelijke proces, alsook het in beeld brengen van betrokken keteninfrastructuur en zijn eigenaars met een verwijzing naar een risicoanalyse hierin. Risico's die geërfd worden(bv. O365) dienen niet opgenomen te worden.
  - oplijsten van alle informatie die in de betrokken zakelijke processen verwerkt wordt – dit per gegevenscategorie in detail vermelden
  - deze gegevens aftoetsen aan het Vo informatieclassificatie model, nl. bepalen tot welke classificatieschaal deze gegevens behoren;
  - de maturiteit bepalen van de reeds genomen controlemaatregelen, binnen de Vo informatieclassificatie model, aan de hand van de volgende beoordelingstabel:

Maturiteit controlemaatregel	Score	Rating	Beschrijving
	5	Effectief	Solide / betrouwbare / effectieve controlemaatregelen
	4	Gelimiteerde verbeteringen mogelijk	Solide controlemaatregelen, maar geïdentificeerde verbeteringen mogelijk
	3	Gemiddelde verbeteringen mogelijk	Bestaande controlemaatregelen, maar significante verbeteringen mogelijk
	2	Significante verbeteringen mogelijk	Gelimiteerde controlemaatregelen, restrisico blijft hoog
	1	Kritieke verbeteringen mogelijk	Quasi onbestaande of ineffectieve controlemaatregelen

De maturiteit van een controlemaatregel bepaalt mee de kwetsbaarheid van een bedreiging: hoe lager de maturiteit, hoe hoger de kwetsbaarheid van de omgeving op een bedreiging kan zijn.

Rollen	Werkwijze	Middelen
〉 coördinator 〉 proces-eigenaar 〉 systeem-eigenaar	〉 oplijsten van de betrokken zakelijke processen binnen de scope van de risicoanalyse; 〉 oplijsten van de informatieverwerkende systemen die de betrokken zakelijke processen ondersteunen 〉 oplijsten van de informatie die in de betrokken zakelijke processen verwerkt wordt 〉 deze gegevens aftoetsen aan het Vo informatieclassificatie model, nl. bepalen tot welke classificatieschaal deze gegevens behoren 〉 de maturiteit bepalen van de reeds genomen controlemaatregelen, binnen het Vo informatieclassificatiemodel bepalen	〉 workshop 〉 sjabloon rapport risicoanalyse

Resultaat
〉 een overzicht van de betrokken zakelijke processen, de gerelateerde betrokken systemen, categorisatie en specificatie van de informatie, classificatieschaal en een maturiteitsoverzicht van de bestaande controlemaatregelen 〉 dit wordt opgenomen binnen het rapport van de risicoanalyse

<u>Systemen</u>

Inzicht in de gebruikte systemen is nodig om in de volgende stap, nl. de bedreigingen goed in kaart te kunnen brengen.

Binnen de Vo zal hiervoor een model, zoals verder beschreven onder “risico-identificatie”, gebruikt worden.

Het is hierbij de bedoeling dat deskundigen - bijvoorbeeld de proceseigenaar, de systeemeigenaar en de toepassingseigenaar - de betrokken componenten voor het betrokken informatiesysteem gaan beschrijven. Hierbij wordt dan in beeld gebracht welke **mensen** het informatiesysteem beheren en gebruiken welke een invloed kunnen hebben op het functioneren van het informatiesysteem, en welke **technische** en **organisatorische aspecten** er bestaan waardoor het informatiesysteem niet meer kan functioneren.

Met het begrip systeem bedoelen we hier de alomvattende elementen binnen een ICT-landschap: netwerk-apparatuur, servers(printer, database, website,…), cloud-elementen, toepassingen,…
Deze oplijsting dient wel beperkt te blijven tot direct gerelateerde toepassingen en infrastructuur die binnen het zakelijke proces gebruikt worden.

2.4. Risicobeoordeling

Op basis van het verkregen inzicht in de te beoordelen informatie en de systemen, kunnen keuzes gemaakt worden voor de volgende stappen .

