Informatieclassificatie Vlaamse overheid (Vo-ICR)

Informatieveiligheid

ORGANISATIE

Team Informatieveiligheid| Digitaal Vlaanderen

Dit is een document voor publiek gebruik

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

Classificatie: Klasse 2

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 de processen in relatie tot de beveiliging van informatieverwerking binnen de verschillende Vo entiteiten. Het beschrijft de criteria voor informatieveiligheid, de opbouw van documentatie en het beheer van het informatieclassificatieraamwerk.

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

Zoals we in het hoofdstuk 'informatieveiligheid versus bescherming van persoonsgegevens' aangeven, is er een verschil tussen beide en dit vertaalt zich ook in verschillende contactpunten:

- Het Team Informatieveiligheid buigt zich over het informatieclassificatieraamwerk en kan gecontacteerd worden via security@vlaanderen.be
- Vragen in het kader van AVG kunnen gericht worden aan de DPO (functionaris gegevensbescherming) van de eigen organisatie of de DPO van Digitaal Vlaanderen. Er is ook de mogelijkheid om beroep te doen op het Bureau voor Gegevensbescherming van Agentschap Digitaal Vlaanderen. Voor informatie hieromtrent kan je terecht op Bureau voor Gegevensbescherming | 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	1 augustus 2022	Kristel Van Aken	Opsplitsen doc organisatie als onderdeel van ICR2.0
V2.1			NVT
V2.2	3 mei 2023	Kristel Van Aken	CISO rol toegevoegd

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 categorieen persoonsgegevens / 19 januari 2018
- Bestuursdecreet: https://codex.vlaanderen.be/PrintDocument.ashx?id=1030009&datum=&geannoteerd=false&print=false

Inhoudsopgave

INLEIDING

Binnen de Vlaamse overheid (hierna afgekort als “Vo”) is het besef gegroeid dat informatieveiligheid geen alleenstaande opdracht is die door een entiteit op zichzelf kan worden aangegaan. Dit besef heeft geleid tot een Vo-brede strategie en beleid voor informatieveiligheid, goedgekeurd en bekrachtigd door de Vlaamse regering. Betere samenwerking tussen de Vo-entiteiten en een consistente, gecoördineerde aanpak van informatiebeveiliging sluit de rangen tegen cyberaanvallen en zorgt voor een niveau van informatieveiligheid dat beantwoordt aan de noden van de entiteit en van de informatie die het beschermt.

De strategie voor informatieveiligheid houdt een Vo-breed informatieveiligheidsbeleid in, onder vorm van het Vo-informatieclassificatieraamwerk (ICR). Dit raamwerk is eveneens bekrachtigd door de Vlaamse regering en is aldus bindend voor alle entiteiten die behoren tot de Vo-administratie zoals beschreven in het bestuursdecreet.

Dit document maakt onderdeel uit van een set van documenten over het ICR. Er zijn twee documenten die de context en de werking van het ICR beschrijven:

- Het huidige document geeft het brede kader weer rond informatieveiligheid, beschrijft de verschillende niveaus van documentatie en documenteert de processen voor beheer van het ICR. Het geeft bovendien inzicht in het raamwerk, hoe het tot stand komt en wie het beheert. Dit document is belangrijk voor iedereen binnen een entiteit met verantwoordelijkheid op het gebied van informatieveiligheid, dus met name leidinggevend topkader, de CISO, de DPO, de eigenaar en gedelegeerd eigenaar.
- Het tweede document, genaamd ‘Vo informatieclassificatie – Organisatie Informatieclassificatieraamwerk’, beschrijft het raamwerk zelf, de verschillende klassen, het principe van de minimale maatregelen en hoe het raamwerk moet worden toegepast. Dit document is belangrijk voor wie het raamwerk moet implementeren, dus met name de CISO en uitvoerders.

1. Informatieveiligheid

1.1. Informatieveiligheid en haar plaats in de organisatie

1.1.1. Informatieveiligheid en beleid

Informatieveiligheid gaat over het beveiligen van informatie. Waarom is dit zo belangrijk? Cybercriminelen worden steeds slimmer en hebben ook steeds meer tools ter beschikking om hun doelen te bereiken. Als overheid moeten we daarnaast ook het voorbeeld geven en ervoor zorgen dat de informatie van haar burgers en van de eigen organisatie beschermd is.

Informatiebeveiliging is een werkwoord. Het vraagt om voortdurende aandacht in alle lagen van de organisatie. Het beperkt zich dus niet tot één (ICT) afdeling of tot louter technische maatregelen maar vraagt een zorgvuldige inbedding in de organisatie.

Het informatieclassificatieraamwerk of afgekort ICR is gemeenschappelijk voor alle entiteiten van de Vlaamse administratie. Het dient dus als basis voor het eigen informatieveiligheidsbeleid van elke entiteit.

