Informatieclassificatie Vlaamse overheid (Vo-ICR)

Risicoanalyse

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 het uitvoeren van een risicoanalyse. 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 2 delen. Eerst worden de minimale maatregelen besproken, alvorens in het 2de deel al de nodige aanvullende informatie ter beschikking wordt gesteld.

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	12 februari 2020	Kristel VAN AKEN	Draft
v.0.2	19 februari 2020	Kristel VAN AKEN	Feedback na interne bespreking
v.0.3	28 februari 2020	Kristel VAN AKEN	Feedback taakgroep
v.1.0	14 april 2020	Kristel VAN AKEN	Feedback leespanel
v 1.0	20 april 2020	Guy KLERKX	Aanpassing definitie risico
v.1.1	29 april 2020	Kristel VAN AKEN	Kleine aanpassingen aan de tekst Verklarende woordenlijst
v.2.0	21 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 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)

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

Inhoudsopgave

INLEIDING

Risicoanalyses vormen een belangrijke stap in het beveiligingsproces. Immers, informatiebeveiliging is ingericht op basis van een actueel inzicht in de interne en externe risico's en bedreigingen, de potentiële impact van bestaande bedreigingen en de risicobereidheid van de organisatie.

Organisaties staan vaak bloot aan tal van bedreigingen met de daarmee samenhangende risico's. Een risico bestaat uit de waarschijnlijkheid dat de bedreiging werkelijkheid wordt, en de impact hiervan. Vaak worden de bedreigingen tijdig opgemerkt en wordt er adequaat op geanticipeerd, maar soms zijn er negatieve gevolgen door slecht risicomanagement, waar risicoanalyse een onderdeel van is. Risicoanalyse helpt organisaties om de bedreigingen in kaart te brengen en mogelijk passende maatregelen te identificeren.

Naast de identificatie van mogelijke bedreigingen moet er vastgesteld worden hoe groot de waarschijnlijkheid is dat de bedreiging zich daadwerkelijk voordoet en welke consequenties (impact) dat heeft voor de bedrijfsprocessen. Daarna moet de afweging gemaakt worden of de kosten van de maatregelen opwegen tegen de kosten van het gevolg als een bedreiging werkelijkheid is geworden.

Veel factoren zorgen ervoor dat een organisatie wordt blootgesteld aan risico's. Hierbij wordt onderscheid gemaakt tussen interne en externe factoren.

Externe factoren:

- Demografische factoren
- Sociologische ontwikkelingen
- Politieke situaties
- Economische factoren
- Natuurlijke oorzaken
- Technologische ontwikkelingen
- Wetgevende factoren

Interne factoren:

- Bedrijfscultuur
- Personeelsrisico
- Interne organisatie
- Technologie

Er kunnen verschillende aanleidingen zijn om een risicoanalyse uit te voeren:

- **Ontwikkelingen in het bedreigingsniveau**: hete dreigingsniveau is aan verandering onderhevig, bijvoorbeeld wanneer een moedwillige verstoring heeft plaatsgevonden, een nieuwe kwetsbaarheid in de infrastructuur is geïdentificeerd of de organisatie in de publiciteit staat en daarmee de aandacht trekt van potentiële daders.
- **Ontwikkelingen in de omgeving**: ook omgevingsontwikkelingen kunnen aanleiding vormen voor het opnieuw uitvoeren van een risicoanalyse. Bijvoorbeeld wanneer een nieuwe dienst wordt opgezet, een significante infrastructuurwijziging plaatsvindt of een toepassing ontsloten wordt naar het internet.
- **Planning & controle processen in de organisatie**: de risicoanalyse vormt input voor het informatie beveiligingsplan en kan ertoe leiden dat de organisatie maatregelen wil implementeren die investeringen vergen. In dat geval is het van belang aan te sluiten bij de

planning van de begroting, omdat deze investeringen dan kunnen worden afgewogen tegen andere (potentiële) investeringen.

- **Regelgeving**: soms is er een wettelijke of andere regelgevende verplichting om een risicoanalyse uit te voeren, bv. in het kader van de GDPR of indien er sprake is van conformiteit met de Minimale Normen van de KSZ (Kruispuntbank van de Sociale Zekerheid).

1. MINIMALE MAATREGELEN

1.1 Minimale algemene maatregelen

Vertrouwelijkheid

IC klasse	Minimale maatregelen
	〉 Geen risicoanalyse vereist (minimale risico afweging is gewenst).
	Maatregel van Klasse 1 + 〉 Bij verwerking van persoonsgegevens van klasse 2 (contactgegevens) is een risico afweging gewenst.
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Uitvoeren van risicoanalyses conform de Vo risicoanalyse methodiek, 〉 Uitvoeren van een risicoanalyse minstens jaarlijks of bij significante wijzigingen in de omgeving (infrastructuur, dienstverlening, dreigingen) na validatie van de minimale maatregelen voorzien in het ICR. 〉 Uitvoeren pentest of vulnerability scan om de kwetsbaarheden in kaart te brengen is aanbevolen. 〉 Risico's moeten behandeld (mitigatie of overdracht), geaccepteerd of vermeden worden. 〉 Het management moet formeel de beslissingen over de behandeling van risico's aanvaarden. 〉 Formele acceptatie van het restrisico door het management.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Bij ontsluiting buiten de perimeter: uitvoeren pentest of vulnerability scan om de kwetsbaarheden in kaart te brengen is verplicht.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + 〉 Overdracht van risico's is niet toegestaan.

