Informatieclassificatie Vlaamse overheid (Vo-ICR)

Informatieclassificatieraamwerk (Vo-ICR)

ORGANISATIE

Team Informatieveiligheid| Digitaal Vlaanderen

Dit is een document voor publiek gebruik

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

INHOUD VAN DIT DOCUMENT

Doel van het document

Dit document maakt deel uit van de begeleidende documentatie in het kader van het Vo-brede informatieveiligheidsbeleid.

Het document beschrijft het Vo-brede informatieclassificatieraamwerk en hoe het toe te passen.

Het doelpubliek van dit document is elke entiteit die deel uitmaakt van de Vlaamse administratie in lijn met het bestuursdecreet van 7 december 2018.

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

Contact

Voor vragen in verband met het informatieclassificatieraamwerk kan je terecht bij het Team Informatieveiligheid via 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(s)	Opmerking(en)
v.2.0	4 augustus 2022	Kristel Van Aken	Opsplitsen doc organisatie als onderdeel van ICR2.0

Bronnen en verwijzingen

Onderstaande bronnen werden gebruikt om de inhoud van dit document te verbinden met de toegepaste wetgeving:

- VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD / 27 April 2016 (GDPR/AVG)
- AANBEVELING (BV) 06/2017 VAN DE COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER / 14 juni 2017 (Toepassing register van de verwerkingsactiviteiten)
- Informatieclassificatie/Standaard categorieën persoonsgegevens / 19 januari 2018
- Bestuursdecreet: https://codex.vlaanderen.be/PrintDocument.ashx?id=1030009&datum=&geannoteerd=false&print=false

Inhoudsopgave

INLEIDING

Het ICR is bindend!

De Vlaamse regering heeft tijdens de ministerraad van 15 oktober 2021 de strategie voor informatieveiligheid binnen (de dienstverlening van) de Vlaamse overheid goedgekeurd (zie nota VR 2021 1510 DOC.1151-1). Hiermee bekrachtigd de Vlaamse regering de toepassing van het ICR als volgt:

'*De Vlaamse Regering geeft, overeenkomstig art. 3 laatste lid van het decreet van 23 december 2016 houdende de oprichting van het stuurorgaan Vlaams Informatie-en ICT-beleid, het mandaat aan het Stuurorgaan, om samen met de werkgroep Informatieveiligheid en het agentschap Digitaal Vlaanderen deze beleidsdocumenten vorm te geven en op te volgen volgens, in overeenstemming met de afspraken binnen het organisatiemodel. Deze documenten en de toepassing van de VO-informatieclassificatie zijn bindend voor alle entiteiten van de Vlaamse overheid in scope van de strategie.*'

De scope van de nota - en dus ook de scope van de strategie en het daaruit voortvloeiende informatieveiligheidsbeleid - is de Vlaamse administratie zoals bepaald in het bestuursdecreet van 7 december 2018. Indien er uitwisseling van informatie nodig is met andere overheidsinstanties, waaronder de lokale besturen, wordt beroep gedaan op protocollen, zoals voorzien in het e-govdecreet van 18 juli 2008 (decreet betreffende het elektronische bestuurlijke gegevensverkeer).

Informatieveiligheid en haar kwaliteitskenmerken

ICR draait rond de 3 belangrijkste principes van informatiebeveiliging:

- Vertrouwelijkheid;
- Integriteit;
- Beschikbaarheid.

Vertrouwelijkheid

Met vertrouwelijkheid bedoelen we dat informatie alleen te gebruiken is door diegene die hiervoor geautoriseerd is. De eigenaar van de informatie stelt dit recht en de motivatie tot verwerking vast.

We moeten de vertrouwelijkheid van de informatie beschermen tegen verwerking door een niet-geautoriseerde derde. Dit kan gaan om personen, overheden of organisaties.

Integriteit

Integriteit is een synoniem voor betrouwbaarheid. Betrouwbare informatie voldoet aan volgende integriteitskenmerken:

Technische integriteit

- We kunnen de informatie via een betrouwbaar kanaal benaderen
- Het heeft een betrouwbare bron

Contextuele integriteit

- De informatie is correct (rechtmatigheid is hier een kernbegrip)

- De informatie is volledig
- De informatie is tijdig (op tijd)
- De informatie is geautoriseerd (aangemaakt of aangepast door een persoon of organisatie die gerechtigd is een aanpassing aan te brengen)

Beschikbaarheid

Beschikbaarheid geeft aan in hoeverre toepassing en de daaraan gerelateerde informatie toegankelijk is voor de geautoriseerde gebruikers. We maken een onderscheid tussen beschikbaarheid en bedrijfscontinuïteit. Bedrijfscontinuïteit houdt in dat kritieke dienstverlening gegarandeerd kan worden ingeval van ramp. Beschikbaarheid houdt in dat de dienstverlening geleverd wordt tijdens normale omstandigheden. Met dienstverlening bedoelen we het leveren van informatie en informatie verwerkende middelen aan burgers en organisaties.

Een voorbeeld om dit verschil duidelijk te maken: een disaster recovery site dient om in geval van een ramp de kritische componenten terug operationeel te maken binnen een afgesproken tijdsbestek. Overgaan naar zo'n disaster recovery oplossing vraagt veel werk en is niet iets wat je zomaar even in gang zet. Het is dan ook geen geschikte oplossing om alle componenten tijdens normale gang van zaken operationeel te houden. Anderzijds bieden vele technische oplossingen voor hoog-beschikbaarheid ('high-availability') zoals ontdubbelen van componenten geen oplossing voor rampscenario's, bv. omdat ze op dezelfde site ingezet worden. Als zo'n site dan getroffen wordt, zijn alle componenten, ontdubbeld of niet, eveneens getroffen.

We houden ook rekening met het aspect performantie: een verminderde of vertraagde werking van de performantie of een verminderde capaciteit heeft ook impact op de beschikbaarheid.

Een ander deelaspect waar we aandacht aan besteden is herstelbaarheid: de mate waarin de dienstverlening bestaande uit informatie en de informatievoorziening, na onbeschikbaarheid hersteld kan worden. Herstel van informatie houdt in dat we op zoek gaan naar de meest recente versie van de informatie, maar ook naar de meest volledige informatieset.

En ten slotte houden we ook rekening met kritische bedrijfsmomenten: het is best mogelijk dat informatie gedurende een groot deel van het jaar weinig beschikbaar moet zijn, maar op bepaalde momenten hoog beschikbaar moet zijn, bijvoorbeeld de salarisberekening is vooral cruciaal op het einde van elke maand.

In de architectuur fase van een toepassing worden op basis van de eisen van de opdrachtgever de technische architectuur en de technische componenten gekozen om de gewenste beschikbaarheid te realiseren.

Beschikbaarheid wordt beïnvloed door verschillende factoren. De belangrijkste is de uitval van de dienst. Daarbij zijn twee verschillende soorten uitval relevant:

- Gepland, bijvoorbeeld tijdens een gepland onderhoud of tijdens de implementatie van een project;
- Ongepland, bijvoorbeeld door een incident.

Bij het bepalen van de beschikbaarheid wordt de geplande onbeschikbaarheid niet meegenomen. Dat wil zeggen dat het geplande onderhoud geen negatieve invloed heeft op de beschikbaarheid die wordt gerapporteerd, tenzij de planning wordt overschreden.

Een andere factor is de end-to-end beschikbaarheid en de beschikbaarheid van de tussenliggende componenten. Ook al is de informatie en de toepassing beschikbaar, door falen van een component is het eindresultaat evenzeer een onbeschikbaarheid van informatie naar de burger of organisatie. Dit aspect wordt in de praktijk geregeld via OLA's (*Operational Level Agreement*), dit zijn overeenkomsten tussen de dienstenleverancier en een ander deel van de organisatie.

Beschikbaarheid van een dienst is afhankelijk van de beschikbaarheid van elk van de samenstellende delen.

We vatten samen welke kenmerken we in overweging nemen als het gaat over beschikbaarheid:

- De onverwachte uitval van één of meerdere componenten die deel uitmaken van het leveren van informatie en informatie verwerkende systemen aan de burger of organisatie;
- Een vermindering van de performantie;
- De gehele of gedeeltelijke herstelbaarheid van informatie;
- De kritische bedrijfsmomenten waarop informatie of informatie verwerkende systemen niet mogen uitvallen.

Volgende kenmerken maken geen deel uit van beschikbaarheid:

- Geplande werkzaamheden zoals gepland onderhoud, implementaties;
- Projecten (beschikbaarheid gaat enkel over de operationele omgeving);
- Rampscenario's (hiervoor wordt het bedrijfscontinuïteitsplan ingeschakeld).