Risicobeoordeling is gebaseerd op de volgende stappen:

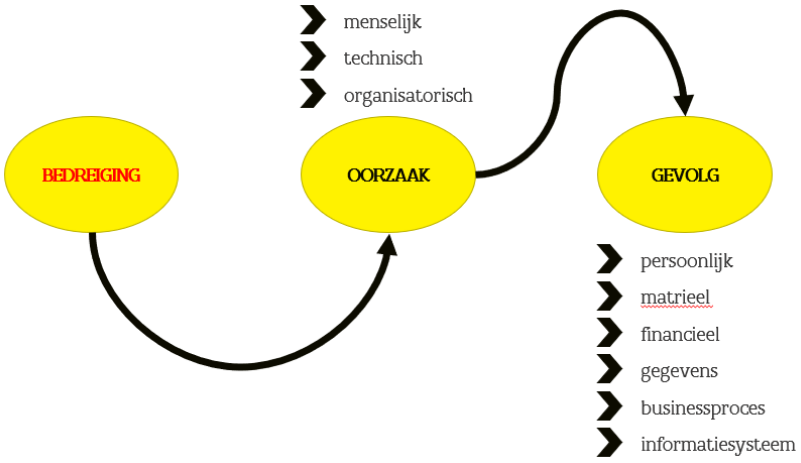
- risico-identificatie
- risicoanalyse
- bepalen risicostrategie
- risico-evaluatie

Risico-identificatie

Het doel van risico-identificatie is om inzicht te krijgen in de bedreigingen. Bij de risico-identificatie is het van belang om een brede en gestructureerde benadering te hanteren.

De relevante bedreigingen worden in kaart gebracht. Dit is een taak voor de coördinator van de risicoanalyse in samenwerking met een aantal deskundigen, zoals de systeemeigenaar, CISO/ISO, DPO/PO. Het betreft bedreigingen waardoor verlies aan beschikbaarheid, integriteit of vertrouwelijkheid van de informatievoorziening kan ontstaan.

Middels naaststaand model kan een bedreiging gekoppeld worden aan een oorzaak en gevolg, dit op basis van de eerder vermelde componenten, welke een gevolg kunnen hebben op het functioneren van het informatiesysteem, nl.: menselijke aspecten, technische incidenten en organisatorische fouten.



Er bestaan immers allerhande bedreigingen op vlak van gegevens, betrokken systemen en processen, die de doelstellingen van een instantie kunnen bedreigen.

Op basis van bovenvermeld model kunnen we bedreigingen vaststellen. Dit doen we door de verschillende elementen met elkaar te combineren. Zo komen we tot een uitgebreide lijst van relevante bedreigingen.

> Bv. *"Er bestaat een kans op een **bedreiging** dat subsidies niet op tijd uitbetaald kunnen worden dat **veroorzaakt wordt door** een technisch incident, namelijk gebruik van verouderde databaseservers, met **als gevolg** dat er een financieel verlies is tengevolge van opgelegde boete's"*

Via dit model is het zo mogelijk om tot een Vo-breed gehanteerde risicoanalyse te komen, opdat de bedreigingen op een uniforme manier vastgesteld kunnen worden. Het resultaat zal zo leiden tot een vergelijkbare risicoanalyse binnen de Vo.

Het model biedt in eerste instantie een handvat om bedreigingen te analyseren waarbij de mogelijkheid bestaat deze risico-identificatie verder uit te breiden. Dit geeft iedere instantie meer vrijheid bij het oplijsten van bedreigingen en is zo meer afgestemd op de maturiteit van de instantie.

Het resultaat is een lijst van bedreigingen, dus een overzicht van omstandigheden die een kwetsbaarheid binnen de organisatie kunnen activeren (door misbruik of ongeluk) om zo een gevolg uit te lokken.

- identificatie van alle potentiële bedreigingen:
  - oplijsten van de bedreigingen middels hoger model en gehanteerde definitie, waarbij de bedreiging wordt gedocumenteerd
  - aan elke bedreiging wordt een ID-nummer toegekend

Rollen	Werkwijze	Middelen
〉 coördinator 〉 proces-eigenaar 〉 systeem-eigenaar 〉 CISO/ISO 〉 DPO/PO	〉 per betrokken zakelijk proces en zijn aanverwante informatie verwerkende systemen, oplijsten van de mogelijke bedreigingen 〉 per bedreiging een korte beschrijving geven van de bedreiging 〉 geef iedere bedreiging een ID-nr.	〉 workshop 〉 sjabloon rapport risicoanalyse

Resultaat
〉 een oplijsting van mogelijke relevante bedreigingen, met een beschrijving van de bedreiging en zijn impact 〉 dit wordt binnen het rapport van de risicoanalyse genoteerd

Risico-analyse

Per bedreiging wordt op een 5-puntenschaal aangegeven hoe groot de invloed ervan is op de werking van het informatiesysteem (**het gevolg**), en wat de **waarschijnlijkheid** is op het optreden van de betreffende bedreiging. Op basis van een standaard tabel wordt bepaald wat het totale effect is van de bedreiging, namelijk de wiskundige formule waarschijnlijkheid vermenigvuldigd met gevolg.