Integriteit

IC klasse	Minimale maatregelen
	〉 Geen risicoanalyse vereist (minimale risico afweging is gewenst).
	Maatregel van Klasse 1 + 〉 Bij verwerking van persoonsgegevens van klasse 2 (contactgegevens) is een risico afweging gewenst.
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Uitvoeren van risicoanalyses conform de Vo risicoanalyse methodiek, 〉 Uitvoeren van een risicoanalyse minstens jaarlijks of bij significante wijzigingen in de omgeving (infrastructuur, dienstverlening, dreigingen) na validatie van de minimale maatregelen voorzien in het ICR. 〉 Uitvoeren pentest of vulnerability scan om de kwetsbaarheden in kaart te brengen is aanbevolen. 〉 Risico's moeten behandeld (mitigatie of overdracht), geaccepteerd of vermeden worden. 〉 Het management moet formeel de beslissingen over de behandeling van risico's aanvaarden. Formele acceptatie van het restrisico door het management.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Bij ontsluiting buiten de perimeter: uitvoeren pentest of vulnerability scan om de kwetsbaarheden in kaart te brengen is verplicht.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + 〉 Overdracht van risico's is niet toegestaan.

Beschikbaarheid

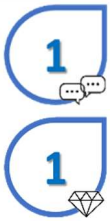
IC klasse	Minimale maatregelen
	〉 Geen risicoanalyse vereist (minimale risico afweging is gewenst).
	Maatregel van Klasse 1 +

	〉 Bij verwerking van persoonsgegevens van klasse 2 (contactgegevens) is een risico afweging gewenst.
	Alle maatregelen van Klasse 1 / Klasse 2 + 〉 Uitvoeren van risicoanalyses conform de Vo risicoanalyse methodiek, 〉 Uitvoeren van een risicoanalyse minstens jaarlijks of bij significante wijzigingen in de omgeving (infrastructuur, dienstverlening, dreigingen) na validatie van de minimale maatregelen voorzien in het ICR. 〉 Uitvoeren pentest of vulnerability scan om de kwetsbaarheden in kaart te brengen is aanbevolen. 〉 Risico's moeten behandeld (mitigatie of overdracht), geaccepteerd of vermeden worden. 〉 Het management moet formeel de beslissingen over de behandeling van risico's aanvaarden. 〉 Formele acceptatie van het restrisico door het management
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + 〉 Bij ontsluiting buiten de perimeter: uitvoeren pentest of vulnerability scan om de kwetsbaarheden in kaart te brengen is verplicht.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + 〉 Overdracht van risico's is niet toegestaan.

1.2 Minimale specifieke (GDPR) maatregelen

De minimale algemene maatregelen voor risicoanalyse 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.

	Er zijn geen GDPR specifieke maatregelen voor Klasse 2
	Klasse 3 en Klasse 4 kennen dezelfde maatregelen: 〉 Uitvoeren van een DPIA conform GDPR is verplicht in het geval van: 〉 systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, waaronder profilering, waarop besluiten worden gebaseerd die een natuurlijke persoon wezenlijk treffen, 〉 grootschalige verwerking van bijzondere categorieën van persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten, 〉 stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten. 〉 De DPIA moet volgende elementen bevatten: 〉 een gedetailleerde en duidelijke beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden. Het register van verwerkingsactiviteiten kan hier richtinggevend zijn, 〉 een beoordeling van de noodzaak en de evenredigheid van de verwerkingen in functie van de doeleinden, 〉 een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen, 〉 de beoogde maatregelen om de risico's aan te pakken.
	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 (NISII) 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 toegepast worden in het kader van een risicoanalyse:

Beschikbaarheid, Integriteit & Vertrouwelijkheid

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). 〉 Elke organisatie moet een risico analyse in het begin van het project uitvoeren om de noodprocedures te definiëren. Deze moeten bevatten: o De verwerking bij verminderde beschikbaarheid van informatiesystemen o De beschrijving van alternatieve informatiesystemen met inbegrip van de uitrol, de exploitatie modaliteiten en de eventuele ontwikkeling van de noodsystemen o De kerntaken en kernprocedures in geval van systeemonderbreking o De taken, de sleutelrollen en de in te zetten middelen om tot een optimale beschikbaarheid te komen Ref. KSZ 5.11.9 f). 〉 Een risico-beoordeling uitvoeren om de gepaste methode te bepalen voor het wissen van een informatiedrager (Ref. KSZ. 5.8.3 c). 〉 Gebeurtenissen en zwakheden over informatieveiligheid of privacy die verband houden met informatie en informatiesystemen van de organisatie zodanig kenbaar maken dat de organisatie tijdig en adequaat corrigerende maatregelen kan nemen (Ref. KSZ 5.13.1 c).