1.1.2. Informatieveiligheid en haar kwaliteitskenmerken

De beveiliging van informatie houdt in dat zij beschermd wordt tegen onbevoegde toegang en verwerking, waarbij er maatregelen worden genomen om volgende kwaliteitskenmerken te garanderen:

- Vertrouwelijkheid: de gegevens zijn alleen toegankelijk voor geautoriseerde personen en entiteiten of voor de juiste processen;
- Integriteit: de juistheid en volledigheid van gegevens;
- Beschikbaarheid: op het gewenste moment toegang hebben tot gegevens en erover kunnen beschikken.

Dit zijn de 3 kenmerken die we hanteren in het ICR. Ze worden verder uitgediept in het document 'Vo informatieclassificatie – organisatie informatieclassificatieraamwerk'.

Merk op dat er vaak nog 2 andere kenmerken worden gehanteerd (maar deze zijn niet expliciet opgenomen in het ICR):

- Authenticiteit: de mate van betrouwbaarheid van de originaliteit en herkomst van de gegevens;
- Onweerlegbaarheid: het kunnen aantonen dat een actie of een gebeurtenis effectief plaatsvond.

Eveneens is het begrip auditeerbaarheid belangrijk, m.a.w. het opspoorbaar zijn van handelingen en activiteiten door bevoegde (of onbevoegde) personen.

In het domein van informatieveiligheid staan vragen centraal zoals: Wie heeft toegang tot welke informatie en wanneer? Zijn de activiteiten, bij het opvragen van informatie, traceerbaar (en dus auditeerbaar)? Hoe beveiligen we de opslag en de uitwisseling van gevoelige informatie tussen verschillende partijen? Wat zijn onze beveiligingsrisico's en welke maatregelen kunnen we nemen om de risico's te verminderen en te beantwoorden aan de wetgeving? Hoe kunnen we aantonen dat onze organisatie informatiebeveiliging onder controle heeft? Hoe realiseren we informatiebeveiliging op een effectieve, efficiënte (en kostenefficiënte) manier? Wie is verantwoordelijk voor wat?

Het ICR biedt hierop een antwoord door middel van de classificatie van informatie en de daaraan gekoppelde controlemaatregelen.

1.1.3. Informatieveiligheid versus informatiebeveiliging

De begrippen ‘informatieveiligheid’ en ‘informatiebeveiliging’ worden vaak simultaan gebruikt. Er is echter een verschil tussen beide begrippen: om informatieveiligheid (doel) te waarborgen, wordt gebruik gemaakt van informatiebeveiliging (maatregelen).

De Vo kiest overwegend voor de term ‘informatieveiligheid’, omdat deze term in de perceptie meer recht doet aan de breedte van het onderwerp dan de term ‘informatiebeveiliging’, dat vaak wordt geassocieerd met ICT.

1.1.4. informatieveiligheid versus bescherming van persoonsgegevens

Vaak worden informatieveiligheid en bescherming van persoonsgegevens als hetzelfde beschouwd. Dat is begrijpelijk, want er zijn verschillende raakvlakken. Zo speelt de risico gebaseerde aanpak, waarbij op basis van een risicoanalyse maatregelen worden geselecteerd om de veiligheid van de gegevens te borgen, binnen beide domeinen een centrale rol. En beide domeinen zijn erop gericht om informatieveiligheidsrisico’s te verkleinen. Maar er zijn ook verschillen:

- De aard van de risico’s: zowel bescherming van persoonsgegevens als informatieveiligheid beoogt risico’s terug te brengen tot een aanvaardbaar niveau. Maar er zit een verschil in de aard van die risico’s. Bij bescherming van persoonsgegevens draait het om risico’s die impact hebben op mensen. Bij informatieveiligheid draait het niet om de impact voor individuen, maar om het beheersen van bedrijfsrisico’s: informatieveiligheid gaat dan over het beschermen van informatie om de bedrijfsvoering te kunnen garanderen. Oftewel, hoe ervoor zorgen dat de juiste mensen en systemen toegang hebben tot de juiste informatie op het juiste moment.
- Al dan niet aanvaarden van risico’s: bij het beheersen van risico’s wordt er bekeken of er al dan niet actie moet worden genomen. Organisaties bepalen zelf hoeveel risico zij bereid zijn om te nemen. Sommige organisaties zijn risico avers en zullen er alles aan doen om deze bedrijfsrisico’s zo klein mogelijk te houden. Andere organisaties hebben een grotere risico appetijt en zijn bereid om meer risico te accepteren, als daar een potentieel voordeel tegenover staat. Binnen de Vo moet risicoacceptatie op het juiste managementniveau gebeuren afhankelijk van het risico; indien een risico rechtstreeks impact heeft op andere Vo entiteiten moet hiermee rekening worden gehouden. De afweging hoeveel bedrijfsrisico wordt genomen is dus aan de Vo zelf. Gaat het echter over bescherming van persoonsgegevens, dan geldt er strikte wetgeving, namelijk de AVG. Het accepteren van risico’s voor persoonsgegevens zou een directe inbreuk van de AVG kunnen betekenen, waardoor het geen optie meer is om die risico’s te accepteren. Organisaties zullen in die gevallen dan noodgedwongen moeten kiezen voor het vermijden of verkleinen van risico’s.

