VRD 2 - PROJECTDOSSIER 23.08 – Uitvoeren Informatieveiligheidsstrategie Vlaamse Overheid

1 PROJECTOMSCHRIJVING

Informatieveiligheid vormt een ondeelbaar geheel met de manier waarop we iedere dag omgaan met informatie, tijdens elke activiteit op de werkvloer, tijdens elk contact met de burger, bedrijven, overheden en entiteiten. Hoe triviaal deze interacties soms lijken te zijn, telkens is er wisselwerking aan informatiestromen en processen die de noodzakelijke beschermende maatregelen verantwoorden, op maat van de toepassing en het achterliggende proces.
Dit programma is de voorzetting van het informatieveiligheidselement (waaronder ook cybersecurity valt) van het relanceproject VV065: "Cybersecurity en uitrol SIEM" en geeft invulling aan de op 15 oktober 2021 door de Vlaamse Regering goedgekeurde "Strategie Informatieveiligheid". Deze strategie wil een antwoord bieden op de toenemende dreiging van cybercriminelen en ervoor zorgen dat de Vlaamse overheid een betrouwbare partner is én blijft op het vlak van informatieveiligheid.

Dit programma voorziet o.m. in verschillende bijkomende gerichte flankerende initiatieven en investeringen op vlak van informatieveiligheid om de digitale transformatie veilig en in lijn met privacy (GDPR) regelgeving en andere Europese cyberwetten (NIS2) te versnellen.
In de zomer van 2021 heeft Audit Vlaanderen een thema-audit IT-beveiliging laten uitvoeren binnen de Vlaamse Overheid om te onderzoeken in welke mate de belangrijkste beheersmaatregelen aanwezig zijn om de gewenste IT-beveiliging en IT-continuïteit te kunnen garanderen opdat de burger voldoende kan vertrouwen op de Vlaamse overheid en of de betrokken entiteiten. In het auditrapport constateert Audit Vlaanderen dat genoemde strategie potentieel de basis kan vormen voor een sterke vooruitgang op het vlak van IT-beveiliging bij de Vlaamse overheid.

Binnen de Vlaamse overheid coördineert het Stuurorgaan Informatie- en ICT-Beleid de implementatie van deze strategie en heeft het Team Informatieveiligheid van Digitaal Vlaanderen, het programma informatieveiligheid opgezet. Dit document beschrijft de doelstellingen van de projecten die onderdeel uitmaken van dat programma in 2023 welke in scope zijn van dit VRD 2-project.

De strategie en het programma vervullen de Vlaamse ambitie om van digitaal werken de norm te maken en omvat drie pijlers. Binnen deze 3 pijlers zijn voor 2023 de volgende activiteiten voorzien voor de pijlers A en B:

A. Overheidsbrede aanpak van informatieveiligheid
   - Ontwikkeling van een dashboard Informatieveiligheid en bescherming van persoonsgegevens en een statusrapport aan het Stuurorgaan;
   - Self-assessments voor entiteiten ontwikkelen en organiseren met betrekking tot het informatieclassificatie raamwerk van de Vlaamse overheid;
   - Uitbreiding van het informatieclassificatieraamwerk van de Vlaamse overheid door de ontwikkeling van compliance met andere raamwerken;
   - Het verbreden van de toepasbaarheid van het informatieclassificatieraamwerk door het verkrijgen van erkenning door toezichthouders en regelgevers.
B. Verhoging van de digitale competenties

- Uitbouwen van de overkoepelende informatieveiligheidsdienst voor het coördineren van transversale initiatieven en een overheidsbreed gedragen aanpak, onder andere door het afstemmen van de taken en verantwoordelijkheden en door de invoering van het drielijnenmodel;
- Communicatie -en bewustmakingscampagne verder vormgeven;
- Uitwerken van een ondersteunende dienstverlening CISO ter ondersteuning van een uniforme werking op het vlak van kennisdeling, uitvoering en coördinerende taken. Deze dienstverlening omvat ook de dienste Security Officer as a Service
- Overheidsbrede aanpak voor beheer van contractuele risico's door het ontwikkelen van modelclausules met betrekking tot informatieveiligheid op basis van de industriestandaarden.