2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1. Scope van de risicoanalyse

Wat zijn risico's

Risico wordt ervaren als een onzekerheid dat latent aanwezig is en dat met een bepaalde waarschijnlijkheid impact kan hebben op het functioneren van de organisatie. Deze onzekerheden kunnen leiden tot gebeurtenissen die de doelstellingen van de organisatie zowel positief als negatief kunnen beïnvloeden: we spreken van opportuniteiten of bedreigingen.

Een risico in het ICR wordt daarom als volgt gedefinieerd:

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

Elk geïdentificeerde bedreiging moet op eenzelfde wijze beschreven worden:

> "Een **bedreiging** wordt veroorzaakt door een **oorzaak** en heeft een **gevolg** op het behalen van de doelstellingen van een organisatie als impact"

Risicoanalyses in het ICR

Risicoanalyses worden uitgevoerd op diverse aspecten van de organisatie. Zo zijn er financiële risicoanalyses, operationele risicoanalyses, enz. In het kader van het ICR is er sprake van risicoanalyses voor informatiebeveiliging en bescherming van persoonsgegevens.

2.2. Elementen van een risicoanalyse in het ICR

Risico = waarschijnlijkheid x impact van een bedreiging.

Wanneer ingezoomd wordt op deze formule, komen volgende elementen aan bod:

- Identificatie van de bedreigingen.
- De waarschijnlijkheid dat een bedreiging zich manifesteert, dit hangt nauw samen met de kwetsbaarheden van de omgeving en het aantal/aard van de actoren die kunnen ingrijpen op de omgeving.
- De impact indien een bedreiging zich manifesteert.

- De risicoweging: welke risico's zijn van groter belang voor de organisatie en moeten met hogere prioriteit aangepakt worden.

Analyse van de bedreigingen

In deze analyse worden de relevante bedreigingen in kaart gebracht. Het betreft bedreigingen waardoor verlies aan **beschikbaarheid**, **integriteit** of **vertrouwelijkheid** van de informatievoorziening kan ontstaan. Een bedreiging is elke omstandigheid die een kwetsbaarheid in de organisatie kan activeren (door misbruik of ongeluk) om zo een impact uit te lokken.

Het volledige spectrum van mogelijke bedreigingen wordt hierbij in kaart gebracht: natuurlijke dreigingen (overstromingen, bliksemschade, …), systeem faling, misdrijven, terroristische en andere aanvallen, ongelukken, enz.

Naast het inventariseren van de bedreigingen moet ook nagekeken worden hoe kwetsbaar de omgeving is voor de bedreiging. Deze kwetsbaarheid heeft gevolg voor de waarschijnlijkheidsberekening voor elke bedreiging: hoe hoger de kwetsbaarheid, hoe hoger de waarschijnlijkheid dat een bedreiging zich voordoet.

Een kwetsbaarheid moet ruim opgevat worden: het kan gaan om kwetsbaarheden in de infrastructuur, maar ook in de processen en er moet ook rekening worden gehouden met de menselijke factor. Voor kwetsbaarheden in de infrastructuur kan men vaak beroep doen op geautomatiseerde tools zoals 'vulnerability scans' en pentests. Maar ook leveranciers en andere instanties rapporteren regelmatig gevonden kwetsbaarheden in systemen (software en hardware) en de oplossing om deze kwetsbaarheden weg te werken. Daarnaast zijn ook gerapporteerde incidenten een bron van informatie over de kwetsbaarheden in een organisatie.

Analyse van de impact

Dit is het resultaat of effect van een bedreiging. Er kan een reeks mogelijke gevolgen verbonden zijn aan een bedreiging. De impact kan positief of negatief zijn in relatie tot de strategie of de bedrijfsdoelstellingen.

Voorbeelden van impact zijn:

- Reputatieschade.
- Financiële verliezen.
- Burgerlijke aansprakelijkheid.
- Schade aan de programmatorische doelstellingen van de instelling of aan het publieke belang.
- Lekken van informatie.
- Veiligheid en gezondheid van personen.
- Schending van het burgerlijk- , bestuurs- of strafrecht.