Natuurlijk zijn er ook raakvlakken: waar een organisatie technische en organisatorische maatregelen inricht om bedrijfsinformatie te beschermen, zijn die er ook om persoonsgegevens die de organisatie verwerkt, te beveiligen.

Bij bescherming van persoonsgegevens staat dus veel meer de mens (persoon van wie gegevens opgeslagen/verwerkt worden) centraal, waar bij informatiebeveiliging de gegevens zelf en de verantwoordelijke organisatie centraal staan.

Binnen organisaties zien we dan ook vaak dat verschillende partijen zich bezighouden met informatieveiligheid dan wel bescherming van persoonsgegevens: informatieveiligheid is het domein van de CISO (Chief Information Security Officer) terwijl de DPO (Data Protection Officer) zich buigt over de bescherming van persoonsgegevens en conformiteit met de betreffende wetgeving. Men zou

kunnen stellen dat de technisch/organisatorische bescherming van informatie en persoonsgegevens het domein is van de CISO terwijl de conformiteit met AVG het werkgebied is van de DPO.

1.2. Informatieveiligheid volgens een informatieclassificatie

Zoals we al hebben verduidelijkt, is informatieclassificatie een belangrijke basis voor informatiebeveiliging. Door het indelen van informatie in een klasse, wordt het duidelijk welke maatregelen moeten worden genomen om deze informatie te beveiligen. Zo garanderen we dat er voldoende, maar niet overmatig maatregelen worden genomen. Het zou immers jammer zijn om middelen te veel te investeren in informatie die publiek beschikbaar mag zijn of anderzijds te weinig maatregelen te voorzien waardoor gevoelige informatie het gevaar loopt in handen te vallen van verkeerde mensen. Het document 'Vo informatieclassificaite – organisatie informatieclassificatieraamwerk' is volledig gewijd aan informatieclassificatie zoals dit binnen de Vlaamse administratie wordt geregeld.

2. Rollen en verantwoordelijkheden

De identificatie van rollen en verantwoordelijkheden, voor het beheer van informatieveiligheid, zorgt voor helderheid, voorkomt conflicten en vaagheid. Hiervoor gebruiken we een RACI model met de volgende rollen: verantwoordelijke ('Responsible'), aansprakelijke ('Accountable'), geconsulteerde ('Consulted') en geïnformeerde ('Informed').

We identificeren eigenaar, gedelegeerd eigenaar en uitvoerder. In het RACI model is een eigenaar aansprakelijk ('Accountable') en zijn de gedelegeerd eigenaar en de uitvoerder verantwoordelijk ('Responsible'). Merk op dat rollen steeds toegewezen worden aan een unieke persoon op basis van zijn/haar organisatorische functie. De entiteiten zijn verantwoordelijk voor de autonome toewijzing van functies, rollen en verantwoordelijkheden binnen de eigen entiteit.

2.1. RACI-model en eigenaarschap

Voor het beheer en onderhoud van het ICR geldt volgende:

	Verantwoordelijke (Uitvoerder) (Responsible)	**Aansprakelijke** (Accountable)	**Raadpleging** (Consulted)	**Informeren** (Informed)
Ontwikkeling en beheer van het ICR	Voorzitter Werkgroep Informatieveiligheid	Voorzitter van het Stuurorgaan Vlaams Informatie- en ICT-beleid	Leden van het Stuurorgaan Vlaamse Informatie- en ICT-beleid Leden van de Werkgroep Informatieveiligheid	Toezichthouders

Voor het implementeren van het ICR in elke entiteit geldt volgende:

Informatie-classificatie	(gedelegeerd) eigenaar of uitvoerder	eigenaar	DPO (*) CISO (*)	Leden van het Stuurorgaan Vlaams Informatie- en ICT-beleid
Toepassen van maatregelen	(gedelegeerd) eigenaar of uitvoerder Uitbesteding aan externe leverancier mogelijk mits expliciet toezicht en controle door de organisatie	Eigenaar	DPO (*) CISO (*)	Leden van het Stuurorgaan Vlaams Informatie- en ICT-beleid

DPO: Data Protection Officer
CISO: Chief Information Security Officer

2.2. De rol van CISO

2.2.1. CISO als verplichte rol

De uitdagingen waarmee de Vlaamse overheid geconfronteerd wordt op gebied van informatieveiligheid, worden steeds groter, mede door de snelle digitalisering, geopolitieke veranderingen en de voortschrijdende technologische evoluties. Het is dan ook niet verwonderlijk dat de nood aan een adviserende, coördinerende en sturende rol in de organisatiestructuur toeneemt.

Het Stuurorgaan heeft dan ook tijdens de zitting van 17 april 2024 beslist om de rol van CISO verplicht te maken voor alle entiteiten onder haar bevoegdheid. Deze beslissing werd geïntegreerd in de ICR documentatie van Juni 2024.

De term CISO staat voor 'Chief Information Security Officer' en is een gebruikelijke en goed gekende rol in de wereld van informatieveiligheid. Chief Information Security Officer is de referentie die gehanteerd wordt naar het in te vullen takenpakket, maar de entiteiten hebben de vrijheid om zelf de titelvoering te kiezen.

