Informatieclassificatie Vlaamse overheid (Vo-ICR)

Risicobeheer

Minimale maatregelen

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 kwaliteitseisen van de minimale maatregelen die moeten afgedwongen worden in het kader van de deelprocessen beheer van incidenten. Deze kwaliteitseisen worden verbonden aan de informatieklassen zoals deze zijn beschreven in het ICR van de Vo.

Werkprincipe van het document

Het huidige document bestaat uit 4 delen. Eerst worden de minimale maatregelen besproken alvorens in het 2e deel al de nodige aanvullende informatie ter beschikking wordt gesteld. Vervolgens bespreken we de link met andere maatregelen. Het document wordt afgerond met de prestatie indicatoren.

De organisatie van de maatregelen in het kader van informatieclassificatie wordt beschreven in het document 'Vo informatieclassificatie – Organisatie - Informatieclassificatieraamwerk'.

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	4 maart 2020	Guy KLERKX	Draft
v.0.2	19 maart 2020	Kristel VAN AKEN	Feedback
v.0.3	26 maart 2020	Guy KLERKX	Feedback Johan Smekens en Beau Janssens verwerkt inzake: -aanpassing risicokaart -aanpassing risico-evaluatie -bepalen risico-strategie
v.0.4	26 maart 2020	Kristel VAN AKEN	Feedback Johan Smekens en Beau Janssens verwerkt + hoofdstukken link met andere beheerprocessen en succesfactoren.
v.0.5	31 Maart 2020	Johan SMEKENS	Feedback (Minor)
v.1.0	29 oktober 2020	Beau JANSSEN	Update voor kwaliteitskenmerk Integriteit
v.1.1	10 augustus 2021	Beau JANSSEN	Update voor kwaliteitskenmerk Beschikbaarheid
v.2.0	22 juli 2022	Kristel VAN AKEN	Verbeteren leesbaarheid Geen inhoudelijke wijzigingen
V.2.1	17 oktober 2023	Nele Lowet	Update KSZ

Bronnen en verwijzingen

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

Documentverwijzingen:

- *Vo Informatieclassificatie – Organisatie Informatieveiligheid* (PDF)
- *Vo Informatieclassificatie – Organisatie Informatieclassificatieraamwerk* (PDF)
- Vo Informatieclassificatie – Minimale maatregelen – (PDF):
  - *Vo Informatieclassificatie - Minimale maatregelen - asset en configuratiebeheer*
  - *Vo Informatieclassificatie - Minimale maatregelen - beheer gebeurtenissen*
  - *Vo Informatieclassificatie - Minimale maatregelen - probleembeheer*
  - *Vo Informatieclassificatie - Minimale maatregelen - release en deployment beheer*
  - *Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer*
- Vo Informatieclassificatie – Overzicht baseline maatregelen (XLS)

De laatste versies van deze documenten zijn te raadplegen op vlaanderen.be.

Inhoudsopgave

INLEIDING

Het proces risicobeheer

Begrippenkader

Risicobeheer is echter 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 eruitziet, de methodiek en welk instrumentarium kan aangewend worden.

Het proces risicobeheerproces omvat de systematische aanpak om risico's te identificeren, analyseren, evalueren, behandelen en monitoren, maar ook de consultatie en communicatie gedurende dat proces.

Scope, doelgroep en voordelen

Het proces risicobeheer is bedoeld voor alle typen organisaties binnen de Vlaamse overheid, ongeacht grootte en aard van de activiteiten, en is vooral gericht op organisatie-breed risicobeheer.

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 erop toe moeten zien dat een organisatie haar risico's goed beheert of de aanpak daarvan moet beoordelen.

De voordelen van toepassing van risicobeheer zijn velerlei, bijvoorbeeld het verbeteren van de c*orporate governance* en daarmee van vertrouwen dat stakeholders in de organisatie hebben. De grotere weerstand tegen bedreigingen. Beter inzicht in de kansen voor ontwikkeling en groei. Maar ook goede besluitvorming, naleving van wet- en regelgeving, het voorkomen van calamiteiten en *business continuity*.

Het proces

In het hart van het proces risicobeheer zitten de bekende stappen van het identificeren, analyseren en evalueren van risico's verbonden aan proces, product, project of organisatie als geheel. Dit kan dus gebeuren nadat er een analyse is gebeurd op zakelijke omgeving, waarbij de scope en context zal bepaald worden, en waarbij een validatie is gebeurd naar de minimale maatregelen informatieclassificatie. Die stappen vormen tezamen de risicobeoordeling. Die beoordeling kan alleen goed worden uitgevoerd als de context en scope zijn bepaald. Die context wordt ten dele ontleend aan het hogervermelde raamwerk.

Op basis van de beoordeling wordt besloten of en zo ja hoe het risico wordt 'behandeld'. Dat kan variëren van het volledig vermijden van het risico door de activiteit waarmee het risico verbonden is te beëindigen, via het beïnvloeden van waarschijnlijkheid op optreden of effect ervan tot en met het accepteren van het risico zonder verdere aanpassingen. Dit houdt in dat bepaalde controlemaatregelen zullen getroffen worden om het risico te behandelen. Vervolgens is monitoring en beoordeling van de ontstane situatie belangrijk om na te gaan of toegepaste beheersmaatregelen effectief zijn of dat de context verandert waardoor de bepaalde risico's anders moeten worden gewaardeerd en aangebrachte controlemaatregelen moeten worden aangepast. De activiteiten 'communicatie en overleg' zorgen ervoor dat de resultaten van specifieke risicobeheerprocessen worden gerapporteerd en geconsolideerd naar het gewenste niveau van de organisatie.

Risicobeheer in het kader van informatieclassificatie

De definities van 'beschikbaarheid, 'vertrouwelijkheid' en 'integriteit' zijn al gegeven binnen het document "Vo Informatieclassificatie – Organisatie - Informatieclassificatieraamwerk".