Grootte van waarschijnlijkheid en impact

Al deze informatie leidt tot de waarschijnlijkheid dat een dreiging zich voordoet en de impact ervan. Waarschijnlijkheid en impact moeten worden geschat of uitgedrukt. Dit kan op verschillende manieren:

- **Kwalitatief:** De waarschijnlijkheid van een mogelijk voorval of een omstandigheid en de bijbehorende impact (binnen de tijdshorizon die wordt overwogen door het bedrijfsdoel, bijvoorbeeld twaalf maanden) uitgedrukt in een bepaalde relatieve schaal (bvb hoog, medium of laag).
- **Kwantitatief:** De mogelijkheid van een voorval of een omstandigheid en de bijbehorende impact (binnen de tijdshorizon die wordt overwogen door het bedrijfsdoel, bijvoorbeeld twaalf maanden) uitgedrukt in een bepaald percentage.
- **Frequentie:** De mogelijkheid van een voorval of een omstandigheid en de bijbehorende impact (binnen de tijdshorizon die wordt overwogen door het bedrijfsdoel, bijvoorbeeld twaalf maanden) uitgedrukt in een hoeveelheid binnen een bepaalde periode (bvb drie maal per jaar).

2.3. Vormen van risicoanalyse

Over het algemeen wordt er onderscheid gemaakt tussen twee soorten risicoanalyse:
In een **kwantitatieve risicoanalyse** worden de rekenkundige risico's van een bedreiging berekend, gebaseerd op theoretische modellen. De risico's worden in een kwantitatieve risicoanalyse altijd uitgedrukt in meetbare criteria. Vaak gaat het om financiële gevolgen die berekend worden.

In **kwalitatieve risicoanalyses** worden relatieve schattingen gemaakt van de gelopen risico's. Kwalitatieve risicoanalyses gaan vaak uit van mogelijke scenario's, waarna vaak een 'worst case' en 'best case' scenario ontstaat. Het geeft onder meer een beter inzicht over het gedrag en cultuur van de mensen in een organisatie.

Het is van belang dat er een goede balans is tussen kwantitatief en kwalitatief risicomanagement. Statistische gegevens helpen bij het inschatten van de risico's, maar ook de menselijke kant is zeer belangrijk. Het kan inzicht geven in waarom mensen bepaalde acties wel of niet uitvoerden in het verleden, hoe ze de risico's aanpakten of hoe de bedrijfscultuur veranderd werd.

Soorten risico

Elke organisatie heeft in de loop der tijd controlemaatregelen getroffen voor de beveiliging van informatie, bv. Firewalls, antivirus programma's, fysieke toegangsbeperking enz.

In het kader van risicoanalyse kunnen verschillende soorten risico's benoemd worden, waarbij al dan niet rekening wordt gehouden met reeds genomen of nog te nemen maatregelen:

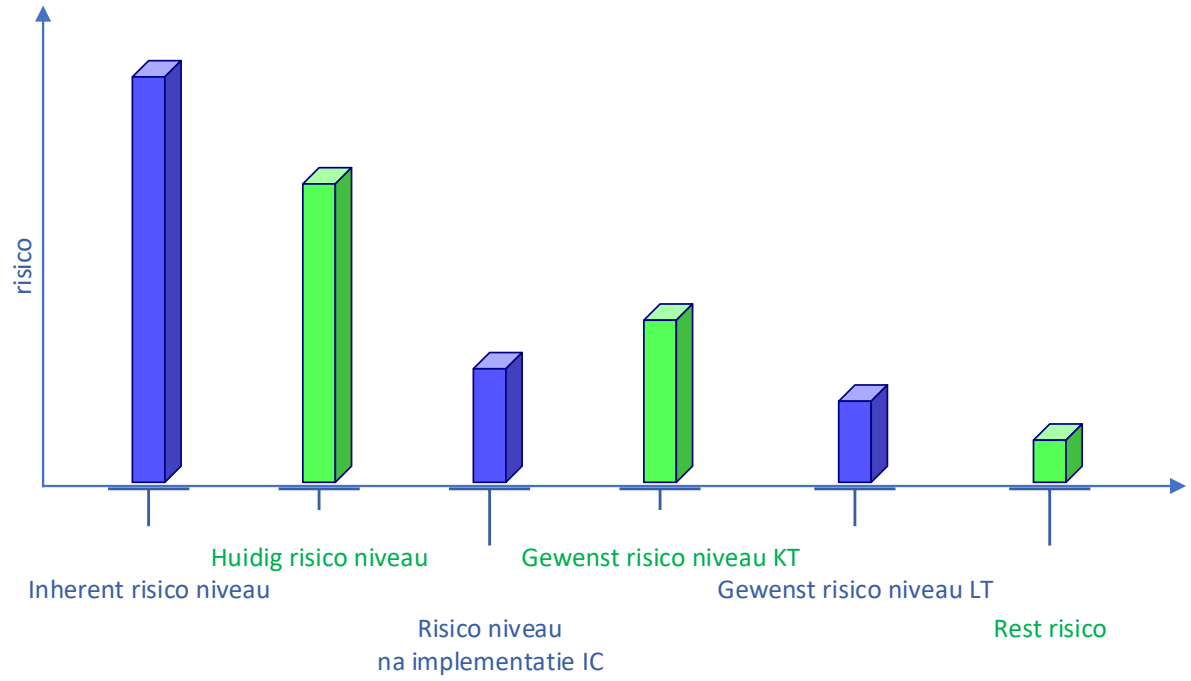
- **Inherente risico's**: het 0-punt ofwel de situatie waarin geen enkele controlemaatregel is getroffen.
- **Huidige risiconiveau**: het risiconiveau van nu, inclusief de reeds genomen controlemaatregelen.
- **Minimaal risiconiveau**: het risiconiveau rekening houdend met alle relevante minimale maatregelen van het ICR.
- **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?