- risico-analyse
  - per geïdentificeerde bedreiging, inschatten van de **waarschijnlijkheid (1-5)** dat deze zich zal kunnen voordoen, alsook verder het inschatten van het **gevolg (1-5)** van de bedreiging
  - bepalen van de maturiteit van de reeds genomen controlemaatregelen
  - bepalen van de **risicoscore (1-25)** = waarschijnlijkheid x gevolg per bedreiging
  - overbrengen van de risicoscore van elke bedreiging in een **risicokaart** (gebruik het ID-nummer)
  - bepalen van de **risico-prioriteit** van elke bedreiging

Rollen	Werkwijze	Middelen
〉 coördinator 〉 proces-eigenaar 〉 systeem-eigenaar 〉 CISO/ISO 〉 DPO/PO	〉 bepaal per geïdentificeerde bedreiging zijn waarschijnlijkheid dat deze **inherente** bedreiging zich zal kunnen manifesteren, middels de tabel “waarschijnlijkheid” 〉 bepaal per geïdentificeerde bedreiging de impact die deze **inherente** bedreiging zal hebben op de organisatie, middels de tabel “impact” 〉 bepaal de maturiteit van de reeds genomen controlemaatregelen, en som ze op 〉 bereken de score van het huidige risiconiveau 〉 rangschik de bedreigingen volgens prioriteit (hoog naar laag) 〉 breng de bedreigingen over op een risicokaart(facultatief)	〉 workshop 〉 sjabloon rapport risicoanalyse

Resultaat
〉 een gerangschikte lijst van bedreigingen, met een inschatting van hun waarschijnlijkheid van optreden en hun impact op de organisatie. De lijst is gerangschikt naar de ernst van het berekende risico, en houdt rekening met genomen controlemaatregelen 〉 dit wordt binnen het rapport van de risicoanalyse genoteerd

Waarschijnlijkheid

De analyse van de waarschijnlijkheid van elke geïdentificeerde bedreiging gebeurt aan de hand van de volgende schalen (1 – 5) zoals gedefinieerd in het document ‘Vo informatieclassificatie – Minimale maatregelen – Risicoanalyse’.

waarschijnlijkheid	Score	Rating	Kans	Horizon
	5	Voorzienbaar	> 90%	1x/maand of >
	4	Hoog	< 90%	1x/kwartaal
	3	Gemiddeld	< 60%	1x/jaar

	2	Laag	< 30%	1 - 5 jaar
	1	Zeer laag	< 10%	> 5 jaar

Voor de beoordeling van de waarschijnlijkheid dat een bepaald risico optreedt, kan men kijken naar:

- Het verleden: Heeft de bedreiging zich al voorgedaan?
- De vertrouwdheid: Hebben we de activiteiten al eerder gedaan?
- De omstandigheden: Onder welke condities treedt het op?
- De frequentie: Hoe vaak kan het voorkomen?
- De risicogevoeligheid in tijd: Is er sprake van een stijging of een daling?

Elke bedreiging is een omstandigheid die een kwetsbaarheid binnen de organisatie kan activeren om zo een gevolg uit te lokken. Deze kwetsbaarheid heeft een gevolg op de kansberekening van elke bedreiging, immers, hoe hoger de kwetsbaarheid, hoe hoger de kans dat een dreiging zich voordoet. Zoals hoger gesteld heeft de maturiteit van de genomen controlemaatregelen invloed op de kwetsbaarheid: hoe lager de maturiteit, hoe hoger de kwetsbaarheid.

Hierbij moet men dus rekening houden met reeds bestaande maatregelen die de waarschijnlijkheid van de bedreigingen verminderen. (zie definitie “huidig risico niveau”). Zoals hoger bepaald onder hoofdstuk “Risicoanalyse”, hebben we zicht op de maturiteit van een maatregel. Door de kwetsbaarheid af te wegen tegenover de maturiteit van de bestaande maatregel kan men tot een juiste inschatting van de waarschijnlijkheid komen.

Impact

Er zijn verschillende impactcategorieën te onderscheiden (1 – 5) zoals gedefinieerd in het document ‘Vo informatieclassificatie – Minimale maatregelen – Risicoanalyse’. Per risicoanalyse moet worden bepaald welke van deze categorieën van toepassing zijn. Hierbij houden we rekening met impact op verschillende vlakken: financieel, juridisch, naar dienstverlening belanghebbenden en naar imago.