De beschikbaarheidsschalen worden in de praktijk als een percentage gepresenteerd, waarbij een hogere waarde een positievere uitkomst is dan een lage waarde. In het kader van de dienstverlening worden deze waarden als vereisten opgenomen in de SLA (*Service Level Agreement*), dit is een overeenkomst tussen de aanbieder en de afnemer. De vertaalslag van de beschikbaarheidsschalen naar de SLA en de OLA maakt geen deel uit van dit document (maar wordt wel opgenomen in documentatie level 3), we geven wel een voorbeeld:

Hoge beschikbaarheid wordt uitgedrukt in het aantal negens:
2 negens: 99% dienst is 3,65 dagen per jaar niet beschikbaar
4 negens: 99,99% dienst is 52 minuten per jaar niet beschikbaar
6 negens: 99,9999% dienst is 31 seconden per jaar niet beschikbaar
Wanneer verschillende componenten achtereenvolgens in een informatiesysteem worden gebruikt, wordt de beschikbaarheid bepaald door de beschikbaarheidsfactoren met elkaar te vermenigvuldigen. Combinatie van de twee componenten met een beschikbaarheid van resp. 2 en 4 negens betekent een totale niet-beschikbaarheid voor het systeem van 3,69 dagen per jaar.

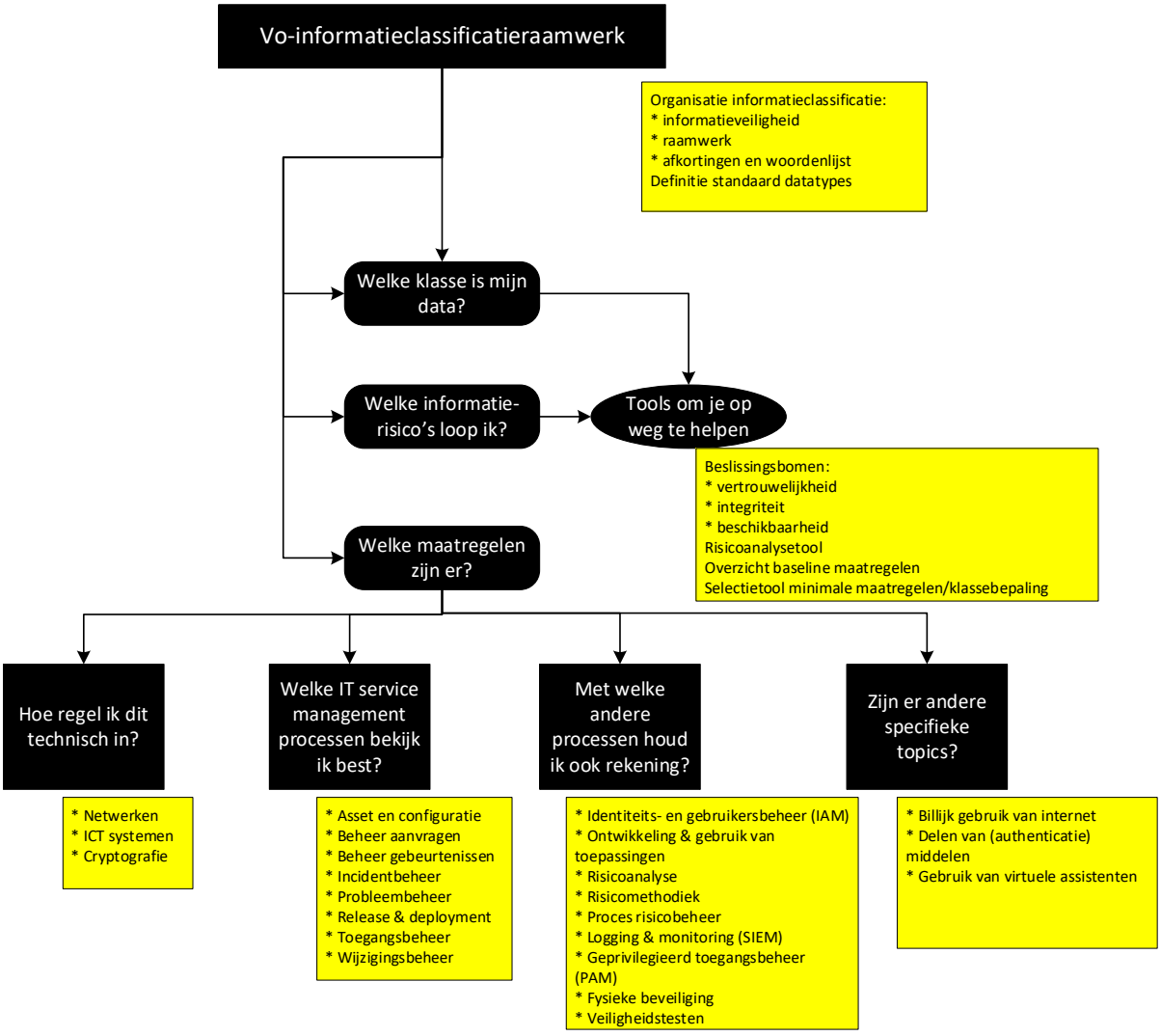
1. Informatieclassificatieraamwerk (ICR)

1.1. Componenten van het ICR

Zoals uitgelegd in het document '[Vo informatieclassificatie – organisatie – informatieveiligheid]', behoort het ICR tot documentatie level 2. Het bestaat uit volgende componenten:

- De basis van het raamwerk wordt gevormd door de informatieklassen. Er zijn 5 klassen, telkens voor vertrouwelijkheid, integriteit en beschikbaarheid. Elk significant informatie-asset moet een klasse voor vertrouwelijkheid, een klasse voor integriteit en een klasse voor beschikbaarheid toegewezen krijgen. Dit proces is cruciaal omdat het de basis vastlegt voor de beveiliging van het informatie-asset.
- Het bepalen van de informatieklassen voor een informatie-asset is een eerste, belangrijke stap om te bepalen welke technische en organisatorische maatregelen moeten worden genomen om het geschikte niveau van veiligheid te bereiken. Deze maatregelen vormen het tweede element in het raamwerk. Er zijn minimale maatregelen gedefinieerd binnen het raamwerk voor elke informatieklasse.

De structuur van het ICR ziet er als volgt uit:



Het ICR omvat de volgende documenten:

- Twee documenten over de organisatie van informatieveiligheid:
  - Organisatiedocument Informatieclassificatieraamwerk (ICR) (huidig document): beschrijft de principes, werking en toepassing van het ICR.
  - Organisatiedocument Informatieveiligheid: geeft het brede kader weer rond informatieveiligheid, hoe het raamwerk tot stand komt en wie het beheert.
- Overzicht baseline maatregelen volgens ISO27001: inventaris van alle maatregelen volgens de verschillende klassen.
- Minimale maatregelen: set van documenten die enkele specifieke domeinen uitwerken:
  - Technologieën:
    - Netwerken
    - ICT-systemen
    - Cryptografie
  - Servicemanagement (ITIL):
    - Asset en configuratiebeheer
    - Beheer aanvragen
    - Beheer gebeurtenissen
    - Incident beheer
    - Release en deployment beheer
    - Toegangsbeheer
    - Wijzigingsbeheer
    - Probleembeheer
  - Processen:
    - IAM
    - Ontwikkeling en gebruik van toepassingen
    - Risicomethodiek
    - Risicoanalyse
    - Proces risicobeheer
    - SIEM
    - PAM
    - Fysieke beveiliging

1.2. Hoe het ICR toe te passen in de praktijk

Het ICR toepassen begint met een inventarisatie van alle significante informatie-assets waarover een entiteit beschikt. Per informatie-asset wordt dan de klasse bepaalt voor vertrouwelijkheid, integriteit en beschikbaarheid. Om de entiteiten hierbij te helpen, werd een toolset samengesteld, deze vind je op Informatieclassificatieraamwerk | Vlaanderen.be.

Met elk van de klassen komt een set minimale maatregelen overeen. De entiteit zorgt voor een passend niveau van beveiliging voor elke geïnventariseerde informatie-asset door middel van het ‘pas toe of leg uit’ principe:

- Het toepassen van de minimale maatregelen zoals bepaald voor de informatieklasse van toepassing (‘pas toe’ principe).

- Indien een minimale maatregel niet kan worden toegepast, dan moet er transparant gecommuniceerd worden (‘leg uit’ principe):
  - Ofwel voorziet de entiteit in een set van complementaire maatregelen die samen minstens een gelijkwaardig niveau van beveiliging bereikt. Deze afwijking van de minimale maatregelen moet gedocumenteerd worden en goedgekeurd door de hoogste instantie van de entiteit (leidend ambtenaar of gelijkwaardig).
  - Ofwel is een toepassing of evenwaardige maatregel niet mogelijk, dan moet er een zwaarwegende reden voorhanden zijn en die moet dan gedocumenteerd worden en goedgekeurd door de hoogste instantie van de entiteit (leidend ambtenaar of gelijkwaardig).