CISO moet minimaal als rol ingevuld worden, maar een entiteit kan de rol als functie definiëren. Dat geeft de entiteiten meer mogelijkheden om het bijhorende takenpakket in te vullen volgens de noden en mogelijkheden van hun organisatie.

De aanduiding van een CISO gebeurt steeds door de desbetreffende entiteit en kan door het aanduiden van een personeelslid dat reeds in dienst is, een aanwerving of door een externe medewerker. Eén persoon kan ook voor meerdere entiteiten de rol van CISO uitvoeren voor zover er geen belangenconflicten optreden.

Er moet een centraal register (onder toezicht van het Stuurorgaan) zijn voor de CISO's, bijvoorbeeld in het kader van crisiscommunicatie.

2.2.2. Plaats van de CISO in de organisatie

Om optimale informatiebeveiliging mogelijk te maken is het raadzaam dat de CISO over het juiste mandaat, middelen en budget beschikt. De CISO heeft een mandaat nodig om beslissingen te kunnen nemen binnen het kader van zijn/haar werkzaamheden, en budget/middelen om activiteiten waar te maken.

De CISO werkt op strategisch en tactisch niveau. Het is dan ook belangrijk dat de CISO een onafhankelijke positie in de organisatie kan bekleden, waarbij de belangen van bijvoorbeeld een afdelingshoofd of dienstenleverancier niet mee mogen wegen als het gaat om onafhankelijk advies. Onafhankelijkheid is tevens belangrijk om kritisch de implementatie van het beleid te kunnen toetsen.

Het is niet ongebruikelijk dat de CISO operationele verantwoordelijkheden heeft. Dit is afhankelijk van de grootte van de organisatie, het maturiteitsniveau en de beschikbaarheid van gekwalificeerd personeel. Het mengen van verantwoordelijkheden vraagt enige waakzaamheid. Vanuit regelgeving en industrienormen wordt functiescheiding verwacht en vermijding van belangenvermenging.

Concreet houdt dit in dat de CISO hiërarchisch[1] weliswaar onder een bepaalde afdeling kan ressorteren maar functioneel[2] rapporteert over informatieveiligheid aan het management waarbij deze persoon geen controle uitoefent op directe leidinggevende waar dit een belangenconflict kan

[1] Hiërarchisch: vanuit leidinggevende positie, inclusief personele en financiële aspecten.
[2] Functioneel: vanuit een specifieke vakinhoudelijke verantwoordelijkheid.

geven. Bij de aanduiding van de CISO zorgt het management ervoor dat er geen onverenigbaarheden met andere rollen en/of afdelingen zijn.

In kleine organisaties zal men geneigd zijn om verschillende rollen toe te kennen aan dezelfde persoon. Samenvoegen van rollen is mogelijk, zolang belangen, taken, verantwoordelijkheden en bevoegdheden niet conflicteren.

Aangezien de CISO zich toelegt op beleidsvorming en beleidstoezicht, is zijn/haar rol onverenigbaar met beleidsuitvoering. We denken hierbij bijvoorbeeld aan IT manager, HR manager, … Een CISO mag niet het eigen werk controleren en kan dus geen toezicht houden op het resultaat van een operationele taak die al dan niet tijdelijk is opgenomen door dezelfde persoon.

Is de rol van CISO verenigbaar met de rol van DPO?

Hoewel de CISO en de DPO best in nauw overleg samenwerken, is het de taak van de CISO om een gepast veiligheidsbeleid uit te werken en aan de DPO om toezicht te houden op de gepastheid hier van specifiek voor de bescherming van persoonsgegevens. Wanneer dit dezelfde persoon is, kan er mogelijk een belangenconflict optreden.

Risico's verbonden aan combineren van rollen moeten door het management van de entiteit expliciet aanvaard en gedocumenteerd worden.

Entiteiten die geen nood hebben aan een voltijdse CISO of niet beschikken over de nodige kennis en ervaring profielen hebben er baat bij om deze rol uit te besteden. Uitbesteden van de CISO rol is in principe mogelijk onder bepaalde voorwaarden:

- Zijn/haar onafhankelijkheid moet gegarandeerd worden.
  (inclusief vermijden van commerciële belangen)
- Er is aantoonbare expertise en ervaring.
- Een stabiele relatie kan gewaarborgd worden.
- De nodige contractuele voorwaarden zijn geborgd

  (vertrouwelijkheidsclausules, continuïteit in de dienstverlening, aansprakelijkheid …)

2.2.3. CISO taakomschrijving

De CISO beweegt zich op strategisch en tactisch niveau. Dit veronderstelt een door het management gedocumenteerd en goedgekeurd informatieveiligheidsbeleid, inclusief de beschrijving van de rollen en verantwoordelijkheden en het nodige mandaat om de CISO rol te kunnen invullen. Naast een adviserende rol is hij/zij verantwoordelijk voor beleidsvorming en beleidstoezicht in het kader van informatieveiligheid.