Genoemde activiteiten zijn verdeeld over drie programmasporen, te weten:

1. Het verbeteren en versterken van de governance van informatieveiligheid;
2. De uitbouw en verbetering van de dienstverlening van informatieveiligheid;
3. De uitbouw en verbetering van het informatieclassificatieraamwerk.

Per programmaspoor zijn de strategische doelstellingen geformuleerd.

2 DOELSTELLINGEN

De Vlaamse overheid wil in de eerste plaats het vertrouwen genieten van de burger, onderneming en/of vereniging, de persoonlijke levenssfeer van de burger beschermen en de reputatie hooghouden van de Vlaamse overheid als betrouwbare partner.
Voor het succes van de Vlaamse overheid als een betrouwbare partner en de verdere digitale transformatie die de Vlaamse overheid wil uitvoeren is het v**erzekeren van bedrijfscontinuïteit** essentieel. Door het voeren van een adequaat informatieveiligheidsbeleid worden bedreigingen snel geïdentificeerd en laat de Vlaamse overheid toe snel in te grijpen en ernstige incidenten af te wenden en eventuele gevolgen in te perken. Dit draagt aanzienlijk bij aan de robuustheid van de informatiesystemen, wat op haar beurt de bedrijfscontinuïteit en het vertrouwen in onze overheid positief beïnvloedt.
Om de doelstelling van de Vlaamse regering inzake digitalisering te versnellen is het van cruciaal belang dat een veilige digitale dienstverlening kan gerealiseerd worden met een zo klein mogelijke impact op de werking en budgetten.

1. Het verbeteren en versterken van de governance van informatieveiligheid

Dit spoor richt zich op het verbeteren en versterken van de besturing van informatieveiligheid:

- Een duidelijk beleidskader binnen de Vlaamse overheid rond het beheersen van risico's op het vlak van informatieveiligheid, met inbegrip bescherming van persoonsgegevens;
- Versterkte slagkracht met betrekking tot informatieveiligheid garanderen door een sterke coördinatie onder toezicht van het Stuurorgaan Informatie- en ICT-Beleid;
- Een breed draagvlak creëren door participatie van diverse stakeholders (werkgroep, private sector, onderzoek, …) en door het zorgdragen van de erkenning van het informatieveiligheidsbeleid door toezichthouders en regelgevers;
- Minder blootstelling aan risico's met betrekking tot informatieveiligheid door opleiden en bewustmaken van de werknemers van de Vlaamse overheid;
- Inzicht in de stand van zaken met betrekking tot informatieveiligheid binnen de Vlaamse overheid om te komen tot geïnformeerde beslissingen over investeringen en bijsturing.

2. De uitbouw en verbetering van de dienstverlening van informatieveiligheid

Dit spoor richt zich op de volgende doelstellingen:

- Interne competentie -en kennisopbouw verhogen door een pool aan specialisten met brede inzetbaarheid;
- Verhogen van de maturiteit van onze veiligheidsorganisatie door ondersteuning met betrekking tot veiligheidsdienstverlening & tools;
- Geïntegreerde dienstverlening met betrekking tot het beheersen van risico's van onze gemeenschappelijke ICT-systemen.

3. De uitbouw en verbetering van het informatieclassificatieraamwerk

Dit spoor richt zich op de verdere uitbouw, verbetering en implementatie van het informatieclassificatieraamwerk resulterend in een overheidsbrede aanpak van informatieveiligheid. Door een overheidsbrede focus op informatieveiligheid te leggen, beoogt de strategie informatieveiligheid volgende doelstellingen te bereiken:

- Betere en geïnformeerde beslissingen zowel op overheidsbreed niveau als op entiteitsniveau door een duidelijk begrip van de risicoblootstelling van de Vlaamse overheid op het vlak van informatieveiligheid en veiligheid van persoonsgegevens.
- Vergroten van de compliance van het informatieclassificatieraamwerk met federale en Europese regelgeving waardoor de toepasbaarheid breder wordt en het draagvlak ervoor vergroot wordt.