Score	Rating	Financiële impact	dienstverlening	Imago	belanghebbenden	rechtelijk
5	Kritiek	Impact op budget > 20%	Bijsturing van de criteria en/of maatregelen zijn dwingend en noodzakelijk om het voortbestaan van de dienstverlening te garanderen. Reservering van financiële middelen is noodzakelijk en overstijgen lopende en toekomstige budgetten. Bedreigend voor het voortbestaan van de organisatie. Onderbreking met een onbepaalde duur, of permanente onbeschikbaarheid van	continue berichtgeving op radio, TV & kranten, sociale media (creatie van een "schandaalsfeer")	Beëindigen financiële autonomie Compensatie onmogelijk Fysieke integriteit Marteling en mishandeling met, al dan niet, blijvende fysieke of psychologisch trauma Levensbeëindiging	rechtelijke vervolging

				de dienstverlening is mogelijk			
	4	significant	Impact op budget 15% - 20%	Bijsturing van de criteria en/of maatregelen zijn noodzakelijk op korte termijn, om de dienstverlening te ondersteunen. Reservering van financiële middelen is noodzakelijk en hebben invloed op het lopende en toekomstige werkingsbudgetten. Onderbreking met een maximaal gekende duur van de dienstverlening is mogelijk	gedurende enkele dagen (negatieve) persberichten in de belangrijkste media	Belangrijke financiële schade voor het individu Aantoonbare blijvende impact op levenskwaliteit Compensatie mogelijk op basis van juridische dwangmaatregelen Ernstige immateriële schade voor het individu: Eigenwaarde Reputatie en stigmatisering Gelijkheid Integriteit van de persoon Ongestoord leven Autonomie Fysieke integriteit Verlies aan zelfstandigheid Bewegingsvrijheid	inbreuk van rechtsregels met substantiële gevolgen (bv. boete)
	3	Groot	Impact op budget 10% - 15%	Bijsturing van de criteria en/of maatregelen zijn noodzakelijk om de dienstverlening te ondersteunen. Financiële middelen worden ondersteund door het lopende werkingsbudget. Korte onderbreking van de dienstverlening is mogelijk, binnen VO-breed spreken we tussen ½ en 2 dagen	(negatieve) persberichten her en der	Belangrijke financiële schade voor het individu Geen aantoonbare blijvende impact op de levenskwaliteit Potentiële compensatie mogelijk op basis van juridische dwangmaatregelen Geen tot minimale immateriële schade voor het individu: Eigenwaarde Reputatie en stigmatisering	beperkte inbreuk van een bepaalde regel met lichte gevolgen (bv. aanmaning)

	2	Gemiddeld	Impact op budget 5% - 10%	Bijsturing van de criteria en/of maatregelen zijn aangewezen om de dienstverlening te ondersteunen. Korte onderbreking van de dienstverlening mogelijk. VO-breed spreken we van minder dan ½ dag	enkel interne communicatie & communicatie naar belanghebbenden	Minimale financiële schade voor het individu Geen aantoonbare impact op de levenskwaliteit Potentiële compensatie mogelijk zonder juridische dwangmaatregelen Geen tot minimale immateriële schade voor het individu: Eigenwaarde Reputatie en stigmatisering	beperkte inbreuk van een bepaalde regel zonder enige gevolgen
	1	Klein	Impact op budget < 5%	Geen impact op de organisatie. Dienstverlening gegarandeerd	enkel interne communicatie & communicatie naar belanghebbenden	Geen tot verwaarloosbare financiële schade voor het individu Geen aantoonbare impact op levenskwaliteit Geen tot minimale immateriële schade voor het individu: Eigenwaarde Reputatie en stigmatisering	overtreding van normen en waarden

Risicoscore

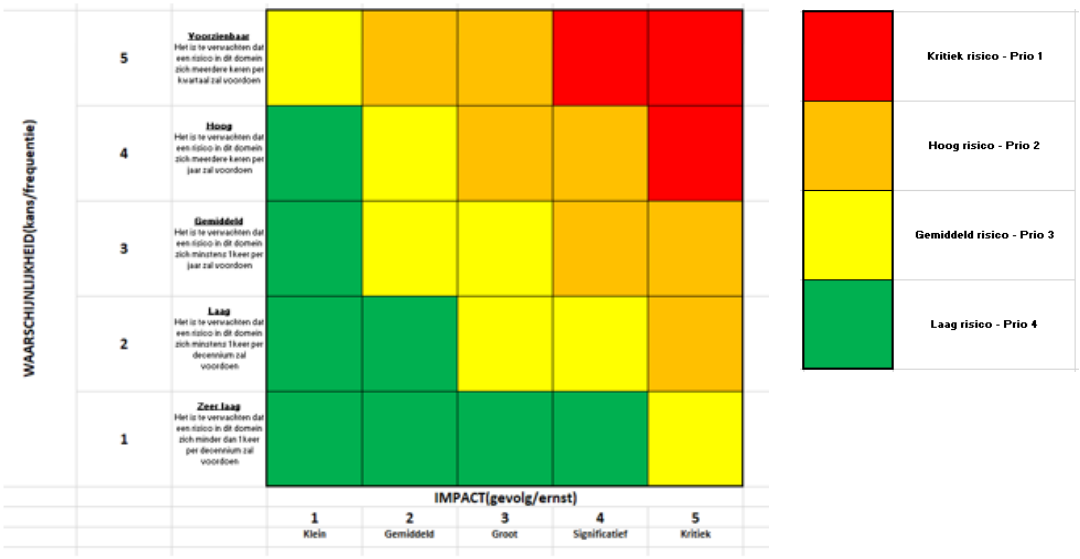
De coördinator van de risicoanalyse werkt de invulling uit, waarbij hij zorgt voor bepaling van het risico volgens de formule **waarschijnlijkheid x impact**. Hierbij wordt er rekening gehouden met de maturiteit van de reeds bestaande controlemaatregelen, waardoor het resultaat van de berekening een inzicht geeft in het huidige risiconiveau.