Een programma voor informatiebeveiliging kan diverse grote en kleine doelen nastreven, maar de belangrijkste principes in een informatiebeveiligingsprogramma zijn te herleiden naar beschikbaarheid, integriteit en vertrouwelijkheid. De controlemaatregelen die op grond van deze basisprincipes gesteld worden, variëren per organisatie. Dit komt doordat elke organisatie haar eigen specifieke eisenpakket opstelt op basis van bedrijfs- en beveiligingsdoelen- en eisen.

Met behulp van het proces risicobeheer wordt binnen de Vlaamse overheid een kader gegeven om te kunnen streven naar een uniformiteit tot het bepalen van maatregelen.

Alle beveiligingsmaatregelen worden geïmplementeerd om een of meer van deze BIV-principes in te vullen. Alle dreigingen worden beoordeeld op hun potentie om één of meer van de principes rond beschikbaarheid, integriteit en vertrouwelijkheid 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 op te lossen.

Beveiligingsconcepten

Organisaties en hun informatiesystemen en netwerken worden blootgesteld aan beveiligingsdreigingen van zeer uiteenlopende aard. Voorbeelden zijn computer gerelateerde fraude, spionage, sabotage, vandalisme, brand en overstroming. Oorzaken van schade zoals kwaadaardige code, hacking en *Denial-of-Service*-aanvallen komen vaker voor, zijn ambitieuzer en worden steeds geavanceerder.

Voordat we starten met het vaststellen van een beveiligingsstrategie, moeten we weten wat we beveiligen en tegen welke dreigingen we beveiligen. De methode die we gebruiken om dit inzicht te krijgen noemen we risicoanalyse.

Beveiligingsmaatregelen worden vastgesteld op basis van een methodisch onderzoek gebaseerd op de risico's die een organisatie loopt. De genomen beveiligingsmaatregelen moeten in harmonie zijn met de risico's die een organisatie loopt en de schade die een bedreiging aan de organisatie toe kan brengen. De resultaten van een risicoanalyse helpen het management bij het stellen van prioriteiten en het nemen van de juiste acties en beslissingen voor het managen van de informatiebeveiligingsrisico's. Het helpt hen bij de juiste keuzes bij het implementeren van beveiligingsmaatregelen om die risico's te beheersen.

Risicobeoordelingen moeten regelmatig worden herhaald om wijzigingen in werkwijze systemen en ook wijzigingen in interne en externe dreigingen te kunnen vaststellen, en daarop indien nodig de beveiligingsmaatregelen aan te passen.

1. MINIMALE MAATREGELEN

1.1. Minimale algemene maatregelen

Vertrouwelijkheid

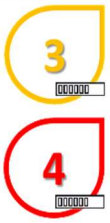
IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Analyse van de zakelijke omgeving; 〉 Toepassen van de minimale maatregelen volgens Vo informatieclassificatie raamwerk; 〉 Validatie: maturiteit bepalen van de minimale maatregelen.
 	Klasse 3 en Klasse 4 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Risico identificatie met alle stakeholders inclusief CISO; 〉 Risicoanalyse met alle stakeholders inclusief CISO; 〉 Risico evaluatie waarbij minimaal het huidig risiconiveau, het gewenste risiconiveau en het restrisico bepaald wordt; 〉 Formele aanvaarding van het restrisico door topmanagement; 〉 Risicostrategie bepalen: risico's worden gemitigeerd, geaccepteerd, vermeden of overgedragen; 〉 Risico behandelen volgens gekozen risicostrategie met rapportering aan het topmanagement en aan CISO; 〉 Communicatie en overleg met alle stakeholders; 〉 Opvolgen implementatie risicostrategie; 〉 Beoordelen risicostrategie met rapportering aan topmanagement en aan CISO.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 / Klasse 4 + 〉 Risicostrategie bepalen: mitigeren, accepteren of vermijden (overdragen is niet toegestaan voor klasse 5)

Integriteit

IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Analyse van de zakelijke omgeving; 〉 Toepassen van de minimale maatregelen volgens Vo informatieclassificatie raamwerk; 〉 Validatie: maturiteit bepalen van de minimale maatregelen.
 	Klasse 3 en Klasse 4 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Risico identificatie met alle stakeholders inclusief CISO; 〉 Risicoanalyse met alle stakeholders inclusief CISO; 〉 Risico evaluatie waarbij minimaal het huidig risiconiveau, het gewenste risiconiveau en het rest risico bepaald wordt; 〉 Formele aanvaarding van het rest risico door topmanagement; 〉 Risicostrategie bepalen: risico's worden gemitigeerd, geaccepteerd, vermeden of overgedragen; 〉 Risico behandelen volgens gekozen risicostrategie met rapportering aan het topmanagement en aan CISO; 〉 Communicatie en overleg met alle stakeholders; 〉 Opvolgen implementatie risicostrategie; 〉 Beoordelen risicostrategie met rapportering aan topmanagement en aan CISO.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 / Klasse 4 + 〉 Risicostrategie bepalen: mitigeren, accepteren of vermijden (overdragen is niet toegestaan voor klasse 5).

Beschikbaarheid

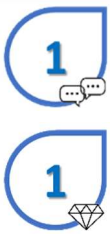
IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: 〉 Analyse van de zakelijke omgeving; 〉 Toepassen van de minimale maatregelen volgens Vo informatieclassificatie raamwerk; 〉 Validatie: maturiteit bepalen van de minimale maatregelen.

	Klasse 3 en Klasse 4 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Beschikbaarheid proces beheer van risico's (10ux5dagen); 〉 Risico identificatie met alle stakeholders inclusief CISO; 〉 Risicoanalyse met alle stakeholders inclusief CISO; 〉 Risico evaluatie waarbij minimaal het huidig risiconiveau, het gewenste risiconiveau en het rest risico bepaald wordt; 〉 Formele aanvaarding van het rest risico door topmanagement; 〉 Risicostrategie bepalen: risico's worden gemitigeerd, geaccepteerd, vermeden of overgedragen; 〉 Risico behandelen volgens gekozen risicostrategie met rapportering aan het topmanagement en aan CISO; 〉 Communicatie en overleg met alle stakeholders; 〉 Opvolgen implementatie risicostrategie; 〉 Beoordelen risicostrategie met rapportering aan topmanagement en aan CISO.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 / Klasse 4 + 〉 Risicostrategie bepalen: mitigeren, accepteren of vermijden (overdragen is niet toegestaan voor klasse 5).