- **Restrisico**: het risico dat overblijft nadat controlemaatregelen 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.

Het verschil tussen de gewenste situatie en de inherente risico's geeft een totaalbeeld van de risico's waar de organisatie mogelijk mee geconfronteerd wordt. Het verschil tussen de huidige situatie en de gewenste situatie en geeft een beeld van de gebieden waar bijkomende controlemaatregelen nodig zijn.

Het gewenste risiconiveau op korte en lange termijn kan hoger of lager zijn dan het risico na implementatie van het ICR; dit hangt af van de risicoappetijt van het management.

Volgende schema geeft een overzicht van de verschillende risiconiveaus (IC staat voor informatieclassificatie):



Het lijkt voor de hand te liggen om rekening te houden met reeds genomen controlemaatregelen en te focussen op de risico's waar nog actie op moet worden ondernomen. Toch is het belangrijk om ook stil te staan bij het totaalbeeld. Dat geeft namelijk een indicatie van wat ooit de grootste risico's waren en welke controlemaatregelen daarvoor genomen zijn. Deze informatie kan van pas komen om een management buy-in te bekomen.

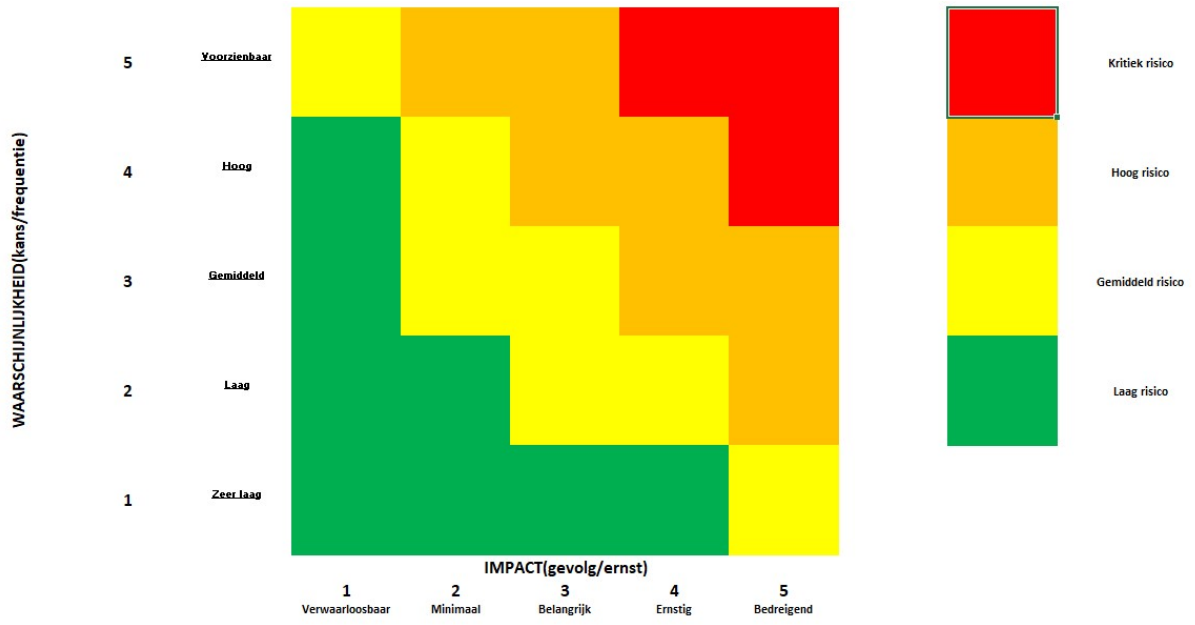
Nieuwe controlemaatregelen kunnen zelf weer nieuwe risico's met zich meebrengen. Een (hypothetisch) voorbeeld: Om de informatie uit personeelsdossiers te beschermen heeft een bedrijf een kluis aangeschaft waar deze dossiers in worden bewaard. De sleutel van de kluis hangt in een sleutelkastje met een cijferslot. De verantwoordelijke medewerker haalt 's ochtends bij binnenkomst de sleutel uit het kastje en draagt die de hele dag op haar lichaam. Maar als het sleutelkastje de hele dag van het slot af is (zonder de zichtbaarheid van de code actief te veranderen), kan iedereen de code aflezen en zich dus zo toegang tot de kluis verschaffen. Bij het bepalen van het risico speelt ook

mee voor wie informatie afgeschermd moet worden. Zijn dat in bovenstaand voorbeeld externen, dan werkt de genomen beheersmaatregel waarschijnlijk prima. Maar is het ook noodzakelijk om de informatie voor interne medewerkers af te schermen? Dan is deze maatregel een stuk minder effectief. Genomen controlemaatregelen kunnen een voedingsbodem zijn voor nieuwe risico's.