De CISO:

- Heeft een adviserende rol in informatieveiligheid, waaronder ICT en OT[3] security.
- Definieert het informatiebeveiligingsbeleid en de informatieveiligheidsstrategie vanuit een op risico gebaseerde benadering, conform het veiligheidsbeleid van de Vlaamse overheid. Hierbij houdt hij rekening met een continu veranderend dreigingsbeeld en analyseert daarbij trends en organisatiebehoeften.
- Richt de informatiebeveiligingsorganisatie in, definieert de daarvoor benodigde middelen en wijst ze toe.
- Initieert en coördineert de implementatie van informatiebeveiliging voor de hele organisatie, houdt toezicht vanuit een tweedelijnsrol en rapporteert aan het topkader.
- Zorgt voor een geschikt niveau van informatiebeveiliging en informatiebeveiligingsgedrag in de organisatie, gebaseerd op de behoeften en de risicobereidheid van de organisatie.
- Neemt deel aan de vergaderingen van de Werkgroep Informatieveiligheid.
- Wordt door interne en externe belanghebbenden gezien als de deskundige op het gebied van informatiebeveiligingsstrategie.

De CISO heeft volgende opdrachten:

- Opstellen, sturen en handhaven van het informatieveiligheidsbeleid.
- Opstellen van jaarlijkse doelstellingen en strategisch/tactisch informatieveiligheidsplan.
- Communiceren van het informatieveiligheidsbeleid aan alle relevante belanghebbenden.
- Initiëren van bewustzijn campagnes voor verschillende doelgroepen.
- Ontwikkelen, onderhouden en publiceren van beheerprocessen voor informatieveiligheidsbeleid.
- Adviseren van programma's en projecten bij de uitvoering van diverse veiligheidsactiviteiten zoals klassebepaling, risicoanalyse, implementatie beheersmaatregelen, etc.
- Behouden van overzicht over informatieveiligheidsrisico's en erop toezien dat deze regelmatig worden geactualiseerd en effectief gemitigeerd door de risico-eigenaren.
- Monitoren van compliance met het informatieveiligheidsbeleid.
- Aggregeren van informatieveiligheidsrisico's tot een geconsolideerd overzicht ten behoeve van rapportering aan het management en stuurgroepen over veiligheidsgerelateerde zaken op regelmatige en ad-hoc basis indien nodig.
- Stimuleren van een lerende organisatie ten behoeve van continue verbetering van informatieveiligheid.
- Fungeren als aanspreekpunt voor belangrijke overheidsinstanties over veiligheidskwesties.
- Geven van deskundig advies aan het management.

[3] OT = Operational Technologie: hardware en software ter ondersteuning van industriële apparatuur en processen (bijvoorbeeld voor bediening van sluizen, opvolging verkeer).

- Geven van deskundig advies aan aanpalende vakgroepen, zoals persoonsgegevensbescherming, informatiemanagement en bedrijfsrisicobeheer, met betrekking tot technische en organisatorische maatregelen rond informatieveiligheid.

Volgende taken zijn niet gevat in de rol van CISO:

- Het uitvoeren van informatieklassebepalingen of risicoanalyses.
- Het opstellen en implementeren van informatieveiligheidsmaatregelen.
- Operationele taken.
- De uitvoering van het informatieveiligheidsplan.

2.2.4. CISO competenties

Gezien het takenpakket van de CISO moet hij/zij beschikken over een aantal technische en niet-technische vaardigheden:

- Brede kennis op gebied van informatieveiligheid en -beveiliging alsook de wet- en regelgeving ter zake (helikopter view), zowel op technisch als organisatorisch domein.
- Het vermogen om strategisch en tactisch te denken.
- Diplomatieke en communicatieve vaardigheden: de CISO moet overtuigend communiceren over technische en niet-technische onderwerpen, zowel richting medewerkers als richting management en bestuur.
- Goede rapporterings- en presentatie vaardigheden: vanuit zijn/haar adviserende rol is het belangrijk om zaken goed op papier te zetten (rapporteren) en te presenteren.

2.3. Team Informatieveiligheid van Digitaal Vlaanderen

2.3.1. Relatie met ICR

Het Team informatieveiligheid treedt op als een overkoepelende veiligheidsdienst om zo de veiligheidsorganisatie op het niveau van Vo te versterken. Door het inzetten van deze gespecialiseerde dienstverlening kan het de verschillende entiteiten beter ondersteunen.

Het Team informatieveiligheid zorgt voor de uitbouw en het onderhoud van het informatieclassificatieraamwerk en ondersteunt de entiteiten bij de implementatie ervan door middel van advies.

Het Team informatieveiligheid is organisatorisch ondergebracht bij het agentschap Digitaal Vlaanderen maar wordt functioneel aangestuurd door het Stuurorgaan Vlaams informatie- en ICT-beleid en rapporteert ook aan dit stuurorgaan voor wat betreft het informatieclassificatieraamwerk.

2.3.2. Missie van het Team informatieveiligheid

De opdracht van het team informatieveiligheid bij Digitaal Vlaanderen is tweeledig:

- Het team zal een veilig verwerkingskader bieden met als doel een maximale reductie van informatieveiligheidsrisico's binnen de informatieverwerking te bewerkstelligen.
- Het team heeft de opdracht de doelstellingen informatieveiligheid voor Digitaal Vlaanderen in te vullen, alsook op te treden als vertrouwde partner voor een informatieveilige verwerking bij de andere entiteiten van de Vlaamse overheid.