1.2. Minimale specifieke (GDPR) maatregelen

De minimale algemene maatregelen voor risicobeheer moeten toegepast worden: per klasse zijn de overeenkomende maatregelen van toepassing (zie hoofdstuk 'minimale algemene maatregelen').

Vertrouwelijkheid en integriteit

IC klasse	Minimale maatregelen
	Er zijn geen GDPR specifieke maatregelen voor klasse 1.
	GDPR specifieke maatregelen voor Klasse 2: 〉 Geen maatregelen maar ter herinnering: jaarlijks moet een revaluatie uitgevoerd worden van de informatieklasse en waar nodig bijgestuurd.

	Klasse 3 en Klasse 4 kennen dezelfde maatregelen: Alle maatregelen van Klasse 2 + 〉 Risico identificatie met alle stakeholders inclusief CISO en DPO; 〉 Risicoanalyse met alle stakeholders inclusief CISO en DPO; 〉 Risicobehandeling volgens gekozen risicostrategie met rapportering aan het topmanagement en aan CISO en DPO; 〉 Beoordelen risicostrategie met rapportering aan topmanagement en aan CISO en DPO.
	Er zijn geen GDPR maatregelen voor klasse 5.

Beschikbaarheid

Er zijn geen GDPR specifieke maatregelen gedefinieerd in het kader van beschikbaarheid.

1.3. Minimale specifieke (NIS II) maatregelen

In afwachting van de goedkeuringen omtrent NISII is er in dit document alvast de nodige ruimte voorzien voor toekomstige minimale specifieke NISII maatregelen.

1.4. Minimale specifieke (KSZ) maatregelen

Volgens de Minimale Normen van de Kruispuntbank Sociale Zekerheid moeten volgende maatregelen in het kader van risicobeheer toegepast worden:

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: 〉 De organisatie moet bij elk proces en bij elk project een risico-beoordeling rond informatieveiligheid en privacy uitvoeren, valideren, communiceren en onderhouden (Ref. KSZ 5.2.2 a). 〉 Alle risico-beoordelingen met een hoog residueel risico communiceren naar de directie voor bespreking en beslissing : behandelen of aanvaarden (Ref. KSZ 5.2.2 b). 〉 De richtlijn rond risico-beoordeling toepassen zoals vermeld in bijlage C van de beleidslijn 'Risico-beoordeling' (Ref. KSZ 5.2.2 c): o In de regel beslist de verwerkingsverantwoordelijke vrij over de procedure en methodologie die hij wenst te hanteren bij het inschatten en beheren van risico's, op voorwaarde dat deze beantwoordt aan een aantal minimumkenmerken van betrouwbaarheid en objectiviteit. Zo moet het risicobeheer volgende elementen bevatten: Methodologisch onderbouwd, gestructureerd, op maat, begrijpelijk, voldoende genuanceerd. Met voldoende communicatie, consultatie, beheer en nazicht. 〉 De controlemaatregelen afstemmen op de risico's, waarbij rekening dient te worden gehouden met technische mogelijkheden en de kosten van de te nemen maatregelen (Ref. 5.5.1 f). 〉 Een risico-beoordeling uitvoeren om de gepaste methode te bepalen voor het wissen van een informatiedrager (Ref. KSZ. 5.8.3 c). 〉 Overeenkomsten met derde partijen alle vereisten omvatten om risico's van informatieveiligheid en privacy te behandelen die geassocieerd zijn met ICT diensten (Ref. KSZ 5.12.1 d).

2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1. Beheer van risico's als maatregel

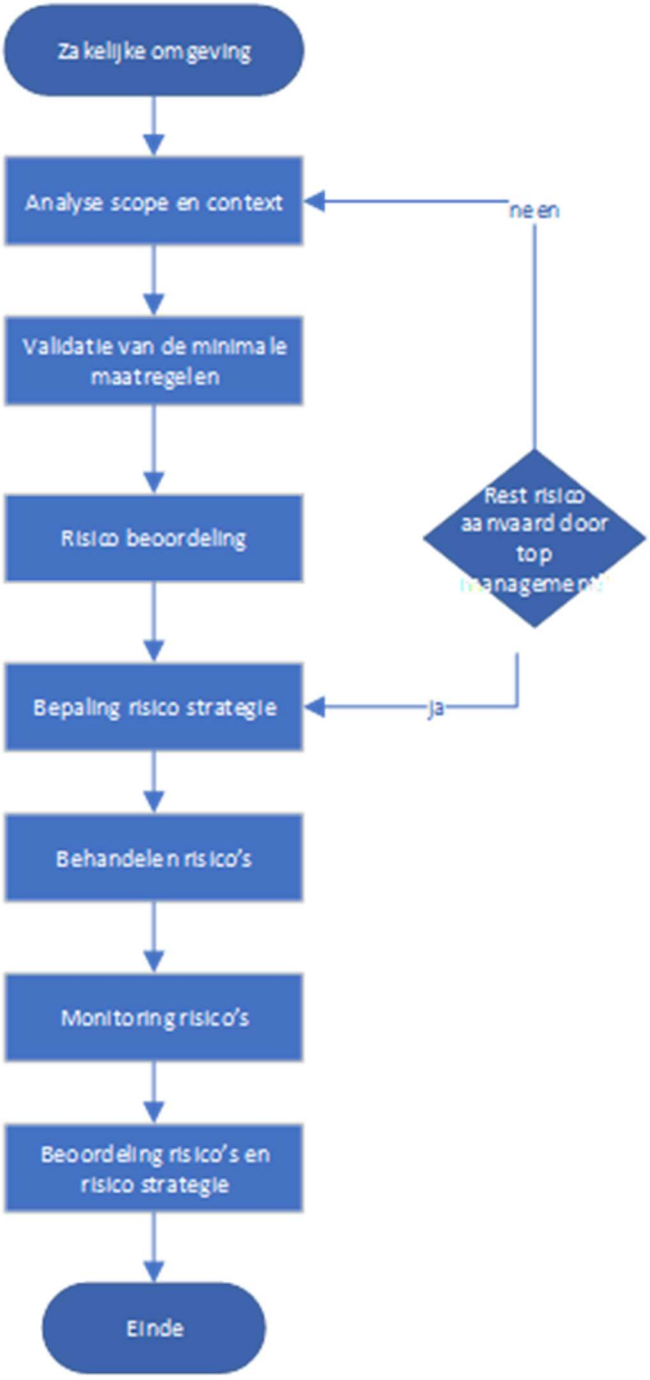
2.1.1. De verschillende activiteiten van risicobeheer