Risicokaart

Op basis van de berekening van **het risico,** bepaald de coördinator van de risicoanalyse welke bedreigingen het meest ernstig worden geacht.

Bedreigingen waarvan de waarschijnlijkheid en impact in schalen ingedeeld zijn, kunnen geplaatst worden in een risicokaart. De risicokaart geeft dus inzicht in de spreiding van de risico's naar waarschijnlijkheid en impact.

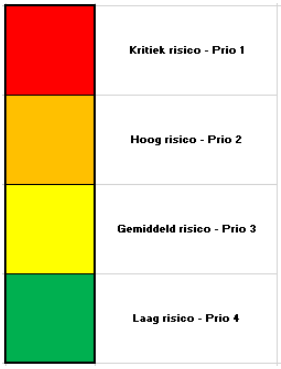
Met behulp van de risicoscore kunnen bedreigingen, middels hun toegekende ID-nummer, uitgezet worden op de volgende risicokaart:



Dit geeft aan zowel het topmanagement, als het lijnmanagement een snel overzicht in de ernst van de geïdentificeerde bedreigingen. Deze stap is niet verplicht binnen de uitvoering van een risicoanalyse volgens de Vo risicoanalyse methodiek.

Risico-prioriteit

Met behulp van de risico-scores kunnen de bedreigingen gerangschikt worden van hoog naar laag, op basis van volgende beoordelingstabel:



Dit laat toe om de risico's te prioriteren zodat de belangrijkste (= met de hoogste risico-score) eerst aangepakt kunnen worden.

Bepalen risicostrategie

Er bestaan vier soorten risicostrategieën: vermijden, mitigeren, overdragen en accepteren die samenhangen met de mate van de waarschijnlijkheid en de impact. Hierbij bepalen de coördinator van de risicoanalyse, de deskundigen, waaronder ook de CISO en de DPO de risicostrategie.

De specifieke activiteiten van een organisatie beïnvloeden de keuze van de strategie. Zo kan het zijn dat een organisatie x een keuze zal maken tot mitigeren van een risico, terwijl organisatie y eerder hetzelfde risico gaat accepteren. Verder hangt de keuze die gemaakt wordt ook af van de afweging ten

aanzien van de geldende maatregelen binnen de Vo informatieclassificatie, bv op basis van de kostprijs om die specifieke maatregel(en) te implementeren.

- bepalen risicostrategie:

Op basis van de beoordeling in prioriteit van het **huidige risiconiveau,** wordt de verdere aanpak (vermijden, mitigeren, overdragen of accepteren) van de bedreiging bepaald:

- De organisatie kiest voor het **mitigeren**, en deze keuze is gebaseerd op de missie, visie en doelstellingen en in kader van dienstverlening.
- Er kan gekozen worden voor **overdragen** van het risico, onder andere door het inschakelen van een ICT-dienstverlener of door het afsluiten van diverse raamcontracten of verzekeringen.
- Een aantal specifieke risico's waarbij de controlemaatregelen veel meer inzet en tijd vergen dan het gunstige effect op het risico worden **geaccepteerd**.
- Risico's die we **vermijden** hebben geen gevolg meer op de missie, visie, doelstellingen en dienstverlening van de organisatie. Dit vraagt wel een aanpassing van de organisatie of haar dienstverlening.