We doen dit door:

- actief op te treden als CISO voor het agentschap Digitaal Vlaanderen,
- de risico's informatieveiligheid binnen de informatieverwerking te identificeren, correctieve acties op te starten en op te volgen binnen de verwerkingsopdracht van Digitaal Vlaanderen en ter ondersteuning van de afnemers van de dienstverlening binnen het ICT raamcontract Vlaamse overheid,
- door te waken over de processen en veiligheidsbouwstenen van de gemeenschappelijke dienstverlening,
- door actief ondersteuning te bieden aan zowel de risicobeheerder als de functionaris voor gegevensbescherming binnen Digitaal Vlaanderen,
- structurele ondersteuning te bieden voor de entiteiten van de Vlaamse overheid,
- het voorzitterschap van de werkgroep Informatieveiligheid in te vullen en via dit kanaal advies uit te brengen aan het stuurorgaan Vlaams informatie- en ICT-beleid,
- In een breder kader kennis te delen in het hoe en waarom informatieveiligheid integraal deel uitmaakt van de informatie beheer processen.

Om onze missie uit te voeren, ondersteunen we maximaal de strategie voor informatieveiligheid van de Vlaamse overheid en het informatieveiligheidsbeleid van de entiteiten, vertalen we de strategie naar een informatieveiligheidsplan en overzien de uitvoering van dit plan.

3. Documenteren van het beleid

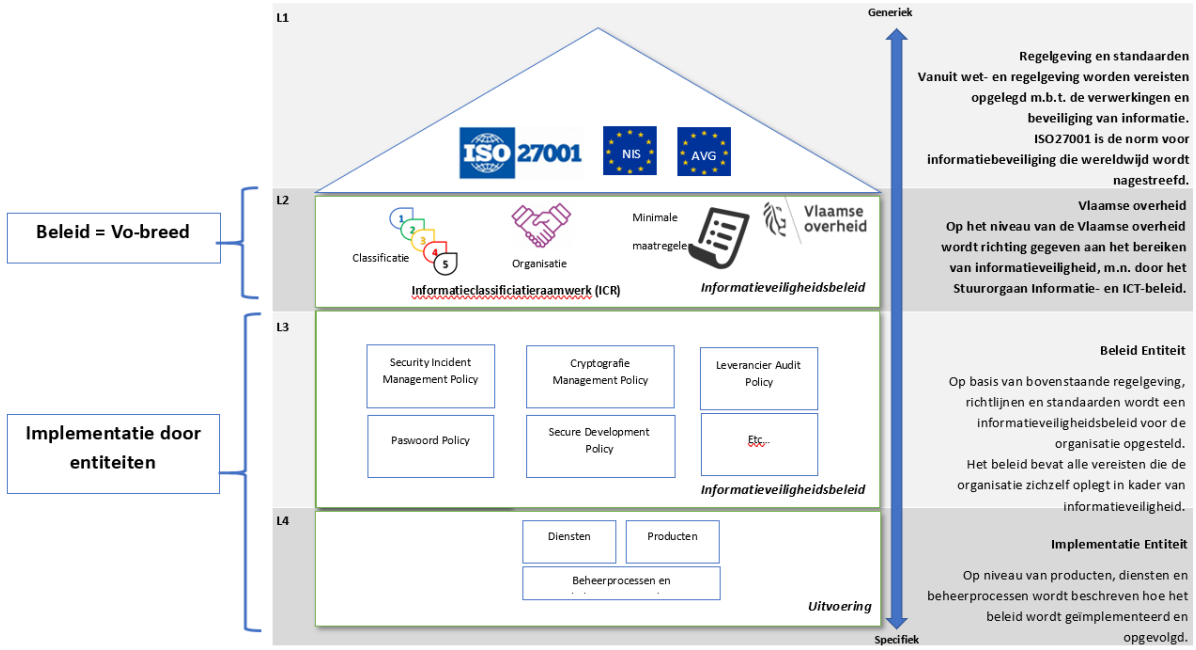
3.1. 4 niveaus van documentatie

Om het beleid te documenteren, werken we met 4 niveaus of levels. Dit gaat breder dan enkel het ICR.

Kort samengevat gaat het over:

	Gaat over	Is voor	Eigenaar	Voorbeelden
Level 1	Wet- en regelgeving	Vo-breed	Wetgevende macht, regelgevende instantie	Wetten, decreten, enz ISO27001 als basis voor ICR
Level 2	Beleid op niveau Vo	Vo-breed	Stuurorgaan Vlaams Informatie- en ICT-beleid	ICR
Level 3	Beleid op organisatienivea u	Entiteit	Topmanagement (leidend ambtenaar, directeur, CEO, …)	Beleidsdocumenten van een entiteit, bvb paswoord beleid.
Level 4	Implementatie van het beleid	Entiteit	Topmanagement (leidend ambtenaar, directeur, CEO, …)	Architectuur documenten Technische firewall policies

Volgend schema illustreert de relatie tussen de 4 documentatieniveaus:



Het is belangrijk om op te merken dat elke niveau conform moet zijn met het bovenliggende niveau. Zo moeten firewall policies in lijn zijn met het informatieveiligheidsbeleid van de entiteit, dat op zijn beurt conform moet zijn met het ICR, dat op zijn beurt conformeert aan wet- en regelgeving.