Het proces risicobeheer is het continue proces van bedreigingen in beeld krijgen, kwantificeren en afwegen of en welke controlemaatregelen er genomen moeten worden (zie Figuur 1). Het proces bestaat uit de volgende stappen:

- Analyse van de zakelijke omgeving
  - Vaststellen context en scope
  - Validatie minimale maatregelen IC
- Risicobeoordeling
  - Risico-identificatie
  - Risicoanalyse
  - Risico-evaluatie
  - Bepalen risicostrategie
- Risicobehandeling
  - Vastleggen acties
  - Opvolgen geformuleerde acties
- Communicatie en -overleg
- Monitoring en beoordeling

2.1.2. Het proces

Alle bouwstenen samen maken deel uit van het proces voor het beheer van risico's. Algemeen ziet dat er als volgt uit:



2.1.3. Link met informatiebeveiliging & Privacy

100% beveiliging bestaat niet. Risico's kan men niet 100% uitsluiten. (Informatie)veiligheidsrisico's zijn bijgevolg niet uit te sluiten. Het is dan ook zaak om de (informatie)veiligheidsdienst te betrekken bij de beoordeling van risico's.

In de praktijk betekent dit dat volgende functies deel uitmaken van het risico-team:

- De CISO ingeval het risico gevolgen heeft voor de beveiliging van informatie en informatie verwerkende systemen;
- De DPO ingeval het risico gevolgen heeft voor de bescherming van persoonsgegevens;

Ook als het de bedreiging zelf geen rechtstreekse gevolgen heeft op de beveiliging van informatie en informatie verwerkende systemen, is het mogelijk dat bij de afhandeling van de bedreiging wijzigingen nodig zijn aan de (ICT) infrastructuur. Hierbij moet de impact op de beveiliging steeds in het vizier worden genomen.

2.2. Succesfactoren voor een goed risicobeheer

Om tot een efficiënt en effectief proces risicobeheer te komen, zijn volgende parameters belangrijk. Zij kunnen meegenomen worden als prestatie-indicatoren of KPI's (*Key Performance Indicatoren*) om het succes of falen van het proces te meten en bij te sturen waar nodig:

- **Ondersteuning door topmanagement**: een zichtbare ondersteuning door de leidend ambtenaar of algemeen directeur is nodig, zowel bij de beoordeling van de risico's als de toewijzing van middelen om de risicostrategie uit te voeren. Topmanagement moet betrokken zijn bij de beoordeling van de risico's en het bepalen van de risico appetijt.
- **Allocatie van middelen**: de benodigde resources moeten door het management ter beschikking worden gesteld. Risicobeheer is geen zaak van de DPO of CISO alleen!
- **Risico perceptie**: de resultaten van de risicoanalyse worden me bepaald door de perceptie van de risico's door de deelnemers aan de risicoanalyse, d.w.z. door de wijze waarop de deelnemers de risico's beleven en op waarde schatten. Het is daarom belangrijk de juiste mensen in te schakelen, met voldoende kennis van zake over 'hun' expertise terrein.
- **Reputatie van risicoanalyses**: een risicoanalyse kan als bedreigend worden ervaren, bvb omdat deze oefening aanzien kan worden als kritiek op persoonlijk functioneren van de deelnemers. Dit kan leiden tot onvolledige of onjuiste informatie of inschattingen omdat over bepaalde onderwerpen niets mag worden gevraagd, of bepaalde mensen niet mogen worden geïnterviewd.

2.3. De bouwstenen van risicobeheer

2.3.1. Analyse van de zakelijke omgeving

Vaststellen context en scope

De eerste stap bij het uitvoeren van een risicoanalyse is het bepalen van de context. Hierbij kan men zich richten tot de aanleiding van de risicoanalyse. Met name bij ad hoc gevraagde analyses is het van cruciaal belang dat de aanleiding om juist nu een analyse uit te voeren goed bekend is.

Met de informatie uit deze stap kan de doelstelling van de risicoanalyse worden vastgesteld en kunnen de juiste keuzes worden gemaakt met betrekking tot de inrichting van de risicoanalyse.

Het resultaat van de context- en doelbepaling is om vast te stellen welke informatiesystemen en welke informatiebronnen aangesproken worden, dewelke meegenomen moeten worden in de risicoanalyse.

Validatie minimale maatregelen Informatieclassificatie

Eens bepaald welke informatiesystemen en welke informatiebronnen aangesproken worden, kan er afgeleid worden welke informatie er verwerkt wordt, waarop dan een toetsing kan gebeuren naar de

aanwezige maatregelen dewelke uitgewerkt zijn binnen het model van de Vo informatieclassificatie. De maturiteit van deze maatregelen kunnen vervolgens beoordeeld worden aan de hand van onderstaande tabel.

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

2.3.2. Risicobeoordeling

Op basis van het verkregen inzicht in het te analyseren object en de doelstelling van de risicoanalyse kunnen keuzes gemaakt worden ten aanzien van inrichting van de volgende stappen in het proces rond risicobeheer.