Rollen	Werkwijze	Middelen
〉 coördinator 〉 proces-eigenaar 〉 systeem-eigenaar 〉 CISO/ISO 〉 DPO/PO 〉 topmanagement	〉 bepaal per opgelijste bedreiging, of het huidige risiconiveau geaccepteerd kan worden. Zoniet dan moet het risico gemitigeerd worden – en indien nodig overgedragen of vermeden worden.	〉 workshop 〉 sjabloon rapport risicoanalyse

Resultaat
〉 een oplijsting van mogelijke relevante bedreigingen, waarvan op basis van het huidige risiconiveau bepaald is of het risico geaccepteerd kan worden - Zoniet dan moet het risico gemitigeerd worden – en indien nodig overgedragen of vermeden worden

Risico-evaluatie

In deze stap worden de bijkomende controlemaatregelen bepaald voor de strategie "mitigeren". Hierbij worden de bedreigingen geviseerd met een prio 1 of prio 2. Hierbij zal gekeken worden naar het gewenste risiconiveau, namelijk het risiconiveau na toepassing van alle maatregelen vernoemd binnen het raamwerk informatieclassificatie. Het gewenste risiconiveau vormt als het ware de baseline waarbij een organisatie zich boven deze baseline bevindt, of juist eronder. Indien een organisatie zich onder deze baseline bevindt, zullen bijkomende controlemaatregelen moeten worden getroffen. Het restrisico, na het treffen van deze bijkomende controlemaatregelen, dient al dan niet aanvaard te worden door het topmanagement. Zowel de coördinator van de

risicoanalyse, de deskundigen, waaronder ook CISO en DPO dienen hiervoor aanwezig te zijn. De maatregelen worden daarbij geformuleerd op het niveau van controlemaatregelen om ervoor te zorgen dat bij de invulling over de tijd heen rekening kan worden gehouden met de stand van zaken op dat moment.

Hierbij kunnen de bijkomende controlemaatregelen bestaan uit:

- de maturiteit van een bestaande controlemaatregel die bepaald werd tijdens de activiteit 'het vastleggen van context en scope' verhogen, ofwel
- kiezen voor een andere controlemaatregel.

Concreet:

- risico-evaluatie:
  - bepalen van de positie van de organisatie ten aanzien van het gewenste risiconiveau. Dit voor bedreigingen die gemitigeerd dienen te worden, dit met name voor de bedreigingen die ingeschaald zijn met een prio 1 of een prio 2. - Het gewenste risiconiveau vormt de baseline, waarbij alle controlemaatregelen zijn getroffen zoals bepaald binnen het raamwerk informatieclassificatie
  - bepalen of de bestaande controlemaatregelen in maturiteit kunnen verhoogd worden, of er gekozen dient te worden voor andere controlemaatregelen
  - bepaal opnieuw de waarschijnlijkheid en de impact na het nemen van deze bijkomende controlemaatregelen, en bereken de risicoscore(=restrisico)
  - topmanagement beslist of het restrisico, en zijn bijhorende controlemaatregelen, al dan niet aanvaard worden

Rollen	Werkwijze	Middelen
- coördinator - proces-eigenaar - systeem-eigenaar - CISO/ISO - DPO/PO - topmanagement	- bepalen van de positie van de organisatie ten aanzien van het gewenste risiconiveau. Dit voor bedreigingen die gemitigeerd dienen te worden, dit met name voor de bedreigingen die ingeschaald zijn met een prio 1 of een prio 2. - Het gewenste risiconiveau vormt de baseline, waarbij alle controlemaatregelen zijn getroffen zoals bepaald binnen het raamwerk informatieclassificatie - bepalen of de bestaande controlemaatregelen in maturiteit kunnen	- workshop - sjabloon rapport risicoanalyse

	verhoogd worden, of er gekozen dient te worden voor andere controlemaatregelen 〉 bepaal opnieuw de waarschijnlijkheid en de impact na het nemen van deze bijkomende controlemaatregelen, en bereken de risicoscore(=restrisico) 〉 topmanagement beslist of het restrisico, en zijn bijhorende controlemaatregelen, al dan niet aanvaard worden	

Resultaat
〉 een oplijsting van mogelijke relevante bedreigingen, dewelke dienen gemitigeerd worden, waarbij de bijkomende controlemaatregelen zijn gedefinieerd. Het topmanagement beoordeelt en aanvaardt het restrisico

Welke risico's te beheersen?

Welke bedreigingen aanvaardbaar zijn, en wat er dient te gebeuren, verschilt voor iedere organisatie. Onderstaande tabel geeft een indicatie van de risico-appetijt.