1.2.1. Levenscyclus

Eigenaars van informatie bekijken regelmatig of de informatieklasse nog steeds relevant en correct is. Het topmanagement (leidend ambtenaar of directeur) is verantwoordelijk voor de informatie(verwerking) en dus aansprakelijk dat een periodieke evaluatie wordt uitgevoerd. Aan de entiteiten wordt aangeraden deze activiteit te integreren in haar veiligheidsplan.

De frequentie van deze oefening hangt af van de informatieklasse:

- Informatieklasses 1, 2 en 3:

  Minstens jaarlijks.

- Informatieklasses 4 en 5:
  - Minstens jaarlijks,
  - Bij significante wijziging van de informatieverwerking
  - Bij significante wijzigingen in de criteria en/of maatregelen.

Een mogelijk gevolg van deze oefening is het bijsturen van organisatorische en technische maatregelen op data die nu anders ingeschaald is.

1.2.2. Link met risicobeheer

Informatiebeveiliging is geen doel op zich, maar beoogt de risico’s ten aanzien van vertrouwelijkheid, integriteit en beschikbaarheid te voorkomen of op z’n minst te verlagen tot een voor de organisatie aanvaardbaar niveau. Risicobeheer is dan ook een belangrijk concept binnen informatiebeveiliging.

Een risico-gebaseerde aanpak is dan ook de basis van het ICR. Voor informatieklassen 1 en 2 volstaat het implementeren van de minimale maatregelen, omdat deze inherent voldoen om de risico’s op deze informatie-assets te mitigeren. Dat neemt niet weg dat een entiteit ook hier nog op basis van een risicoanalyse kan bepalen welke risico’s het al dan niet aanvaardt en welke maatregelen het hier tegenover stelt. Voor informatieklassen 3, 4 en 5 wordt risicobeheer echter expliciet gemaakt: hier volstaat het niet om de minimale maatregelen toe te passen maar is steeds een risicoanalyse en risicobehandeling bij de verwerking van deze informatie-assets vereist. Dit is de verantwoordelijkheid van de entiteit.

1.3. Informatieklassen

1.3.1. Relatie tussen vertrouwelijkheid en integriteit

Vertrouwelijkheid en integriteit hebben geen één-op-één relatie. Conform de opzet en structuur van de informatieklassen, bevatten de minimale algemene maatregelen de basis om aan vertrouwelijkheids- en aan integriteitvereisten tegemoet te komen. Op basis van specifieke regelgeving zullen deze minimale algemene maatregelen uitgebreid worden met minimale specifieke maatregelen. De eigenaar of verwerker van de informatie kan op basis van geïdentificeerde risico's beslissen om bijkomend maatregelen te identificeren en in te richten of om het risico op een andere manier te behandelen (risico overdracht, risico acceptatie).

Vertrouwelijkheids- en integriteitsklassen en beschikbaarheidsklassen worden onafhankelijk van elkaar toegekend aan informatie. Het kan dus gebeuren dat informatie een bepaalde klasse voor vertrouwelijkheid toegekend krijgt – bv. 2 – en een andere voor integriteit – bv. 3. In dit geval moeten de minimale maatregelen voor klasse 2 voor vertrouwelijkheid en voor klasse 3 voor integriteit toegepast worden. Het komt vaak voor dat een maatregel zowel vertrouwelijkheid als integriteit bedient. In dit geval wordt de maatregel voor de hoogste klasse toegepast – in het voorbeeld klasse 3 (integriteit). Een maatregel die uitsluitend vertrouwelijkheid of uitsluitend integriteit afdekt, hoeft aan deze regel niet te voldoen.

1.3.2. Relatie tussen informatieklasse en impact

Het toekennen van informatieklassen aan informatie-assets heeft als doel (relatief) eenvoudig en consistent in te schatten welke controlemaatregelen we nodig hebben om de vertrouwelijkheid, integriteit en beschikbaarheid van de asset op gepast niveau te borgen. Om dit te kunnen doen, moeten we eerst inzicht krijgen in de gevolgen als niet voldaan wordt aan de vertrouwelijkheid, integriteit of beschikbaarheid van de asset. We gaan na welke impact er zou zijn indien de asset gecompromitteerd zou worden, dus als er een inbreuk zou plaatsvinden.

1.4. Impact

1.4.1. Definitie van de impactschalen

We identificeren een informatieklasse door na te gaan wat het (potentieel) gevolg kan zijn van een inbreuk op de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.

De impact is gebaseerd op de potentiële schade van een inbreuk. Deze impact schalen rangschikken we oplopend van lage tot onbestaande impact of schade in klasse 1, tot bedreigende impact of schade in klasse 5. Op deze manier worden deze impact of schade schalen uniek verbonden aan de kwaliteitsgraden in het informatieclassificatieraamwerk.

1.4.2. Impact van de gebruikte criteria

In het ICR gebruiken we deze criteria:

- Informatieveiligheidsstandaarden als basis (ISO27001/2);
- Regelgevingen, die leiden tot een vaste informatieklasse;
- Contractuele verbintenissen die leiden tot een vaste informatieklasse;
- Impact van potentiële inbreuken op basis van onderstaande impact schalen en hun referentie criteria.

Het is hierbij belangrijk het onderwerp van de betrokken regelgeving (en/of contractuele verbintenis) correct te interpreteren.

In specifieke regelgeving kan dit anders liggen. Het bekendste voorbeeld hiervan is de GDPR-wetgeving die het individu beschermt tegen risico's verbonden aan het verwerken van informatie door anderen dan de burger zelf. In GDPR-context is men verplicht om, naast de 'gevolgen van inbreuken voor de organisatie' ook, de 'gevolgen van inbreuken op het betrokken individu in kaart te brengen en te evalueren'.

1.4.3. Inschatting van de impact

Wanneer we het hebben over impact, maken we onderscheid tussen materiële en immateriële schade.

Materiële schade

Materiële schade is het meest 'tastbaar'. Het heeft betrekking op schade waarbij de grootte van het nadeel relatief gemakkelijk monetair uit te drukken is. Doorgaans speken we hierbij over:

〉 **Fysische schade**

Schade aan voorwerpen en goederen
Letselschade of schade aan personen beperkt in tijd die niet resulteren in immateriële schade

〉 **Financiële schade**
〉 **Economische schade**

Tijdelijke (technische) werkloosheid van het personeel

〉 **Verminderde dienstverlening aan burgers en/of bedrijven**

Voorbeelden van materiële schade:
Kosten bij aankoop vervangingsgoederen en diensten, inkomensverlies, pensioenschade, kosten van huishoudelijke hulp, ziektekosten (ziekenhuiskosten, kosten fysiotherapeut, kosten hulpmiddelen), kosten woningaanpassing, extra reiskosten, stijgende verzekeringspremie, telefoonkosten en juridische hulp

Immateriële schade

Immateriële schade is minder makkelijk aanwijsbaar en is veel lastiger uit te drukken in geld. In de meeste gevallen is de compensatie van de schade erg hoog of erg moeilijk tot onmogelijk. We spreken hierbij over:

〉 **Geestelijke schade,** pijn, trauma of smart, gemis, verdriet, verlies van levensvreugde, angsten
〉 **Vrijheidsbeperking**: gedeeltelijk of volledig, tijdelijk of permanent

Verlies van fysieke vrijheid
Verlies van vrijheid van handelen

Verlies van beroep
Verlies van vrijetijdsbesteding

〉 **Fysische schade**, gedeeltelijke of volledige onbeschikbaarheid van handelen, in extreme vormen bedreigend voor het voortbestaan van:

Personen
Organisaties
Diensten

- **Sociale schade,** verlies van sociale contacten
- **Reputatieschade** verbonden aan:
  - Personen
  - Organisaties
  - Producten
  - Diensten

Voorbeeld: *Smaad of laster. Een kritisch artikel over iemands wangedrag kan volkomen rechtmatig zijn ook al schaadt het de betrokkene in zijn reputatie.*

1.5. Impactschalen

In het organisatiedocument Informatieveiligheid hebben we het verschil (en de gelijkenissen) tussen informatiebeveiliging en bescherming van persoonsgegevens uitgelegd. We definiëren ook impactschalen vanuit het standpunt van de generieke organisatie en vanuit het standpunt van individuen (GDPR).

1.5.1. Generieke impactschalen

Rekening houdend met de materiële en immateriële schade, definiëren we de volgende impact schalen, deze zijn generiek en stellen zich in het standpunt van de organisatie:

	Definities van impact op de organisatie
1	**Verwaarloosbare impact/schade** 〉 Geen impact op de organisatie. 〉 Dienstverlening (het leveren van informatie en informatie verwerkende systemen aan de burger of organisatie) kan langere tijd (meer dan een maand) onbeschikbaar zijn zonder significante gevolgen voor de organisatie of voor de burger. 〉 Er zijn geen kritische bedrijfsmomenten.
2	**Minimale impact/schade** 〉 Bijsturing van de criteria en/of maatregelen zijn aangewezen om de dienstverlening te ondersteunen. 〉 Niet beschikbare dienstverlening langer dan één maand heeft significante gevolgen voor de organisatie of de burger. 〉 Er zijn geen kritische bedrijfsmomenten.
3	**Belangrijke impact/schade** 〉 Bijsturing van de criteria en/of maatregelen zijn noodzakelijk om de dienstverlening te ondersteunen. 〉 Het lopende werkingsbudget ondersteunt de financiële middelen.