We geven een voorbeeld van zo'n cascade:

Op niveau 1 situeert zich (onder andere) de AVG. Deze stelt dat de nodige technische en organisatorische maatregelen moeten worden genomen om persoonsgegevens te beveiligen.
Op niveau 2 vertaalt de AVG zich in een Vo-breed beleid onder vorm van het ICR, waar persoonsgegevens een vertrouwelijkheidsklasse 2, 3 of 4 toegemeten krijgen. Aan die klasse zijn bepaalde minimale maatregelen gekoppeld, onder andere IAM (controlemaatregelen over identiteit, authenticatie en autorisatie). Daarin staat (onder andere) dat voor gegevens van klasse 2 een eIDAS laag kan worden ingericht als authenticatiemaatregel. Voor dit type gegevens volstaat dus een account/paswoord als authenticatie. Maar het ICR bepaalt verder geen detail regels over hoe zo'n paswoord er moet uit zien.
Daarvoor dient niveau 3: hier stelt elke entiteit voor zich een paswoordbeleid op dat voldoet aan de regels voorzien in het ICR (niveau 2).
En tenslotte is er nog niveau 4: hier wordt het niveau 3 paswoordbeleid vertaalt naar technische regels die dan ingericht worden, bijvoorbeeld voor MS Windows.

3.1.1. Documentatielevel 1

Dit niveau omvat documenten die de wet- en regelgeving beschrijven en ondersteunen en wordt gebruikt als bron voor de criteria binnen de informatieclassificatie:

- Wetgeving waaronder de informatieverwerking van de Vo valt:
  - EU;
  - EU-lidstaat;
  - Federale overheid;
  - Regionale overheid;
  - ...
- Regelgeving waaronder de informatieverwerking van de Vo valt:
  - Machtigingen;
  - Contractuele verbintenissen en voorwaarden;
  - Generieke en specifieke Vo afspraken.
  - Normen en standaarden die de basis vormen voor het Vo-brede beleid:
  - ISO27001

De regelgevende organisatie is aansprakelijk en verantwoordelijk voor het ter beschikking stellen van deze documentatie. Zij behoren niet tot de Vo administratie.

3.1.2. Documentatielevel 2

Dit niveau bevat het Vo ICR, inclusief de minimale maatregelen met betrekking tot informatieverwerking binnen de Vo. Deze documenten formuleren de manier waarop we de verplichtingen zoals beschreven in de documentatie uit level 1 moeten interpreteren en beantwoorden:

- De unieke en uniforme manier waarop de Vo de informatie uit level 1 positioneert en beantwoordt. (Dit document)
- De manier waarop we de informatieverwerking koppelen aan een reeks te nemen maatregelen, gegroepeerd op basis van informatieklassen. (Dit document)
- De koppeling van organisatorische en technische maatregelen aan een informatieklasse. (De minimale maatregelen)
  - 'Minimale algemene maatregelen' op basis van ISO27001/-2 standaarden zorgen voor de basis van een veilig en gestructureerde informatieverwerking.

- ‘Minimale specifieke maatregelen’ op basis van specifieke regelgeving (bijvoorbeeld GDPR, maar ook andere regelgeving is mogelijk) vervolledigen de ‘Minimale algemene maatregelen’.

De aansprakelijkheid voor het ter beschikking stellen van de documentatie set rond het ICR ligt bij het ‘Stuurorgaan Vlaams Informatie- en ICT-beleid’.

3.1.3. Documentatielevel 3

Dit niveau bevat alle documentatie waarin de informatieverwerker (de entiteit van de Vo administratie of dienstenleverancier) haar eigen beleidslijnen rond informatieveiligheid beschrijft:

- Beleid voor de volledige keten van de informatieverwerking:
  - Voor informatieverwerking binnen de organisatie;
  - Voor informatieverwerkingsdiensten aangeboden aan derden;
  - (Een referentie aan de) documentatie level 3 van toepassing op informatie verwerkende diensten, afgenomen van derden.
- Uitwerking
  - Contractuele afspraken
    - Inclusief bijhorende documentatie (addendum, verwijzingen,…)
  - Verwerkingsovereenkomsten
    - Inclusief bijhorende documentatie (addendum, verwijzingen,…)
  - Processen
    - Inclusief de richtlijnen (policy) die als raamwerk dienen om de processen van de volledige informatieverwerking te ondersteunen en structureren

De aansprakelijkheid voor het ter beschikking stellen van deze documentatie set ligt bij:

- de eigen organisatie, voor de informatieverwerking binnen de eigen organisatie;
- de leverancier voor informatieverwerking buiten de eigen organisatie:
  - commerciële organisaties;
  - andere Vo-organisaties die informatieverwerking aanbieden.