Risicobeoordeling is gebaseerd op de volgende stappen:

- Risico-identificatie
- Risicoanalyse
- Risico-evaluatie
- Bepalen risicostrategie

Risico-identificatie

In deze fase worden alle potentiële bedreigingen geïdentificeerd. Hierbij valt te denken aan een breed scala aan bedreigingen (kwalitatief of kwantitatief), meer bepaald bedreigingen verbonden aan informatiebeveiliging en privacy.

Het doel van risico-identificatie is om inzichtelijk te maken welke bedreigingen een organisatie loopt. Bij de risico-identificatie is het van belang om een brede en gestructureerde benadering te hanteren. Het is een utopie te veronderstellen dat 100% van de risico's in beeld kunnen worden gebracht. Een goede identificatiestructuur kan helpen bij het verkrijgen van een zo volledig mogelijk risicoprofiel. Bij de risico-identificatie is het van belang om een eenduidige definitie van het begrip risico te hanteren. Een risico wordt als volgt gedefinieerd:

"De waarschijnlijkheid op het optreden van een bedreiging met een gevolg op het behalen van de doelstellingen van een organisatie."

Elk geïdentificeerde bedreiging wordt op eenzelfde wijze beschreven:

"Er bestaat een waarschijnlijkheid dat **<beschrijf bedreiging>** veroorzaakt door **<beschrijf oorzaak>** met als gevolg **<beschrijf gevolg>**".

Sommige organisaties vinden het moeilijk om gebeurtenissen, oorzaken en gevolgen te splitsen. Zij hebben vaak baat bij het systematisch opstellen van de hierboven opgenomen schematische weergave, waardoor een heldere en duidelijke omschrijving van het risico ontstaat met aanknopingspunten voor beheersmaatregelen.

Binnen de organisatie wordt gekozen om voornamelijk via brainstormsessies bedreigingen te benoemen en deze te clusteren, o.a. op basis van typologie, zoals:

- Mogelijke invalshoek: juridisch, technisch, organisatorisch, ruimtelijk, financieel, maatschappelijk, politiek (en technieken van projectmethodologie)
- De verschillende types van dreigingen: lichamelijke schade, natuurramp, verlies van essentiële diensten, verstoring veroorzaakt door straling, gecompromitteerde informatie, technisch falen en ongeoorloofde acties. Deze dreigingen kunnen van natuurlijke of menselijke oorsprong zijn en deze kunnen een ongeluk of opzettelijk zijn. (MAPGOOD)

Risicoanalyse

Het in kaart brengen van de bedreigingen maakt het mogelijk om deze te analyseren. De analyse bestaat meestal uit een inschatting van de waarschijnlijkheid dat een gebeurtenis optreedt, waarbij kan worden aangegeven wat de gevolgen daarvan zijn

In de vorige stap uit het proces risicobeheer zijn bedreigingen geïdentificeerd. Resultaat hiervan is een lijst met goed omschreven bedreigingen. Om meer inzicht in de risico's te krijgen, moeten deze bedreigingen geanalyseerd worden.

De risicoscore van een bedreiging wordt bepaald door waarschijnlijkheid en gevolgen in schalen in te delen en deze met elkaar te vermenigvuldigen.

Waarschijnlijkheid

De analyse van de waarschijnlijkheid en de impact van elk geïdentificeerde bedreiging gebeurt aan de hand van de gedefinieerde schalen (1 – 5):

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

Een bedreiging dat 1 keer per 1 jaar voorkomt valt in schaal 3, daarvan is de kans dat deze bedreiging optreedt kleiner dan 60%. De referentiebeelden gelden als hulpmiddel en zullen niet in alle gevallen exact aansluiten bij de werkelijkheid.

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

- Het verleden: Heeft risico zal eerder 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?

Om de subjectiviteit van de inschatting van een bedreiging te beperken is afstemming binnen de organisatie en het onderbouwen van de inschattingen belangrijk. De praktijk leert dat door het plegen van overleg met experts, door een objectieve beoordeling van een buitenstaander en door afstemming binnen een afdelingsoverleg de subjectiviteit enigszins verminderd wordt. Ervaring leert tevens dat medewerkers met logisch redeneren een eind komen met het inschatten van de waarschijnlijkheid van een risico.

Gevolg (of impact)

Zoals in de vorige paragraaf beschreven, zijn verschillende gevolgcategorieën te onderscheiden. Per organisatie kan worden bepaald welke van deze categorieën gebruikt worden. Er kan ook gebruik worden gemaakt van één, niet nader gespecificeerde gevolgschaalindeling waarbij men dus geen onderscheid maakt in de soorten gevolgen. Deze schaalindeling kan praktisch zijn bij een risicoanalyse op hoofdlijnen. Als een meer diepgaande risicoanalyse wordt uitgevoerd wordt beter inzicht in de bedreiging verkregen wanneer men de gevolgen inschat op basis van gevolg categorieën.

Volgende impact schalen worden gehanteerd:

	Score	Rating	Financiële impact	Dienstverlening	Pers	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	Continue berichtgeving op radio, TV en in kranten (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

				en toekomstige budgetten. Bedreigend voor het voortbestaan van de organisatie. Onderbreking met een onbepaalde duur, of permanente onbeschikbaarheid van de dienstverlening is mogelijk			
	4	Significatief	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	Belangrijks financiële schade voor het individu Aantoonbare blijvende impact of 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)

Score	Rating	Financiële impact	Dienstverlening	Pers	Belanghebbenden	Rechtelijk
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	Gemid deld	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. Binnen de 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