2.4. Risicoweging

De risicoweging is de laatste stap in de risicoanalyse. De gevonden bedreigingen op bedrijfsmiddelen en -processen worden geschat op hun waarschijnlijkheid en op de mogelijke impact. Risico is vervolgens waarschijnlijkheid x impact. Daardoor ontstaat een indeling van de gevonden risico's: risico's waarvan de waarschijnlijkheid relatief klein is versus risico's waarvan de waarschijnlijkheid relatief groot is. Tevens is er inzicht in risico's met relatief veel potentiële impact versus risico's met relatief weinig potentiële impact.

Men kan op eenvoudige wijze de waarschijnlijkheid en impact van een risico met elkaar in verband brengen in een risicomatrix. Hierbij bevinden de grootste risico's zich rechtsboven: grote waarschijnlijkheid, grote impact.



Voorbeeld van een risicomatrix

Na de risicoweging heeft de organisatie zicht op de risico's en op de relatieve grootte ervan. Dat vormt de basis voor een discussie die na de risicoanalyse wordt gevoerd, namelijk de discussie of de gevonden risico's aanleiding vormen om aanvullende maatregelen te nemen. Het is belangrijk dat het management betrokken wordt bij deze discussie of minstens haar goedkeuring aan de aanvullende maatregelen hecht.

2.5. Criteria voor risico's

Naast de risicoanalysemethode moeten ook de criteria voor de geïdentificeerde risico's vastgelegd worden. Met andere woorden welke risico's is de organisatie bereid te lopen, en welke impact van een bedreiging op vertrouwelijkheid, integriteit en beschikbaarheid van informatie kan de organisatie dragen. Deze zijn belangrijk om te komen tot de juiste strategie. Immers, impact die de organisatie niet wenst te dragen, zal voorkomen moeten worden.

Dit zijn de criteria voor risico's waarmee rekening moet worden gehouden:

- De aard van de organisatie,
- De grootte van de organisatie,
- Het soort informatie dat verwerkt wordt,
- De bedrijfscultuur,
- De risicoappetijt van het management,
- Aard van het risico zelf,
- De te nemen controlemaatregelen.

2.6. Omgaan met risico's

Of er daadwerkelijk maatregelen genomen worden na het identificeren van de risico's hangt af van een aantal factoren. Pas nadat alle risico's in kaart zijn gebracht kunnen er maatregelen genomen worden. Verschillende soorten maatregelen die genomen kunnen worden zijn:

- **Mitigeren** : door actieve handelingen risico's verminderen of uitbesteden;
- **Overdragen**: risico's overdragen aan een andere partij,
- **Accepteren**: geen gevolg geven aan de risico's, d.w.z. geen maatregelen nemen om risico's te verminderen
- **Vermijden**: risico's wegwerken door de activiteit stop te zetten of aan te passen.

Elke Vo entiteit moet voor de eigen organisatie de risicostrategie bepalen. Dit is een taak van het management en moet ook formeel gedocumenteerd en goedgekeurd worden.

Mitigeren

Risico mitigatie betekent het risico verlagen of verminderen. In de formule risico = waarschijnlijkheid x impact van een bedreiging betekent dit dus inspelen op ofwel de waarschijnlijkheid ofwel de impact van een bedreiging (of beide). Men kan de waarschijnlijkheid van de bedreiging verminderen door kwetsbaarheden weg te werken of men kan de mogelijke impactschade aanpakken en deze minimaliseren.

Overdragen

De organisatie kan er ook voor kiezen om het risico uit te besteden of over te dragen. Dit wordt bv. gedaan voor zeldzame gebeurtenissen met grote impact waarbij voor vele partijen de totale verwachte kost verdeeld wordt (d.m.v. een premie) of wanneer de organisatie de nodige capaciteit mist om het risico te mitigeren.

Accepteren

Is het risico klein, of weegt het niet op tegen de positieve uitkomsten, dan zullen er niet meteen additionele maatregelen genomen worden. De mogelijke impact wordt dan geaccepteerd. Acceptatie van een risico is rationeel indien men verwacht dat de kost van de controlemaatregelen hoger ligt dan de geschatte invloed van het risico op het bedrijfsresultaat. Ook als het risico niet kan worden vermeden, verminderd of uitbesteed, kan het management beslissen om het risico te accepteren. Het accepteren van een risico wil niet zeggen dat het risico niet beïnvloedbaar is. Op een later tijdstip kan er alsnog voor gekozen worden om het risico aan te pakken.