- Niet beschikbare dienstverlening langer dan één week heeft significante gevolgen voor de organisatie of de burger.
- Er kunnen kritische bedrijfsmomenten optreden, waarop een onbeschikbaarheid van meer dan 24 uur significante gevolgen heeft voor de organisatie of burger.

Ernstige impact/schade

- 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 lopende en toekomstige werkingsbudgetten.
- Niet beschikbare dienstverlening langer dan 72 uur heeft significante gevolgen voor de organisatie of de burger.
- Er kunnen kritische bedrijfsmomenten optreden, waarop een onbeschikbaarheid van meer dan 12 uur significante gevolgen heeft voor de organisatie of de burger.

Bedreigende impact/schade

- Bijsturing van de criteria en/of maatregelen zijn 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.
- Niet beschikbare dienstverlening langer dan 24 uur heeft significante gevolgen voor de organisatie of de burger.
- Er kunnen kritische bedrijfsmomenten optreden, waarop een onbeschikbaarheid van meer dan 2 uur significante gevolgen heeft voor de organisatie of de burger.

1.5.2. Specifieke impactschalen voor persoonsgegevens (GDPR)

Onderstaande impact schalen zijn specifiek gericht op de evaluatie van persoonsgegevens. De wetgeving (GDPR) heeft het individu als onderwerp:

Opmerking: *Onderstaande schalen gebruiken we als evaluatie van restrisico's nadat de maatregelen gedetailleerd in de overeenkomstige specifieke maatregelen zijn genomen.*

Definities van impact op het individu

Verwaarloosbare impact/schade

- Materiële schade

Geen tot verwaarloosbare financiële schade voor het individu
Geen aantoonbare impact op de levenskwaliteit

- Immateriële schade

Geen tot minimale immateriële schade voor het individu

Eigenwaarde

Reputatie en stigmatisering

Minimale impact/schade

〉 Materiële schade

Minimale financiële schade voor het individu
Geen aantoonbare impact op de levenskwaliteit
Potentiële compensatie mogelijk zonder juridische dwangmaatregelen

〉 Immateriële schade

Geen tot minimale immateriële schade voor het individu

Eigenwaarde
Reputatie en stigmatisering

Belangrijke impact/schade

〉 Materiele schade

Belangrijke financiële schade voor het individu
Geen aantoonbare blijvende impact op de levenskwaliteit
Potentiële compensatie mogelijk op basis van juridische dwangmaatregelen

〉 Immateriële schade

Geen tot minimale immateriële schade voor het individu

Eigenwaarde
Reputatie en stigmatisering

Ernstige impact/schade

〉 Materiële schade

Belangrijke financiële schade voor het individu
Aantoonbare blijvende impact op de levenskwaliteit
Compensatie mogelijk op basis van juridische dwangmaatregelen

〉 Immateriële schade

Ernstige immateriële schade voor het individu

Eigenwaarde
Reputatie en stigmatisering
Gelijkheid
Integriteit van de persoon
Ongestoord leven
Autonomie

Fysieke integriteit

Verlies aan zelfstandigheid
Bewegingsvrijheid

Bedreigende impact/schade

〉 Materiële schade

Beëindigen financiële autonomie
Compensatie onmogelijk

〉 Immateriële schade

	Fysieke integriteit
	Marteling en mishandeling met, al dan niet, blijvende fysieke of psychologisch trauma
	Levensbeëindiging

1.5.3. Informatieklassen voor vertrouwelijkheid en integriteit

Door de koppeling van de impactschalen aan de klassen van informatie, worden zowel voor vertrouwelijkheid als integriteit 5 klassen voorzien. Gebruik makend van deze 5 impactschalen kunnen de klassen van vertrouwelijkheid en integriteit geïdentificeerd worden:

schaal	Vertrouwelijkheid	schaal	Integriteit
1	Organisatie: 〉 De informatie is consulteerbaar door iedereen. 〉 Er is geen of verwaarloosbare impact als de informatie publiek is. 〉 De dienstverlening blijft gegarandeerd als de informatie publiek is. Personen: 〉 Er is geen tot minimale materiële schade (financiële schade, levenskwaliteit) voor het individu indien de betrokken persoonsgegevens publiek zijn. 〉 Er is geen tot minimale immateriële schade voor het individu indien de betrokken persoonsgegevens publiek zijn.	1	Organisatie: 〉 Schending van de integriteit (foutieve informatie, wijziging door onbevoegden) heeft geen of verwaarloosbare impact op de organisatie. 〉 De dienstverlening blijft gegarandeerd als de informatie gewijzigd wordt. Personen: 〉 Er is geen tot minimale materiële schade (financiële schade, levenskwaliteit) voor het individu indien de betrokken persoonsgegevens foutief zijn. 〉 Er is geen tot minimale immateriële schade voor het individu indien de betrokken persoonsgegevens foutief zijn.
2	Organisatie: 〉 De informatie is toegankelijk voor alle medewerkers van de organisatie. 〉 Bijsturing van de criteria en/of maatregelen zijn aangewezen indien de vertrouwelijkheid geschonden is. Personen:	2	Organisatie: 〉 Minimale fouten in de informatie zijn toegestaan. 〉 De organisatie heeft geen directe hinder indien de informatie gewijzigd wordt door onbevoegden. 〉 Bijsturing van de criteria en/of maatregelen zijn aangewezen indien de integriteit geschonden wordt.

	〉 Er is materiële schade voor het individu indien de betrokken persoonsgegevens consulteerbaar zijn door onbevoegden: minimale financiële schade; geen aantoonbare impact op levenskwaliteit; potentiële compensatie is mogelijk zonder juridische dwangmaatregelen. 〉 Er is geen tot minimale immateriële schade voor het individu indien de betrokken persoonsgegevens consulteerbaar zijn door onbevoegden.		Personen: 〉 Er is materiële schade voor het individu indien de betrokken persoonsgegevens foutief zijn: minimale financiële schade; geen aantoonbare impact op levenskwaliteit; potentiële compensatie is mogelijk zonder juridische dwangmaatregelen. 〉 Er is geen tot minimale immateriële schade voor het individu indien de betrokken persoonsgegevens foutief zijn.
schaal	**Vertrouwelijkheid**	**schaal**	**Integriteit**
3	Organisatie: 〉 De informatie is toegankelijk voor een grote groep gebruikers. 〉 Bijsturing van de criteria en/of maatregelen zijn noodzakelijk indien de vertrouwelijkheid geschonden is, maar dit is nog mogelijk binnen het lopende werkingsbudget. Personen: 〉 Er is materiële schade voor het individu indien de betrokken persoonsgegevens consulteerbaar zijn door onbevoegden: belangrijke financiële schade voor het individu; geen aantoonbare blijvende impact op de levenskwaliteit; potentiële compensatie is mogelijk op basis van	3	Organisatie: 〉 Bijsturing van de criteria en/of maatregelen zijn noodzakelijk indien de integriteit geschonden wordt, maar dit is nog mogelijk binnen het lopende werkingsbudget. Personen: 〉 Er is materiële schade voor het individu indien de betrokken persoonsgegevens foutief zijn: belangrijke financiële schade voor het individu; geen aantoonbare blijvende impact op de levenskwaliteit; potentiële compensatie is mogelijk op basis van juridische dwangmaatregelen. 〉 Er is geen tot minimale immateriële schade voor het individu indien de betrokken persoonsgegevens foutief zijn.

	juridische dwangmaatregelen. 〉 Er is geen tot minimale immateriële schade voor het individu indien de betrokken persoonsgegevens consulteerbaar zijn door onbevoegden.		
	Organisatie: 〉 De informatie is toegankelijk voor een beperkte groep gebruikers. 〉 Bijsturing van de criteria en of maatregelen zijn noodzakelijk op korte termijn indien de vertrouwelijkheid geschonden is en reservering van bijkomende financiële middelen is hiervoor noodzakelijk. Personen: 〉 Er is materiële schade voor het individu indien de betrokken persoonsgegevens consulteerbaar zijn door onbevoegden: belangrijke financiële schade voor het individu en/of; aantoonbare blijvende impact op de levenskwaliteit; potentiële compensatie is mogelijk op basis van juridische dwangmaatregelen. 〉 Er is ernstige immateriële schade voor het individu indien de betrokken persoonsgegevens consulteerbaar zijn door onbevoegden. 〉 De fysieke integriteit (zelfstandigheid,		Organisatie: 〉 Bijsturing van de criteria en of maatregelen zijn noodzakelijk op korte termijn indien de integriteit geschonden is en reservering van bijkomende financiële middelen is noodzakelijk. Personen: 〉 Er is materiële schade voor het individu indien de betrokken persoonsgegevens foutief zijn: belangrijke financiële schade voor het individu en/of; aantoonbare blijvende impact op de levenskwaliteit; potentiële compensatie is mogelijk op basis van juridische dwangmaatregelen. 〉 Er is ernstige immateriële schade voor het individu indien de betrokken persoonsgegevens foutief zijn. 〉 De fysieke integriteit (zelfstandigheid, bewegingsvrijheid) van het individu wordt in zekere mate aangetast indien de betrokken persoonsgegevens foutief zijn.