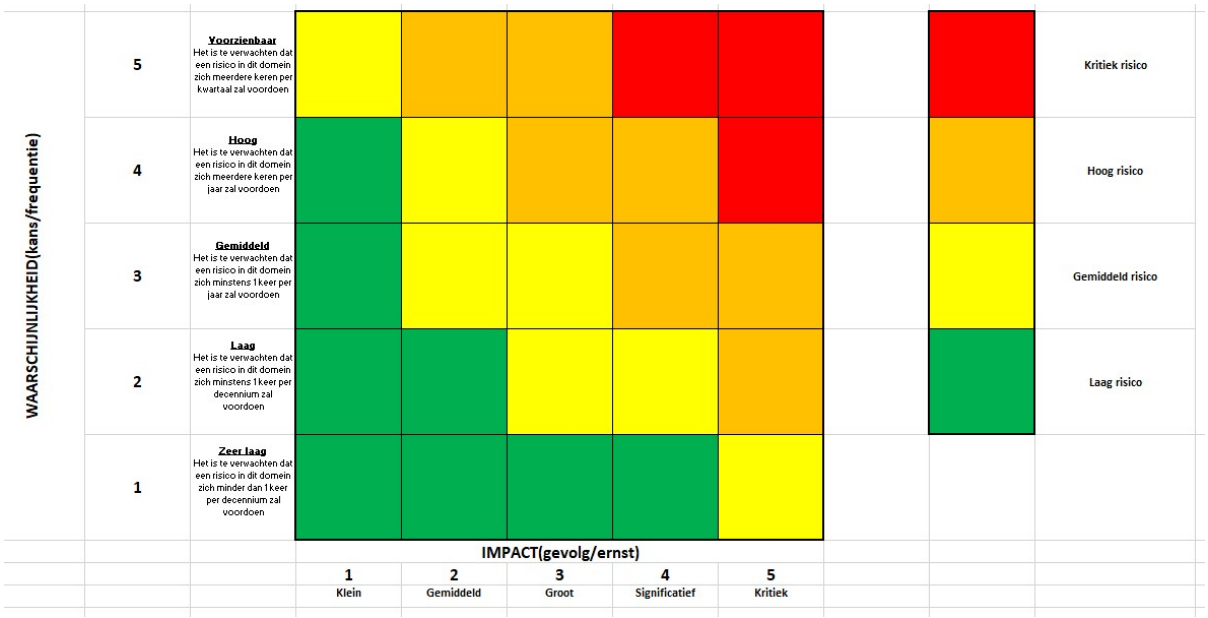
Score	Rating	Financiële impact	Dienstverlening	Pers	Belanghebbenden	Rechtelijk
1	Klein	Impact op budget < 5%	Geen impact op de organisatie. Dienstverlening gegarandeerd	Enkel interne communicatie & communicatie naar belanghebbenden	Geen tot verwaarloosbare financiële schade voor het individu Geen aantoonbare impact op levenskwaliteit Geen tot minimale immateriële schade voor het individu: Eigenwaarde Reputatie en stigmatisering	Overtreding van normen en waarden

Risicoscore

Met behulp van de risicoscore kunnen bedreigingen gerangschikt worden van groot naar klein. De risicoscore wordt bepaald door waarschijnlijkheid en gevolgen van een bedreiging in bovenstaande schalen in te delen en deze schalen te vermenigvuldigen. Dus, risico = waarschijnlijkheid x gevolg.

Risicokaart

Bedreigingen waarvan de waarschijnlijkheid en gevolgen in schalen ingedeeld zijn kunnen geplaatst worden in een risicokaart. De risicokaart geeft inzicht in de spreiding van de risico's naar waarschijnlijkheid en gevolg. De nummers in de risicokaart corresponderen met de aantallen risico's die zich in het desbetreffende vak van de risicokaart bevinden.



Risico-evaluatie

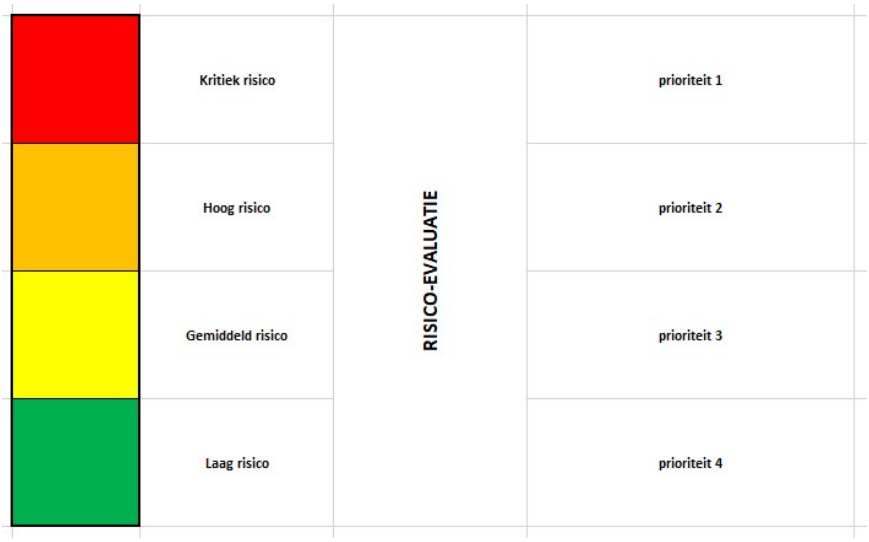
Uiteindelijk gaat risicobeheer over het effectief beheersen van bedreigingen. Als organisatie moet je kunnen aantonen hoe je de belangrijkste bedreigingen beheerst. In de stap risico-evaluatie wordt gekeken welke controlemaatregelen mogelijk zijn en welke het meest geschikt zijn aan de hand van de risicoscore, en aan welke maturiteit deze moet voldoen.

Soorten risico's

- Inherente risico's: het 0-punt ofwel de situatie waarin geen enkele maatregel is getroffen;
- Huidige risiconiveau: het risiconiveau van nu, inclusief de reeds genomen maatregelen;
- Minimaal risiconiveau: het risiconiveau rekening houdend met alle relevante minimale maatregelen van het informatie classificatie raamwerk,
- Gewenst risiconiveau voor de korte termijn: Waar wil de organisatie naartoe op korte termijn?
- Gewenst risiconiveau voor de lange(re) termijn: Welke doelstellingen wil de organisatie nastreven op langere termijn?
- Rest risico: het risico dat overblijft nadat maatregelen genomen zijn of zullen zijn. Dit is het risico dat door het management moet worden aanvaard. De grootte van dit risico hangt af van de organisatie en van de risico 'appetijt' van het management.