Vermijden

Wanneer een dienstverlening, beleid of bedrijfsproces binnen een organisatie teveel risico's met zich meebrengt, kan er voor gekozen worden om de dienstverlening, het beleid of proces te beëindigen of aan te passen zodat het risico niet meer bestaat.

2.7. Risicobeheer

Risicobeheer is een doorlopend proces omdat organisaties en hun omgeving constant veranderen. Om effectief te werk te gaan moet daarom tussentijds gemonitord worden. Na verloop van tijd kan het zijn dat een controlemaatregel niet meer genoeg beschermt tegen de bedreiging. Het effect dat de maatregel dan heeft op het risicoprofiel is dan minimaal en zal geüpdatet moeten worden.

De risico-informatie die beschikbaar komt na de analyses is bruikbaar voor besluiten die genomen worden in de toekomst. Bij elk nieuw groot project of ander omvangrijk proces of besluit moet bewust worden stilgestaan bij de risico's om het negatieve effect zo nodig te minimaliseren.

De kenmerken van het proces risicobeheer in het ICR zijn terug te vinden in '[Vo informatieclassificatie – Minimale maatregelen –risicobeheer]'.

2.8. Risicoanalyse als maatregel

Elementen van de risicoanalyse

Analyse van de zakelijke omgeving

Een eerste analyse betreft het gebruik van informatie in de zakelijke omgeving. Deze analyse moet een antwoord bieden op volgende vragen:

- Welke informatie wordt verwerkt?
- Met welke doeleinden wordt deze informatie verwerkt?
- Wanneer er sprake is van verwerking van persoonsgegevens moet tevens nagegaan worden welke de rechtsgrond van de verwerking is.

Validatie van reeds genomen maatregelen

Vervolgens moet bekeken worden of de risico's voldoende zijn afgedekt aan de hand van de minimale maatregelen zoals gedefinieerd in het ICR:

- Zijn alle minimale maatregelen van het model voorzien?
- Volstaan deze maatregelen om de risico's af te dekken?

De risicoanalyse uitvoeren

Zijn voorgaande elementen eenmaal uitgewerkt, dan is het tijd voor de risicoanalyse zelf: het in kaart brengen van de bedreigingen en kwetsbaarheden, bepaling van de waarschijnlijkheid en

impact indien een bedreiging zich zou manifesteren. Belangrijk is dat hiervoor een risicoanalyse methodiek wordt gebruikt die voldoet aan een aantal criteria om aanvaardbare resultaten te kunnen leveren die betrouwbaar en objectief zijn:

- **Methodisch onderbouwd**: er dient een methode voor risicoanalyses gekozen te worden. Eens deze methode gekozen, moet deze consistent toegepast worden om herhaalbaarheid en vergelijking van resultaten te kunnen garanderen.
- **Gestructureerd**: een goede risicoanalyse verloopt op een gestructureerde wijze waarbij steeds dezelfde stappen worden ondernomen.
- **Maatwerk**: elke risicoanalyse vraagt een inschatting op basis van de specifieke context, tijd, scope en middelen. Zomaar kopiëren van eerder uitgevoerde risicoanalyses is uit den boze.
- **Begrijpelijk en genuanceerd**: de resultaten van de risicoanalyse moeten begrijpelijk geformuleerd worden voor het doelpubliek. Het management moet in staat zijn beslissingen te nemen op basis van de bevindingen en aanbevelingen. De risicoanalyse methodiek dient dan ook de nodige schalen te bevatten om tot een correcte en voldoende genuanceerde inschatting te komen. Hierbij dient rekening te worden gehouden met de impactschalen in het ICR.
- **Communicatie, consultatie en formele aanvaarding door het management**: de nodige medewerkers dienen betrokken te zijn bij de verschillende stappen van de risicoanalyse. Enkel de DPO of CISO betrekken bij de risicoanalyse is niet voldoende.
- **Objectiviteit**: de methodiek moet een objectieve uitwerking van de risicoanalyse ondersteunen.
- **Uniformiteit en vergelijkbaarheid binnen de Vo**: de methodiek moet toelaten om risicoanalyses tussen Vo entiteiten uit te wisselen en/of te vergelijken. Sommige bedreigingen zijn immers Vo-breed en dan kan het interessant zijn om risicoanalyses uit te wisselen.