	bewegingsvrijheid) van het individu wordt in zekere mate aangetast indien de betrokken persoonsgegevens consulteerbaar zijn door onbevoegden.		
5	Organisatie: 〉 De informatie is toegankelijk voor een selecte groep gebruikers. 〉 Bijsturing van criteria en/of maatregelen zijn noodzakelijk indien de vertrouwelijkheid geschonden is en dit vereist reservering van financiële middelen die de lopende en toekomstige budgetten overschrijden. 〉 Schending van de vertrouwelijkheid bedreigt het voortbestaan van de organisatie. Personen: 〉 Er is materiële schade aan het individu indien de betrokken persoonsgegevens toegankelijk zijn voor onbevoegden: beëindigen van de financiële autonomie; compensatie is onmogelijk. 〉 De fysieke integriteit (zelfstandigheid, bewegingsvrijheid) van het individu wordt in grote mate aangetast indien de betrokken persoonsgegevens consulteerbaar zijn door onbevoegden.	5	Organisatie: 〉 Er worden geen fouten in de informatie of wijziging door onbevoegden getolereerd. 〉 Bijsturing van criteria en/of maatregelen zijn noodzakelijk indien de integriteit geschonden is en dit vereist reservering van financiële middelen die de lopende en toekomstige budgetten overschrijden. 〉 Het voorkomen van fouten in de informatie bedreigt het voortbestaan van de organisatie. Personen: 〉 Er is materiële schade aan het individu indien de betrokken persoonsgegevens foutief zijn: beëindigen van de financiële autonomie; compensatie is onmogelijk. 〉 De fysieke integriteit (zelfstandigheid, bewegingsvrijheid) van het individu wordt in grote mate aangetast indien de betrokken persoonsgegevens foutief zijn.

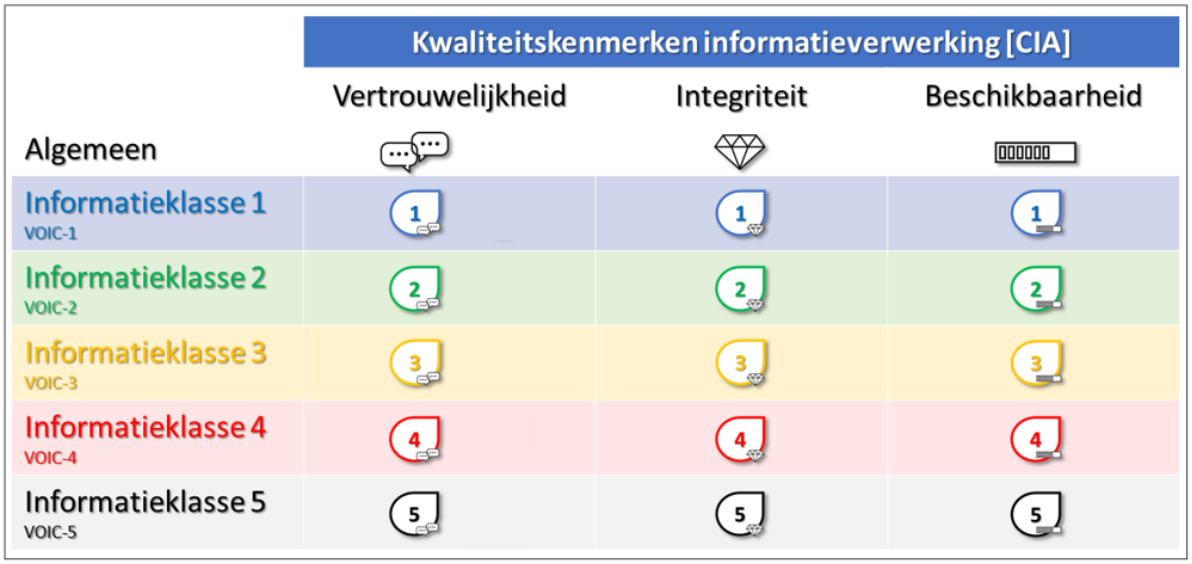
1.5.4. Informatieklassen voor beschikbaarheid

Beschikbaarheid wordt klassiek uitgedrukt in een percentage. Dit cijfer geeft de gewenste beschikbaarheid die overeenkomt met de behoeften gespecifieerd in de verwerkingsovereenkomst voor de betrokken toepassing of dienst. In deze overeenkomst zal het detail worden opgenomen hoe deze beschikbaarheid wordt berekend op basis van ongeplande onbeschikbaarheden. Naar analogie met vertrouwelijkheid en integriteit maken we gebruik van de 5 impactschalen om de verschillende klassen van beschikbaarheid aan te duiden:

Schaal	Beschikbaarheid
	De dienstverlening kan meer dan een maand onbeschikbaar zijn zonder significante gevolgen voor de organisatie of de burger. *En/of* Er is geen kritisch bedrijfsmoment waarop de dienstverlening beschikbaar moet zijn. *En/of* De onbeschikbaarheid treft weinig of geen gebruikers (bijvoorbeeld minder dan 5% van de doelgroep). *En/of* Niet-herstel van informatie heeft geen impact op de organisatie of de burger. *En/of* Performantieverlies heeft geen significante impact voor de organisatie of de burger.
	De dienstverlening mag niet langer dan een maand onbeschikbaar zijn. Is de dienstverlening langer dan 1 maand onbeschikbaar dan heeft dit significante gevolgen voor de organisatie of de burger. *En/of* Er is geen kritisch bedrijfsmoment waarop de dienstverlening beschikbaar moet zijn. *En/of* De onbeschikbaarheid treft een minimaal aantal gebruikers (bijvoorbeeld minder dan 20% van de doelgroep). *En/of* Informatie moet minstens gedeeltelijk hersteld kunnen worden. *En/of* Maximaal 75% performantieverlies is toegestaan.
	De dienstverlening mag incidenteel uitvallen, tot een week. Is de dienstverlening langer dan één week onbeschikbaar dan heeft dit significante gevolgen voor de organisatie of de burger. *En/of* Tijdens kritische bedrijfsmomenten mag de dienstverlening niet langer dan 24 uur onbeschikbaar zijn.

	En/of De onbeschikbaarheid treft een significant aantal gebruikers (bijvoorbeeld tot 50% van de doelgroep) of enkele prioritaire gebruikers (minder dan 10%). Elke entiteit bepaalt zelf de criteria voor een prioritaire gebruiker. *En/of* Informatie moet volledig hersteld kunnen worden tot een zekere datum. *En/of* Maximaal 50% performantieverlies is toegestaan.
	De dienstverlening kan quasi niet uitvallen, maximaal 72 uur. Is de dienstverlening langer dan 72 uur onbeschikbaar dan heeft dit significante gevolgen voor de organisatie of de burger. *En/of* Tijdens kritische bedrijfsmomenten mag de dienstverlening niet langer dan 12 uur onbeschikbaar zijn. *En/of* De onbeschikbaarheid treft een groot aantal gebruikers (bijvoorbeeld tot 75% van de doelgroep), of meerdere prioritaire gebruikers (bijvoorbeeld tot 25%). *En/of* Informatie moet volledig hersteld kunnen worden tot een datum op korte termijn. *En/of* Maximaal 20% performantieverlies is toegestaan.
	De dienstverlening mag enkel zeer uitzonderlijk uitvallen, tot 24 uur. Is de dienstverleningen langer dan 24 uur onbeschikbaar dan heeft dit significante gevolgen voor de organisatie of de burger. *En/of* Tijdens kritische bedrijfsmomenten mag de dienstverlening niet langer dan 2 uur onbeschikbaar zijn. *En/of* De onbeschikbaarheid treft een zeer groot aantal gebruikers (bijvoorbeeld meer dan 75% van de doelgroep) en meerdere prioritaire gebruikers (bijvoorbeeld meer dan 25%). *En/of* Informatie moet volledig hersteld kunnen worden tot het moment van onbeschikbaarheid. *En/of* Maximaal 5% performantieverlies is toegestaan.