Welke risico's te beheersen?

Niet alle risico's uit het risicoprofiel van een organisatie hoeven beheerst te worden. Ook is het niet mogelijk om alle risico's die wel beheerst dienen te worden tegelijkertijd aan te pakken. Om te bepalen welke risico's als eerste beheerst moeten worden, kan gekeken worden naar de waarschijnlijkheid en gevolgen van de verschillende risico's. De hiervoor behandelde risicokaart is hierbij een goed hulpmiddel.



Een risico dat in het groene gebied zit vormt geen direct gevaar voor de continuïteit van de instelling (prio 4). Een risico dat een score heeft die in het geel/oranje gebied zit, vraagt om aandacht (prio 3/ prio 2). Een risico dat een risicoscore heeft die in het rode gebied zit vereist directe aandacht (prio 1) om te voorkomen dat de continuïteit van de instelling wordt bedreigd.

De risico-evaluatie betreft:

- Het inherent risico bepalen door het plaatsen van de geïdentificeerde bedreiging in een risicomatrix als assen de waarschijnlijkheid en de impact
- Het inherent risico geeft aan hoe belangrijk de maturiteit van de beheersmaatregelen zal moeten zijn om de bedreiging te beheersen.
- Het vergelijken van het niveau van het residueel risico met de maturiteit van de bestaande/te nemen controlemaatregel(en)
- Op basis van deze beoordeling over de risicoafdekking (met de huidige beheersmaatregelen en zijn maturiteit) wordt de nood in verdere aanpak (vermijden, mitigeren, overdragen of accepteren – zie risicostrategie hieronder) van de bedreiging bepaald.

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

Bepalen risicostrategie

De literatuur kent vier soorten risicostrategieën, te weten: vermijden, mitigeren, overdragen en accepteren die een samenhang kennen met de mate van de waarschijnlijkheid en de impact.

- Soortgelijk aan de continuïteitsstrategie in het BCP van de organisatie kiest de organisatie in eerste instantie en overwegend voor het **mitigeren**, dit gebaseerd op de missie, visie en doelstellingen en in kader van dienstverlening.
- Voor een aantal diensten werd gekozen voor **overdragen** van het risico, onder andere door het inschakelen van een ICT-dienstverlener en door het afsluiten van diverse raamcontracten.
- Een aantal specifieke risico's waarbij de beheersmaatregelen veel meer inzet en tijd vergen dan het effect van het risico worden **geaccepteerd**.
- Risico's die we **vermijden** hebben geen gevolg meer op de missie, visie, doelstellingen en dienstverlening van de organisatie.

Het bepalen in welke strategie aangewend gaat worden, zal gebeuren op basis van de specifieke activiteiten die binnen een organisatie gebeuren. 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, dit bv op basis van de kostprijs om die specifieke

maatregel(en) te implementeren. Iedere keuze tot een risicostrategie zal gemotiveerd dienen te worden, en ter bevestiging aan de directie voorgelegd dienen te worden.

2.3.3. 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.

Vastleggen acties

De risico appetijt, zoals onder 'Bepalen risicostrategie' beschreven, wordt toegepast om na te gaan of er actie voor verbeteren van bestaande controlemaatregelen en/ of nieuwe controlemaatregelen worden gedefinieerd.

Voor de aanpak van de meest prioritaire risico's zijn volgende opties:

- Mitigeren
- Overdragen
- Acceptie
- Verwijderen

Voor elke actie wordt vastgelegd wat er gedaan moet worden, tegen wanneer en wie verantwoordelijk is voor deze actie. Eventueel wordt ook opgenomen hoe dit kan gemeten worden.

Opvolgen geformuleerde acties

Het doel van de aanpak van een risico is het verhogen van de mate van risicobeheersing zodat het risico voldoende afgedekt is. De mate van risicobeheersing van al de geïdentificeerde risico's is bepalend voor de maturiteit van de organisatie of een proces binnen de organisatie. De vraag van een uitgevoerde actie is of de mate van risicobeheersing hoog is.

Zelfs een aangepakt risico kan nog een rest van waarschijnlijkheid en/ of gevolg in zich houden. Niet alle controlemaatregelen zullen tot een waarschijnlijkheid van nul en/of een impact van nul leiden en er blijft vaak een residueel risico over.

Verantwoording van maatregelen vereist zowel binnen de scope van de AVG als in relatie tot het tactische beleid een Plan-Do-Check-Act-cyclus, die ervoor zorgt dat de organisatie blijft voldoen aan de AVG en het tactische beleid. Veel maatregelen die nodig zijn voor het voldoen aan de AVG vallen samen met de beveiligingsmaatregelen die in het kader van het tactische beleid zijn geïmplementeerd. Uitbesteding van gegevensverwerkingen aan derden vereist bijvoorbeeld zowel in het kader van de AVG als in het kader van het tactische beleid dat verwerkersovereenkomsten worden gesloten met verwerkers. Voor een leidinggevende is het vervelend als hij dezelfde maatregel tegenover twee verschillende functionarissen moet verantwoorden.

2.3.4. Communicatie en –overleg

Communicatie over risico's en het verloop van het proces dient gedurende het gehele proces plaats te vinden. Communicatie betrekt mensen bij risicobeheer en houdt het levend.

Zoals gesteld in dit document:

De verslagen van de individuele risicobeheeroefeningen, met daarin de geformuleerde acties, orden ter validatie voorgelegd aan de directie.

Jaarlijks wordt een overzicht van de activiteiten met betrekking tot risicobeheer voorgelegd aan de directie: een terugblik van gerealiseerde activiteiten m.b.t. risicobeheer in het voorgaande jaar en een vooruitblik op de plannen in het komende jaar.