Risico-appetijt	
Kleurencode	**Omschrijving**
Kritiek risico	Risico is niet aanvaardbaar, controlemaatregelen zijn nodig verhogen maturiteit en/of bepalen nieuwe maatregelen conform informatiebeveiligingsnormen
Hoog risico	Risico is niet aanvaardbaar, controlemaatregelen zijn nodig verhogen maturiteit en/of bepalen nieuwe maatregelen conform informatiebeveiligingsnormen
Gemiddeld risico	Risico verdient extra aandacht tot verdere beheersing verhogen maturiteit en/of bepalen nieuwe maatregelen conform informatiebeveiligingsnormen
Laag risico	Aanvaardbaar risico, extra controlemaatregelen nemen is mogelijk verhogen maturiteit en/of bepalen nieuwe maatregelen conform informatiebeveiligingsnormen

Risico-evaluatie

Er zijn twee manieren om bedreigingen die niet aanvaardbaar zijn, te beheersen: ofwel verhoogt men de maturiteit van de bestaande maatregelen, ofwel identificeert men bijkomende controlemaatregelen.

Het restrisico wordt bepaald door het ingeschatte niveau van waarschijnlijkheid en impact te herbekijken. Dit doet men op basis van de opnieuw ingeschatte maturiteit van bestaande controlemaatregelen of de nieuwe controlemaatregel.

Het restrisico wordt gevormd door opnieuw de waarschijnlijkheid te vermenigvuldigen met de impact.

De beoordeling van het restrisico, in aanvaarding, ligt hierbij in de handen van het topmanagement.

2.5. Risicobehandeling

De in de vorige stap gekozen risicostrategie moet ook daadwerkelijk geïmplementeerd worden in de organisatie. Bovendien dienen afspraken gemaakt te worden over de controle op de uitvoering van de risicostrategie. Voor bedreigingen die niet, of niet volledig worden beheerst, is het mogelijk een financiële buffer aan te leggen.

De risicobehandeling wordt besproken tussen de coördinator van de risicoanalyse, de deskundigen, de CISO en de DPO.

Voor elke actie wordt vastgelegd wat er gedaan moet worden, tegen wanneer en wie verantwoordelijk is voor deze actie. Hiervoor wordt een **actieplan** opgemaakt. Eventueel wordt ook opgenomen hoe dit kan gemeten worden. Indien de organisatie beschikt over een informatieveiligheidsplan, moeten deze acties hierin worden opgenomen. Ook de nodige budgetten moeten worden voorzien om de gedefinieerde acties daadwerkelijk uit te voeren.

Opvolgen geformuleerde acties

Het actieplan moet ervoor zorgen dat de risico's voldoende beheerst worden. De mate van risicobeheersing van alle geïdentificeerde risico's is bepalend voor de maturiteit van de organisatie of van een proces binnen de organisatie.

Het is dus belangrijk om het actieplan op te volgen: voor elke uitgevoerde actie moet men zich de vraag stellen of het doel van de actie bereikt is.

Zelfs een aangepakt risico kan nog een rest van waarschijnlijkheid en / of impact in zich houden. Niet alle controlemaatregelen leiden immers tot een waarschijnlijkheid van (bijna) nul en/of een impact van (bijna) nul en er blijft vaak een restrisico over. Het topmanagement beoordeelt dit restrisico opnieuw en aanvaardt het.

BIJLAGE A – OVERZICHT METHODIEKSTAPPEN

〉 Analyse van de zakelijke omgeving

〉 vaststellen context

Rollen	Werkwijze	Middelen
〉 coördinator 〉 proces-eigenaar 〉 systeem-eigenaar	〉 nagaan welke categorieën gegevens verwerkt worden 〉 nagaan om welke reden deze gegevens verwerkt worden, waarbij de doelstelling van de verwerking gedocumenteerd wordt 〉 omschrijven van de context van de risicoanalyse	〉 interview met applicatie-eigenaar, workshop 〉 sjabloon rapport risicoanalyse

Resultaat
〉 een omschrijving van de context tot de gevraagde risicoanalyse, met een inzicht in de betrokken categorieën gegevens die verwerkt wordt
〉 dit wordt binnen het rapport van de risicoanalyse genoteerd

〉 vaststellen scope

Rollen	Werkwijze	Middelen
〉 coördinator 〉 proces-eigenaar 〉 systeem-eigenaar	〉 oplijsten van de betrokken zakelijke processen binnen de scope van de risicoanalyse; 〉 oplijsten van de informatieverwerkende systemen die de betrokken zakelijke processen ondersteunen 〉 oplijsten van de informatie die in de betrokken zakelijke processen verwerkt wordt 〉 deze gegevens aftoetsen aan het Vo informatieclassificatie model, nl. bepalen tot welke classificatieschaal deze gegevens behoren 〉 de maturiteit bepalen van de reeds genomen controlemaatregelen, binnen het Vo informatieclassificatiemodel bepalen	〉 workshop 〉 sjabloon rapport risicoanalyse