1.5.5. Samenvatting van de schalen voor informatieclassificatie



	Kwaliteitskenmerken informatieverwerking [CIA]		
	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Algemeen			
Informatieklasse 1 VOIC-1	1	1	1
Informatieklasse 2 VOIC-2	2	2	2
Informatieklasse 3 VOIC-3	3	3	3
Informatieklasse 4 VOIC-4	4	4	4
Informatieklasse 5 VOIC-5	5	5	5

Om het gebruik in documentatie te vereenvoudigen krijgt elke schaal een unieke code onder vorm van een cijfer. Bovendien passen we een unieke kleurcode toe om de visuele herkenbaarheid te verbeteren. In de documentatie gebruiken we de terminologie informatieklassen om deze graden te groeperen.

- Referenties naar **Klasse 1**, krijgen een **blauwe** kleur
- Referenties naar **Klasse 2**, krijgen een **groene** kleur
- Referenties naar **Klasse 3**, krijgen een **oranje** kleur
- Referenties naar **Klasse 4**, krijgen een **rode** kleur
- Referenties naar **Klasse 5**, krijgen een **zwarte** kleur

1.6. Samengestelde informatiebronnen

Informatie is in de meeste gevallen een samenstelling van verschillende datasets en/of een samenstelling van verschillende informatietypes. In Bijlage I (Samengestelde informatiebronnen) wordt stap voor stap uitgelegd hoe de informatieklasse bepaling te werk gaat in het geval er meerdere datasets zijn.

2. Controlemaatregelen

2.1. Soorten controlemaatregelen

Controlemaatregelen worden opgedeeld in volgende types:

- Minimale algemene maatregelen
- Minimale specifieke maatregelen
- Aanvullende maatregelen

En we onderscheiden de volgende controlemaatregelen:

- Technische maatregelen;
- Organisatorische maatregelen, dit zijn alle maatregelen, processen en controles die de informatieverwerking in goede banen moeten leiden. In deze categorie sluiten we ook juridische controlemaatregelen en communicatie onder vorm van bewustmaking en training in.

Beide soorten maatregelen komen bij alle drie de types controlemaatregelen voor.

2.1.1. Minimale algemene maatregelen

Minimale algemene maatregelen zijn maatregelen die van toepassing zijn op alle informatieverwerking. Deze minimale maatregelen zijn rechtstreeks verbonden aan een informatieklasse. Ze vormen de baseline van de informatie veiligheidsmaatregelen. Deze maatregelen zijn gebaseerd op de ISO27001 en zorgen voor de basis van een veilig en gestructureerde informatieverwerking.

Opmerking: De minimale maatregelen bevatten mogelijk maatregelen in relatie tot de toestand van de informatie.

Opmerking: Maatregelen, op basis van andere standaarden, zijn mogelijk zolang het generieke maatregelen zijn.

2.1.2. Minimale specifieke maatregelen

De minimale algemene beveiligingsmaatregelen worden uitgebreid met minimale specifieke maatregelen afhankelijk van vereisten die voortkomen uit specifieke regelgeving. Zij vervolledigen de 'Minimale algemene maatregelen'. Minimale specifieke maatregelen hebben als oorsprong:

- Dezelfde IS027001, indien toegepast op een hogere informatieklasse;
- Maatregelen uit andere standaarden (ISO27017, ISO27018, PCI, …);
- Als antwoord op specifieke vereisten in wetgeving en/of regelgeving, bijvoorbeeld GDPR.

Opmerking: De specifieke maatregelen bevatten mogelijk maatregelen die niet zijn opgenomen in het ICR.

*De vereisten die de **GDPR-wetgeving** stelt aan de verwerking van persoonsgegevens, zijn beantwoord via minimale (GDPR) specifieke maatregelen. Gezien de generieke context van deze wetgeving zal de set van minimale (GDPR) specifieke maatregelen uitgewerkt worden binnen de generieke informatieclassificatie.*

2.1.3. Aanvullende maatregelen

Aanvullende maatregelen passen we toe op basis van:

- De verplichte risicoanalyse in informatieklasse 3;
- Het gebruik van alternatieve mitigerende maatregelen ter vervanging van minimale algemene en/of specifieke maatregelen.

Blijkt uit een risicoanalyse dat onaanvaardbare residuele risico's aanwezig zijn en dat aanvullende maatregelen nodig zijn om tot een aanvaardbaar restrisico te komen, dan is het aan de eigenaar van

de informatie om voor een correcte opvolging en rapportering te zorgen. Dit kan risicoacceptatie zijn, of mitigatie door extra maatregelen of overdracht van het risico. Merk op dat acceptatie van een risico door top management gebeurt.

Deze maatregelen zijn niet toegepast op de betrokken klasse op basis van de minimale maatregelen en specifieke criteria.

Aanvullende maatregelen komen voort uit een risicoanalyse.

In informatieklassen 1 en 2 werkt men enkel op basis van minimale algemene en minimale specifieke maatregelen.

2.2. Werkprincipes

Voor de toepassing van maatregelen gelden volgende basisprincipes:

- Algemene minimale maatregelen worden afgedwongen op basis van generieke informatieverwerkingscriteria.
- Specifieke minimale maatregelen hebben een directe relatie met criteria van toepassing op informatie met specifieke contextcriteria. Deze criteria kunnen zowel een relatie hebben met de aard van informatie (vb. GDPR en persoonsgegevens) of een relatie hebben met specifieke data sets (maatregelen gespecifieerd in een overeenkomst). In het ICR wordt enkel GDPR opgenomen onder specifieke minimale maatregelen; de andere specifieke minimale maatregelen zijn organisatie-afhankelijk en worden door de entiteiten zelf bepaald op basis van de voor hun toepasselijke regelgeving.
- Aanvullende maatregelen zijn in tegenstelling tot minimale maatregelen niet afdwingbaar, maar worden toegepast na een risicoanalyse. Hierbij reduceert, verplaatst of aanvaardt men de restrisico's die worden geïdentificeerd na toepassing van de algemene en specifieke minimale maatregelen.
- Het principe van gestapelde maatregelen impliceert dat de minimale maatregelen van de onderliggende informatieklasse ook op de bovenliggende klassen van toepassing blijven, met uitzondering van onverenigbare maatregelen. Deze uitzonderingen zijn expliciet opgenomen in de documentatie.
- De GDPR vormt de basis voor de Minimale Normen van de KSZ (Kruispuntbank van de Sociale Zekerheid), de maatregelen van de GDPR en KSZ kunnen dan ook beschouwd worden als gestapeld, d.w.z. alle GDPR-maatregelen van een informatieklasse zijn ook KSZ-maatregelen in dezelfde informatieklasse.
- Informatie en informatiedragers worden verder in dit document algemeen als middelen (assets) genoemd.
- Maatregelen worden functioneel beschreven, niet technisch.
- In uitzonderlijke gevallen kunnen minimale algemene en/of minimale specifieke maatregelen niet worden toegepast om organisatorische of technische redenen. Mits afspraken met de betrokken regulerende organisatie kunnen alternatieve maatregelen die de rest risico's op gelijkwaardige manier afdekken, worden voorgesteld. Dit gebeurt altijd op basis van een risicoanalyse en met goedkeuring van topmanagement (leidend ambtenaar of directeur), aansprakelijk voor de informatie.

2.3. Relatie tussen de maatregelen en informatieveiligheid

Deze paragraaf geeft een globaal overzicht van de maatregelen en van het beoogde doel in verband met informatieveiligheid.

Voor alle doelstellingen in onderstaande tabel geldt dat de van toepassing zijnde maatregelen worden gedefinieerd, geïmplementeerd, uitgevoerd en gemonitord op effectiviteit. De uitvoering van bepaalde operationele activiteiten kunnen uitbesteed zijn aan externe dienstenleveranciers. Hier geldt dat de entiteit aansprakelijk blijft en er zorg voor dient te dragen dat er duidelijke afspraken zijn gemaakt met dienstenleveranciers betreffende informatieveiligheid en dat de entiteit toezicht uitoefent op deze leveranciers. Een dienstenleverancier is niet altijd een externe partij van buiten de Vo, maar kan ook een interne dienstverlener zijn, zoals Digitaal Vlaanderen is voor andere Vo entiteiten.