Keuze van de risicoanalysemethode

Bij de keuze van de gepaste risicoanalysemethode, wordt rekening gehouden met volgende kenmerken:

- De methode moet geschikt zijn voor de organisatie en het doel van de risicoanalyse. In geval van het ICR gaat het over het uitvoeren van risicoanalyses in het kader van informatiebeveiliging. De gekozen methode sluit hier op aan.
- De methode moet resulteren in een rapport dat de risico's beschrijft in een door de organisatie begrijpbare taal zodat de aard van de risico's en hoe ze kunnen worden behandeld, wordt gedocumenteerd.
- De methode moet granulair inzetbaar zijn: high-level zowel als detail analyse moet mogelijk zijn.
- De methode moet flexibel inzetbaar zijn en onafhankelijk van de infrastructuur.
- De methode moet accurate en betrouwbare resultaten produceren. De resultaten moeten vergelijkbaar zijn en steeds dezelfde output genereren bij eenzelfde input.
- De methode moet eenvoudig en intuïtief toepasbaar zijn. Het moet mogelijk zijn de methode toe te passen zonder expert kennis.
- De methode moet relatief snel werken. De doorlooptijd en de in te zetten medewerkers en hun tijd moeten beperkt blijven.
- De methode moet de analyse van verschillende maatregelen mogelijk maken.
- De methode moet heldere, goed geformuleerde en onderbouwde aanbevelingen voor het management aanleveren.

De details van de risico methodiek worden uitgewerkt in het document 'Vo – informatieclassificatie – Minimale maatregelen – risicoanalyse methodiek'.

Om risicoanalyses uit te voeren wordt veelal gebruik gemaakt van risicoanalyse instrumenten. Rekening houdend met risicoanalysemethode zal de keuze voor de risicoanalyse instrumenten beïnvloed worden door volgende factoren:

- **Kost**: zowel de aankoop als het gebruik, de in te zetten medewerkers en de tijd nodig om een risicoanalyse te maken,
- **Externe factoren**: indien de goedkeuring van externe partijen nodig is, bvb andere overheidsdiensten of autoriteiten,
- **Goedkeuring door management**: het management moet de gekozen instrumenten formeel goedkeuren en ondersteunen,
- **Structuur van de organisatie**: de instrumenten moeten passen in de structuur en grootte van de organisatie,
- **Aanpasbaarheid**: het moet mogelijk zijn de instrumenten aan te passen aan de noden van de organisatie,
- **Complexiteit**: de instrumenten mogen niet te complex zijn zodat het gebruik ervan niet te beperkt of niet te moeilijk is binnen de organisatie,
- **Volledigheid**: alle aspecten van informatie en informatiebeveiliging moeten aan bod komen,
- **Risiconiveau van de organisatie**: een hoog-risico organisatie zal meer rigoureuze instrumenten vragen dan een laag-risico organisatie,
- **Grootte van de organisatie**: deze bepaalt mee de keuze van de risicoanalyse instrumenten,
- **Consistentie**: moet de betrouwbaarheid van de resultaten mee garanderen,
- **Gebruiksgemak**: bepaalt hoe eenvoudig in gebruik, begrijpelijk en in staat om fouten te behandelen,
- **Valideerbaarheid**: het moet mogelijk zijn de resultaten en de aanbevelingen te valideren,
- **Automatisatie**: waar mogelijk moet er in zekere mate geautomatiseerd kunnen worden, bvb door te werken met 'drop-down' lijsten en invulvelden.

Het aanreiken van de instrumenten voor het uitvoeren van risicoanalyses behoort niet tot de scope van het ICR.

2.9. Link met de minimale maatregelen

Minimale maatregelen

Risicoanalyse kan tijdrovend en complex zijn. Binnen de Vo werd hieraan deels tegemoet gekomen door middel van de minimale maatregelen in het ICR. Dit houdt in dat er een stelsel van algemene minimale beveiligingsmaatregelen gedefinieerd wordt voor de gemiddelde organisatie of voor het gemiddelde bedrijfsproces. Organisaties kunnen door middel van het implementeren van deze maatregelen zich weren tegen een aantal vaak voorkomende risico's. De minimale maatregelen bieden een minimaal beschermingsniveau voor een organisatie of proces onder normale omstandigheden.

Het uitvoeren van een risicoanalyse is aangewezen indien de minimale maatregelen onvoldoende beveiliging bieden, of omdat de organisatie bepaalde klassen van informatie verwerkt. Risicoanalyses zijn bovendien in bepaalde gevallen verplicht vanuit de wet- en regelgeving (bv. GDPR).

Impact bepaling van bedreigingen

Het ICR heeft al een model voor impact bepaling voorzien (zie 'Vo informatieclassificatie – informatieclassificatieraamwerk'). Er wordt onderscheid gemaakt tussen materiële en immateriële schade:

- **Materiële schade** omvat fysische schade, financiële schade, verminderde dienstverlening aan burgers en bedrijven en economische schade;
- **Immateriële schade** omvat geestelijke schade, vrijheidsbeperking, sociale schade en reputatieschade.

Het raamwerk heeft 5 impactschalen gedefinieerd, die gekoppeld zijn aan de 5 klassen van informatie. Voor bepaling van de impact van bedreigingen, worden deze impactschalen hergebruikt in de risicoanalyse methodiek.

De impactschalen zijn beschreven in document 'Vo informatieclassificatie – informatieclassificatieraamwerk'.