Resultaat
〉 een overzicht van de betrokken zakelijke processen, de gerelateerde betrokken systemen, categorisatie en specificatie van de informatie, classificatieschaal en een maturiteitsoverzicht van de bestaande controlemaatregelen
〉 dit wordt opgenomen binnen het rapport van de risicoanalyse

Risicobeoordeling

〉 risico-identificatie

Rollen	Werkwijze	Middelen
〉 coördinator 〉 proces-eigenaar 〉 systeem-eigenaar 〉 CISO/ISO 〉 DPO/PO	〉 per betrokken zakelijk proces en zijn aanverwante informatie verwerkende systemen, oplijsten van de mogelijke bedreigingen 〉 per bedreiging een korte beschrijving geven van de bedreiging 〉 geef iedere bedreiging een ID-nr.	〉 workshop 〉 sjabloon rapport risicoanalyse

Resultaat
〉 een oplijsting van mogelijke relevante bedreigingen, met een beschrijving van de bedreiging en zijn impact 〉 dit wordt binnen het rapport van de risicoanalyse genoteerd

〉 risicoanalyse

Rollen	Werkwijze	Middelen
〉 coördinator 〉 proces-eigenaar 〉 systeem-eigenaar 〉 CISO/ISO 〉 DPO/PO	〉 bepaal per geïdentificeerde bedreiging zijn waarschijnlijkheid dat deze **inherente** bedreiging zich zal kunnen manifesteren, middels de tabel “waarschijnlijkheid” 〉 bepaal per geïdentificeerde bedreiging de impact die deze **inherente** bedreiging zal hebben op de organisatie, middels de tabel “impact” 〉 bepaal de maturiteit van de reeds genomen controlemaatregelen, en som ze op 〉 bereken de score van het huidige risiconiveau 〉 rangschik de bedreigingen volgens prioriteit (hoog naar laag) 〉 breng de bedreigingen over op een risicokaart(facultatief)	〉 workshop 〉 sjabloon rapport risicoanalyse

Resultaat
〉 een gerangschikte lijst van bedreigingen, met een inschatting van hun waarschijnlijkheid van optreden en hun impact op de organisatie. De lijst is gerangschikt naar de ernst van het berekende risico, en houdt rekening houdende met genomen controlemaatregelen 〉 dit wordt binnen het rapport van de risicoanalyse genoteerd

〉 risico-strategie

Rollen	Werkwijze	Middelen
〉 coördinator 〉 proces-eigenaar 〉 systeem-eigenaar 〉 CISO/ISO 〉 DPO/PO 〉 topmanagement	〉 bepaal per opgelijste bedreiging, of het huidige risiconiveau een risico is dat geaccepteerd kan worden. Zoniet dan moet het risico gemitigeerd worden – en indien nodig overgedragen of vermeden worden	〉 workshop 〉 sjabloon rapport risicoanalyse

Resultaat
〉 een oplijsting van mogelijke relevante bedreigingen, waarvan op basis van het huidige risiconiveau bepaald is of het risico geaccepteerd kan worden - Zoniet dan moet het risico gemitigeerd worden – en indien nodig overgedragen of vermeden worden

〉 risico-evaluatie

Rollen	Werkwijze	Middelen
〉 coördinator 〉 proces-eigenaar 〉 systeem-eigenaar 〉 CISO/ISO 〉 DPO/PO 〉 topmanagement	〉 bepalen van de positie van de organisatie ten aanzien van het gewenste risiconiveau. Dit voor bedreigingen die gemitigeerd dienen te worden, dit met name voor de bedreigingen die ingeschaald zijn met een prio 1 of een prio 2. - Het gewenste risiconiveau vormt de baseline, waarbij alle controlemaatregelen zijn getroffen zoals bepaald binnen	〉 workshop 〉 sjabloon rapport risicoanalyse

	het raamwerk informatieclassificatie 〉 bepalen of de bestaande controlemaatregelen in maturiteit kunnen verhoogd worden, of er gekozen dient te worden voor andere controlemaatregelen 〉 bepaal opnieuw de waarschijnlijkheid en de impact na het nemen van deze bijkomende controlemaatregelen, en bereken de risicoscore(=restrisico) 〉 topmanagement beslist of het restrisico, en zijn bijhorende controlemaatregelen, al dan niet aanvaard worden	
Resultaat		
〉 een oplijsting van mogelijke relevante bedreigingen, dewelke dienen gemitigeerd worden, waarbij de bijkomende controlemaatregelen zijn gedefinieerd. Het topmanagement zal het restrisico beoordelen en al dan niet aanvaarden.		

〉 Risicobehandeling
〉 Communicatie en -overleg
〉 Monitoring en beoordeling