Onderwerp	Doelstellingen
Informatieveiligheidsbeleid	Het verschaffen van directieaansturing van, en -steun voor, informatieveiligheid in overeenstemming met bedrijfseisen en relevante wet- en regelgeving. Dit omvat o.a. de opvolging en vertaling van het Vo-brede beleid (Informatieclassificatieraamwerk level 2) in concreet informatieveiligheidsbeleid op entiteitsniveau (level 3 en 4). Het volgende Vo organisatiedocument beschrijft de verschillende levels. ***Referentie: Informatieclassificatie Organisatie - Informatieclassificatieraamwerk***
Organisatie van informatieveiligheid	Opzetten van een kader om de implementatie en uitvoering van informatieveiligheid binnen de entiteit te initiëren en te beheersen. Dit omvat o.a. het definiëren van de governance en rollen en verantwoordelijkheden voor informatieveiligheid binnen de entiteit.
Veilig personeel	Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en uitvoeren in relatie tot informatieveiligheid. Dit omvat o.a. screening, vertrouwelijkheidsclausule in contracten, bewustzijn campagnes, training en een disciplinaire procedure.
Beheer van bedrijfsmiddelen en informatie	Bedrijfsmiddelen van de organisatie identificeren, classificeren en beheren in lijn met het Vo Informatieclassificatieraamwerk. Dit omvat o.a. inventarisatie van de assets, vaststellen eigenaarschap, definiëren van aanvaardbaar gebruik, classificatie, labelen, veilige opslag en vernietiging van informatie.
Toegangscontrole van informatie	Toegang tot informatie en informatie verwerkende faciliteiten beperken tot alleen bevoegde gebruikers. Dit omvat o.a. voor iedere applicatie duidelijk beleid en eigenaarschap van toezicht op de toegang, een registratieproces, beheer van speciale rechten, veilige distributie van authenticatie-informatie, regelmatige beoordeling van rechten en veilige inlogprocedures. Verschillende activiteiten van toegangsbeheer kunnen uitbesteed zijn aan externe leveranciers of maken gebruik van centrale authenticatiediensten. De eigenaar binnen de Vo entiteit blijft echter verantwoordelijk voor het regelmatig beoordelen van de toegangslijst met actieve gebruikers van de applicatie(s) van de entiteit.

	Referentie: ***Minimale maatregelen Toegangsbeheer*** ***Referentie:*** ***Minimale maatregelen Identity & access management*** ***Referentie:*** ***Minimale maatregelen Privileged access management***
Versleuteling van informatie	Het zorgen voor correct en doeltreffend gebruik van versleuteling om de vertrouwelijkheid, authenticiteit en integriteit van informatie te beschermen. Dit omvat o.a. cryptografisch beleid en sleutelbeheer in samenwerking met architectuurstandaarden en IT-afdeling(en). ***Referentie:*** ***Minimale maatregelen Cryptografie***
Fysieke beveiliging	Het voorkomen van verlies, schade, diefstal, onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de entiteit. Dit omvat o.a. fysieke beveiligingsmaatregelen en toegangscontrole, speciale zones, clear desk beleid, bekabeling en bescherming van apparatuur binnen en buiten kantoren of bedrijfsterreinen. ***Referentie:*** ***Minimale maatregelen Fysieke maatregelen***
Operationele beveiliging en communicatiebeveiliging	Het waarborgen van correcte en veilige bediening van informatieverwerkende faciliteiten. Dit omvat verantwoordelijkheden zoals wijzigingsbeheer, capaciteitsbeheer, scheiding van test en productiesystemen, backups, maatregelen tegen malware en softwarekwetsbaarheden, logging, et cetera. Het waarborgen van de bescherming van informatie in netwerken en het handhaven van de beveiliging van informatie die wordt uitgewisseld. Dit omvat o.a. beheersmaatregelen voor netwerken zoals firewalls, inspectie van verkeer, veilige routeringsoplossingen, scheiding in netwerken en het versleutelen van elektronische berichtenverkeer. De uitvoering van operationele activiteiten kunnen uitbesteed zijn aan externe dienstenleveranciers. De entiteit blijft aansprakelijk voor de informatie en dient ervoor te zorgen dat er duidelijke afspraken zijn gemaakt met de externe partij betreffende informatieveiligheid. Daarnaast kunnen er transversale gestandaardiseerde beheerprocessen zijn waarmee applicaties op dezelfde uniforme manier beheerd worden. ***Referentie:*** ***Minimale maatregelen Asset en configuratiebeheer*** ***Referentie:*** ***Minimale maatregelen Wijzigingsbeheer*** ***Referentie:*** ***Minimale maatregelen Netwerken***
Veilige ontwikkeling van informatiesystemen	Het waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus en het bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus (projecten) van informatiesystemen. Dit omvat o.a. opstellen van beveiligingseisen, beleid voor veilige softwareontwikkeling en ontwikkelomgeving, procedures voor wijzigingsbeheer en releases, systeemtesten, acceptatietesten en de bescherming van testgegevens. ***Referentie:*** ***Minimale maatregelen Ontwikkeling van toepassingen***

	Referentie: Minimale maatregelen Release en deployment beheer ***Referentie: Minimale maatregelen Veiligheidstesten***
Veiligheidsafspraken met leveranciers	Het waarborgen van de bescherming van bedrijfsmiddelen van de entiteit die toegankelijk zijn voor leveranciers en het handhaven van de overeengekomen informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten. Dit omvat o.a. inbedding van eisen in contracten, inzicht in de leveranciersketen, monitoren en beoordelen van de beveiligingsaspecten van de dienstverlening en het beheer van veranderingen in de externe dienstverlening.
Informatieveiligheidsincidenten	Het bewerkstelligen van een consistente en doeltreffende aanpak van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging. Dit omvat o.a. de beschrijving van rollen en verantwoordelijkheden, rapportering van gebeurtenissen en zwakke plekken, beoordeling en besluitvorming over gebeurtenissen, response op incidenten, lering trekken uit incidenten en het verzamelen van bewijsmateriaal. ***Referentie: Minimale maatregelen Beheer van gebeurtenissen*** ***Referentie: Minimale maatregelen Incidentbeheer*** ***Referentie: Minimale maatregelen Probleembeheer***
Bedrijfscontinuïteit	De inbedding van continuïteit in de systemen van de entiteit en het bewerkstelligen van beschikbaarheid van informatieverwerkende faciliteiten. Dit omvat o.a. continuiteits- en disaster recovery plannen, high-availability oplossingen, het testen van de plannen en het evalueren en bijsturen van de plannen.
Naleving van informatieveiligheidsbeleid	Het voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen die van toepassing zijn op de entiteit. Dit omvat o.a. het identificeren van toepasselijke wetgeving en contractuele eisen, intellectuele-eigendomsrechten, beschermen van registraties, bescherming van persoonsgegevens en privacy en voorschriften voor gebruik van cryptografie (i.v.m. mogelijke juridische beperkingen). Ten slotte, het verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met het beleid van de Vlaamse overheid zoals vastgelegd in het Informatieclassificatieraamwerk.

2.4. Beschrijving technische maatregelen

Netwerken

Het document 'Minimale maatregelen – Netwerken' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader van beveiliging van netwerken.

ICT-systemen

Het document 'Minimale maatregelen – ICT-systemen' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader van beveiliging van ICT-systemen (servers, middleware, enz).

Cryptografie

Het document 'Minimale maatregelen – Cryptografie' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader van beveiliging door middel van cryptografische middelen. Hiertoe behoren ook maatregelen voor sleutelbeheer.

Fysieke beveiliging

Het document 'Minimale maatregelen – Fysische maatregelen' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader van fysieke beveiligingsmaatregelen.

2.5. Beschrijving procedurele maatregelen

IAM (*identity & access management*)

Het document 'Minimale maatregelen – IAM' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader van identificatie, authenticatie en autorisatie.

Ontwikkeling & gebruik van toepassingen

Het document 'Minimale maatregelen – Netwerken' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader van software development lifecycle.

Risicobeheer

Er zijn 3 documenten uitgewerkt voor het beheer van risico's, het uitvoeren van risicoanalyses en de methodiek voor het uitvoeren van risicoanalyses.

SIEM (*security incident & event management*)

Het document 'Minimale maatregelen – SIEM' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader van beveiliging door middel van logging en monitoring.

PAM (*privileged access management*)

Het document 'Minimale maatregelen – PAM' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader van beheer van geprivilegieerde accounts.

2.6. Beschrijving servicemanagement

2.6.1. ITIL en procesmatig werken

Veel organisaties werken ad hoc en zitten nog volop in de groeifase van proces maturiteit. Door procesmatig te werken wordt structuur aangebracht en wordt een cultuur van continue verbetering opgezet, met het oog op klanttevredenheid, doelmatig werken en efficiëntie. Perceptie, kwaliteit en communicatie staan hierin centraal.

Wanneer een proces op deze wijze wordt beschreven, wordt het inzichtelijk en begrijpelijk. De verantwoordelijkheden en bevoegdheden van medewerkers worden zichtbaar gemaakt en elke activiteit wordt duidelijk.

Activiteiten binnen het proces kunnen snel en efficiënt worden uitgevoerd zonder veel verstoringen en te hoge risico's voor de organisatie. Immers, bij het optreden van een verstoring kan de medewerker zien waar dit in het proces gebeurt en kan hij/zij vervolgens actie nemen.

Procesmatig werken is in de wereld van ICT-beheer goed ingeburgerd. Vooral dankzij ITIL hebben ICT gedreven afdelingen procesmatig leren werken. Processen lopen doorheen meerdere afdelingen en teams en door procesmatig te werken kan een goed eindresultaat bereikt worden. Processen, zoals incident beheer, wijzigingsbeheer en servicemanagement zij dan ook onontbeerlijk voor elke organisatie.