De verantwoordelijkheid voor de beschikbaarheid van deze documentatie ligt bij de organisatie die de informatieverwerking organiseert of afneemt van derden.

3.1.4. Documentatielevel 4

Dit niveau bevat alle documentatie waarin de architectuur en uitwerking van de informatie verwerkende componenten worden beschreven. Deze beschrijving is beschikbaar per applicatie:

- Doel van de informatieverwerking
- Architectuur
  - Processtromen
    - Processen, eigen aan de specifieke informatieverwerking (specifieke toepassing)
    - Externe processen
      - Gebruiksbeheer en applicatie toegangen
      - Beheerderstoegangen

- Informatiestromen
- Informatiebeschrijving
  - Noodzaak van de informatie-attributen binnen de informatieverwerking
- Techniek
  - Technische componenten
    - Applicatie (inclusief externe componenten)
    - Beheer
  - Technische informatiestromen tussen de applicatie componenten
  - Toegangscontrole
    - Toepassing
    - Externe diensten en toepassingscomponenten
  - Genomen veiligheidsmaatregelen
    - Toepassing
    - Ondersteunende platformen
    - Beschikbare adviezen van leveranciers en de toepassing ervan
    - Netwerken
      - Firewall
      - IDS/IDP
      - …
  - Technische 'baselines' en technische 'policies'

De aansprakelijkheid voor het ter beschikking stellen van deze documentatie set ligt bij:

- De eigen organisatie, voor de informatieverwerking binnen de eigen organisatie;
- De leverancier voor informatieverwerking buiten de eigen organisatie:
  - Commerciële organisaties;
  - Andere Vo-organisaties die informatieverwerking aanbieden.

De verantwoordelijkheid voor de beschikbaarheid van deze documentatie ligt bij de organisatie die de informatieverwerking organiseert of afneemt van derden.

3.2. Beheer van het ICR

3.2.1. Documentatie van het ICR

Er zijn 3 omgevingen waar documentatie van het ICR wordt bijgehouden:

- Op de SharePoint van het Team Informatieveiligheid (Digitaal Vlaanderen - Team informatieveiligheid - Informatieveiligheid - Alle documenten (sharepoint.com)): in deze omgeving worden de werkversies bijgehouden en de laatste door het Stuurorgaan goedgekeurde Word versie. De toegang is beperkt tot de beheerders van de documenten, namelijk het Team Informatieveiligheid.
- Op de website Informatieclassificatieraamwerk | Vlaanderen.be: deze pagina is voor iedereen toegankelijk (eventueel na verzoek tot toegang) en bevat de laatste documenten in pdf-formaat goedgekeurd door het Stuurorgaan. Deze set documenten is ook nuttig om te overhandigen tijdens audits.
- Op de Confluence pagina: ook deze pagina is voor iedereen toegankelijk en bevat dezelfde informatie als op de website maar is makkelijker te doorzoeken.

3.2.2. Levenscyclus van het ICR

Het ICR bestaat dus uit een reeks documenten die behoren tot niveau 2. Deze documenten moeten consequent onderhouden worden. Dit houdt in dat het ICR minstens jaarlijks, of bij significante wijzigingen in de wet- en regelgeving, nagekeken en waar nodig herwerkt wordt.

De flow van de documenten ziet er als volgt uit:

- Het Team Informatieveiligheid, dat instaat voor het onderhoud van het ICR, voert de nodige wijzigingen uit.
- Afhankelijk van de grootte van de wijzigingen wordt een taakgroep en/of een leespanel samengesteld om de (ver)nieuw(d)e documenten samen te stellen en na te kijken.
- De nieuwe versie wordt voorgesteld aan de Werkgroep Informatieveiligheid – beleid ter validatie (de leden van deze werkgroep maken ook automatisch deel uit van het leespanel).
- Zodra de werkgroep informatieveiligheid de nieuwe versie heeft gevalideerd (eventueel na iteratie), wordt het document ter goedkeuring voorgelegd aan het Stuurorgaan Vlaams Informatie- en ICT-beleid.
- Na goedkeuring door het stuurorgaan wordt het document gepubliceerd op de website en waar nodig de Confluence pagina aangepast en tevens voorgesteld aan de werkgroep informatieveiligheid – community.

De activiteiten van deze jaarlijkse herziening zijn:

- Evaluatie van de criteria op basis van gewijzigde regelgeving;
- Evaluatie van de maatregelen op basis van geïdentificeerde risico's:
    - Aanpassen;
    - Vervangen;
    - Verwijderen;
    - Toevoegen.

Enkele mogelijke gevolgen van deze oefening zijn:

- Een revaluatie van datasets bij wijziging van classificatiecriteria en/of maatregelen;
- Bijsturing van bestaande technische en organisatorische maatregelen.

3.2.3. Opvolging en monitoring

Om de implementatie van het ICR door de entiteiten op te volgen, wordt nagegaan of/in hoeverre een entiteit voldoet aan het ICR via self-assessment. Dit is nog werk in uitvoering.

Voor nieuwe versies van het ICR wordt steeds een overgangsperiode voorzien van Q4 van het jaar van publicatie + 1 jaar.