Diverse kanalen worden ingezet voor communicatie en consultatie van risicobeheer, zoals overleggen, opmaken en beschikbaar stellen van verslagen en nota's, toelichtingen geven, berichtgeving opnemen in communicatietools, …

2.3.5. Monitoring en beoordeling

Dit onderdeel van het proces bestaat uit een opvolging inzake de implementatie van de genomen controlemaatregelen, alsook een evaluatie inzake het effect van de genomen controlemaatregelen uit de risicostrategie.

Jaarlijks moet verantwoording worden afgelegd over de waarmee informatiebeveiliging aandacht krijgt van de organisatie. De focus ligt op de horizontale verantwoording: binnen de organisatie, met een belangrijke rol voor het management. Met een interne audit sluit de verantwoording over informatieveiligheid aan op de planning en control-cyclus van de organisatie. Hierdoor heeft de organisatie meer overzicht over de informatieveiligheid van hun organisatie en kan het beter sturen en verantwoording afleggen aan o.a. externe audits of een toezichthoudende autoriteit. Uitgangspunt voor de verantwoording is het horizontale verantwoordingsproces aan het management.

3. LINK MET ANDERE MAATREGELEN

Beheer van incidenten is geen alleenstaand proces maar heeft interacties met de andere beheersprocessen:

〉 **Logging (monitoring)** (voor meer informatie zie document: 'Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer')

Bij het onderzoek naar mogelijke bedreigingen kan gebruik gemaakt van de controle op logging uit systemen, netwerkapparatuur en programma's. Los van de detectie, wordt logging ook achteraf gebruikt bij het reconstrueren van een bedreigingen of om te ontdekken welke systemen nog meer geraakt waren. Logs moeten bewaard worden volgens vaste regels en kennen per soort logging een bewaartermijn waarvan afgeweken kan worden (verlenging) als er een vermoeden is van een bedreiging. Als logging op de juiste wijze bewaard en behandeld wordt, kan logging ook dienen als bewijsmateriaal voor de wet. Dan moet wel de integriteit van de logging goed ingericht zijn.

〉 **Beheer van incidenten** (voor meer informatie zie document: 'Vo Informatieclassificatie - Minimale maatregelen – beheer incidenten')

Incidentbeheer om bedreigingen te voorkomen

Incidentbeheer helpt mee een inzicht te geven in de kans tot een mogelijke bedreigingen en welke gevolgen deze met zich mee kunnen brengen. Dit inzicht helpt bij het nemen van controlemaatregelen om bedreigingen te beheersen. Deze controlemaatregelen hebben dus betrekking op het beperken van de kans dat de bedreiging plaatsvindt en het gevolg van de bedreiging. Een goed inzicht in de bedreigingen en de te nemen controlemaatregelen om de bedreigingen te beperken tot een aanvaardbaar niveau heeft ook een gunstig effect op incidenten: er zullen minder incidenten voorkomen en/of de gevolgen ervan zijn beperkt.

Incidenten als input voor risicoanalyses

Anderzijds kan de informatie uit incidenten gebruikt worden om de risicoanalyse effectiever te maken. Immers, deze incidenten geven reële informatie over de bedreigingen die zich hebben voorgedaan en de gevolgen hiervan op de dienstverlening/bedrijfsvoering. Informatie over incidenten over een langere periode kan aldus gebruikt worden om een juistere kwalificatie van de waarschijnlijkheid[1] van een bedreiging te bekomen.

〉 **Wijzigingsbeheer** (voor meer informatie zie document: 'Vo Informatieclassificatie - Minimale maatregelen – wijzigingsbeheer')

Het proces wijzigingsbeheer zorgt voor een gestandaardiseerde werkwijze voor het behandelen van vragen tot wijzigingen in de ICT-infrastructuur zodat deze wijzigingen worden uitgevoerd met minimale impact op de kwaliteit van de dienstverlening en de zakelijke processen.

Elke wijziging houdt een min of meerdere bedreiging – en dus risico – in voor de omgeving waarin zij wordt uitgevoerd. Het is dan ook zaak voor elke wijziging de risico's ervan in te schatten. Minstens moet de wijziging aanleiding geven tot een revaluatie van de klasse van informatie die wordt verwerkt. Zo nodig moet de klasse aangepast worden aan de nieuwe situatie, wat dan weer

inhoudt dat de genomen maatregelen moeten worden herbekeken naar de minimale maatregelen van de nieuwe klasse.

4. Prestatie-indicatoren (KPI's)

Om de efficiëntie en effectiviteit van een proces te kwalificeren en waar nodig bij te sturen wordt een proces gemeten aan de hand van prestatie-indicatoren. De belangrijkste indicatoren worden KPI's of *Key Performance Indicatoren* genoemd. Per KPI wordt een norm afgesproken en de rapportering gebeurt per periode, bvb maandelijks of halfjaarlijks.

KPI's worden ook gebruikt om bij outsourcing en externe dienstverlening de kwaliteit van het uitbestede proces op te volgen. Deze KPI's worden dan ook vaak opgenomen in de SLA.

Voorbeelden van KPI's voor het proces risicobeheer zijn:

- Aantal risico's per maand;
- Aantal openstaande risico's per maand;
- Aantal opgeloste risico's per maand;
- Doorlooptijd van een risico (van melding tot afsluiting);
- Aantal informatie veiligheidsrisico's t.o.v. het totaal aantal risico's;
- Aantal niet geregistreerde of onvolledige risico's;
- Aantal risico's dat bij eerste melding correct verholpen is;
- Aantal risico's met juist communicatie naar betrokkenen;
- Aantal geëscaleerde risico's (functioneel en hiërarchisch);

Het vastleggen van de juiste prestatie-indicatoren is een moeilijke klus die de nodige aandacht vraagt: een teveel aan KPI's zal de organisatie (te) veel werk bezorgen, maar te weinig of onjuiste KPI's schetsen geen goed beeld van de kwaliteit van het risicobeheerproces.

De doelgroep voor de rapportering bepaalt tevens het type KPI: zo zal de risicomanager of CISO belang stellen in andere prestatie-indicatoren dan bvb de directie.