Processen dienen zelf ook beheerd, en waar nodig verbeterd, te worden. Alleen een proces beschrijven levert niets meer op dan een papier in een kast. Om een proces goed te laten draaien in de organisatie moet het proces niet alleen beschreven zijn, maar moeten de medewerkers die een rol spelen in een proces opgeleid worden. Daarnaast zijn prestatie-indicatoren over het proces nodig om de kwaliteit te monitoren en moet er regelmatige nagekeken worden of de uitvoering en de beschrijving van het proces met elkaar kloppen. Het management zal bovendien de uitkomsten van prestatie-indicatoren en reviews moeten gebruiken om de kwaliteit van het proces bij te sturen.

Vele (kleine) organisaties vrezen dat procesmatig werken veel investering vraagt in termen van tijd, opleiding en opvolging, waardoor dit voor hen te hoog gegrepen is. Echter, processen hoeven niet complex of ingewikkeld in mekaar zitten en ITIL hoeft niet in alle details geïmplementeerd te worden. Zo zal het proces incident beheer voor een grote organisatie er heel anders uitzien dan voor een kleine organisatie: crisis cel, incident response team en andere functies spelen dan wel een rol in de grote organisaties, voor kleine organisaties is het vooral van belang dat de activiteiten die typisch toegewezen zijn aan deze teams, op één of andere wijze en passend bij de organisatie uitgevoerd worden. Een grote organisatie moet immers meer en strikter regelen om werkbaar te blijven dan een kleine organisatie: het aantal management lagen verschilt, er zijn minder soorten functies en specialismen en de communicatie loopt anders.

2.6.2. ITIL-processen in het ICR

Asset & configuratiebeheer

Het document '[Minimale maatregelen – Asset en configuratiebeheer]' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader het proces voor beheer van middelen. Dit is het proces dat alle componenten van de IT-infrastructuur en de daaraan gerelateerde documentatie onder controle brengt en houdt ter ondersteuning van de overige servicemanagementprocessen.

Beheer aanvragen

Het document 'Minimale maatregelen – Beheer aanvragen' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader het proces voor beheer van aanvragen. Het proces dat de primaire afhandeling van gebruikers vragen verzorgt.

Beheer gebeurtenissen

Het document 'Minimale maatregelen – Beheer gebeurtenissen' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader het proces voor beheer van gebeurtenissen ('events').

Incident beheer

Het document 'Minimale maatregelen – Incident beheer' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader het proces voor beheer van incidenten. Dit beschrijft het proces dat de primaire afhandeling van verstoringen verzorgt.

Probleembeheer

Het document 'Minimale maatregelen – Probleem beheer' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader het proces voor beheer van problemen. Dit proces zoekt de oorzaak van die incidenten waarvoor incident management geen oplossing heeft. Probleem beheer analyseert incident informatie en levert work-arounds voor incident management zodat aan de gebruiker een tijdelijk herstel van dienstverlening kan worden geboden.

Release & deployment beheer

Het document 'Minimale maatregelen – release en deployment beheer' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader het proces voor beheer en uitrol van nieuwe releases. Dit proces draagt op een systematische wijze zorg voor de invoering van grote en/of cruciale veranderingen in de IT-infrastructuur.

Toegangsbeheer

Het document 'Minimale maatregelen – Toegangsbeheer' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader het proces voor beheer van gebruikerstoegang.

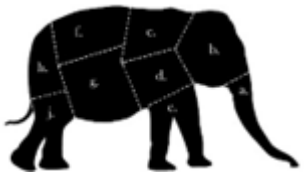
Wijzigingsbeheer

Het document 'Minimale maatregelen – Wijzigingsbeheer' beschrijft de maatregelen die genomen worden per klasse voor beschikbaarheid, integriteit en vertrouwelijkheid in het kader het proces voor beheer van wijzigingen. Dit beschrijft het uitvoeren van wijzigingen op een gecontroleerde wijze zodat verstoringen en afwijkingen van het overeengekomen dienstenniveau als gevolg van deze wijzigingen zo min mogelijk voorkomen.

Bijlage I: Samengestelde informatiebronnen

Informatie is in de meeste gevallen een samenstelling van verschillende datasets en/of een samenstelling van verschillende informatietypes. Met dit gegeven in het achterhoofd moeten we de structuur van de generieke informatieclassificatie toepassen om de correcte informatieclassificatie en achterliggende applicatie en infrastructuur componenten in zijn geheel te bepalen.

Vereenvoudiging van de classificatie



Het is niet altijd zo eenvoudig om een correcte classificatie te maken van informatie gezien de potentiële complexiteit van de verwerking en/of de toe te passen criteria.

We benaderen dit op de spreekwoordelijke ‘eating an elephant’ manier. We verdelen de hap in verteerbare porties.

Om de informatieclassificatie gemakkelijker toe te passen, breken we de informatie op in elementaire logische informatie-elementen of types. Deze elementaire informatie-elementen kunnen individueel gemakkelijker geëvalueerd worden.

Begeleidende documentatie

Als begeleiding zal er een gestandaardiseerde lijst van vooraf geklasseerde informatie types worden gepubliceerd om de uniformiteit binnen de Vo en de lokale besturen te faciliteren. Deze lijst bevat de minimale informatieclassificatie voor het betrokken informatie type waaraan de verwerkers van de informatie zich verplichten.

(Zie bronnen)

In stappen

Stap 1: Identificatie van de individuele informatietypes

Opsplitsen van de informatie in individuele informatie-elementen of informatietypes. Dit kan een recursief proces zijn afhankelijk van het detailniveau dat men wil bekomen.

Stap 2: Evaluatie van de individuele informatie-elementen of informatietypes

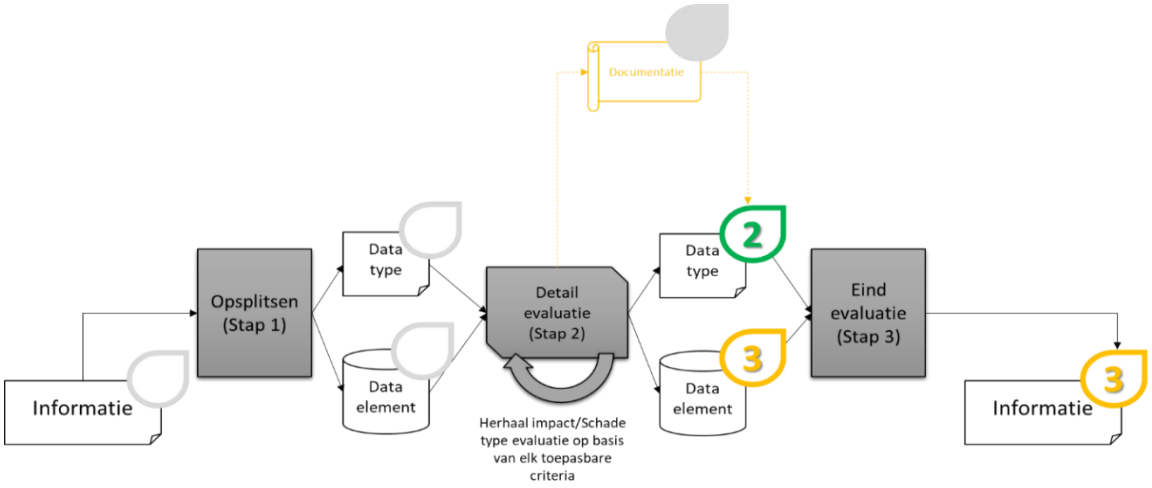
Men evalueert elk individueel informatie-element en/of type op basis van de impact of schade en kent een score toe met een impact/schade categorie. De maximale score zal hierbij weerhouden worden als score voor het geheel van de samengestelde informatie-elementen en/of informatie types.

Stap 3: Evaluatie van de informatie

Na het evalueren van de individuele impact of schade op basis van de verschillende schade types weerhouden we de hoogste score van de individuele evaluatie van de informatie-elementen en/of informatie types als score voor de volledige informatie set.

Grafisch overzicht van de vereenvoudiging

Stap 1 & 2: Opdelen in data-elementen en de detailevaluatie



Stap 3: Eindevaluatie

Informatieclassificatie	Impact of schade	1	2	3	4	5
Informatie-element/type 1	Fysiek	☑				
	Financieel		☑			
	Economisch		☑			
	Geestelijk	☑				
	Vrijheidsbeperking	☑				
	Fysische schade	☑				
	Sociale schade	☑				
	Reputatie schade		☑			
	Evaluatie		☑			
Informatie-element/type N	Fysiek	☑				
	Financieel			☑		
	Economisch		☑			
	Geestelijk		☑			
	Vrijheidsbeperking	☑				
	Fysische schade	☑				

	Sociale schade	☑				
	Reputatie schade			☑		
	Evaluatie			☑		
Informatie	**Eindevaluatie**			☑		