3 BATEN

Net zoals in de rest van de samenleving zijn de dreigingen en aanvallen op de digitale infrastructuur van de overheid het afgelopen jaar sterk gestegen. Daar komt de toegenomen dreiging van verwachte cyberaanvallen als reactie op de Europese sancties voor de inval in Oekraïne bij. De gezamenlijke informatieveiligheidsstrategie omvat het versterken van de veiligheidscultuur en een goed uitgebouwd crisismanagement.

Dit project focust op volgende resultaatgebieden:

A. VO-brede aanpak van informatieveiligheid

- Betere en geïnformeerde beslissingen door een duidelijk begrip van de risicoblootstelling van de Vlaamse overheid op het vlak van informatieveiligheid en veiligheid van persoonsgegevens.
- Een consistente aanpak die onnodige complexiteit en tegenstrijdige adviezen vermijdt binnen dezelfde overheid. Deze aanpak zal de beheersbaarheid én de betaalbaarheid van het informatieveiligheidsbeleid verhogen.

B. Verhogen van digitale competenties

- Verbeterde coördinatie met betrekking tot informatieveiligheid
- Minder blootstelling aan risico's met betrekking tot informatieveiligheid.
- Verhoogde capaciteit door beroep te doen op strategische partners, gespecialiseerd in cybersecurity
- Verhoogde interne competentie en kennis.

C. Weerbare digitale processen en een robuuste infrastructuur.

- Verhoogde maturiteit van onze veiligheidsorganisatie door ondersteuning met betrekking tot veiligheidsdienstverlening & tools.
- Geïntegreerde dienstverlening met betrekking tot het beheersen van risico's van onze gemeenschappelijke ICT-systemen.
- Tijdige detectie van informatieveiligheidsincidenten.
- Versterkte slagkracht met betrekking tot ernstige informatieveiligheidsincidenten

4 DELIVERABLES

Het project realiseert per product onderstaande zelfstandig bruikbare functionaliteiten in 2023:

Product	Deliverable Nr	Omschrijving
Vo-informatieveiligheidsbeleid	D.23.08.01	Het informatieclassificatieraamwerk is actueel en erkend door toezichthouders en regelgevers (D.23.08.1.1)
	D.23.08.02	De transversale en overkoepelende coördinatie van informatieveiligheid is versterkt (D.23.08.1.2.1)
	D.23.08.03	Communicatie -en bewustmaking campagne met betrekking tot informatieveiligheid (D.23.08.1.3.1)
	D.23.08.04	Opbouw en verdere ontwikkeling van standaardrapportering en centraal dashboard voor veiligheidsrisico's (D.23.08.1.4.1)
	D.23.08.05	Ontwikkeling van een Informatieveiligheid tool box met daarin onder andere sjablonen, richtlijnen en kennisbibliotheek ter ondersteuning van het team informatieveiligheid bij de invulling van haar transversale en overkoepelende rol, en ten behoeve van de dienst Information Security Officer as a Service. Deze dienst kan worden afgenomen door Vo-entiteiten ter ondersteuning van hun informatieveiligheidsbeleid (D.23.08.2.1.2)
	D.23.08.06	De modelclausules voor het afdekken van contractuele risico's op het gebied van informatieveiligheid zijn ontwikkeld en beschikbaar gesteld aan alle entiteiten via de aankoopcentrale (D.23.08.2.3.1)00
	D.23.08.07	Het informatieclassificatieraamwerk is verder uitgebouwd en aangevuld met compliance met federale en Europese regelgeving (D.23.08.3.2.3)
	D.23.08.08	De instrumenten, tooling en het proces voor de self-assessments zijn ontwikkeld (D.23.08.3.2)
	D.23.08.09	Algemeen overkoepelend projectmanagement (D.23.08.4)

5 PROJECTAANPAK

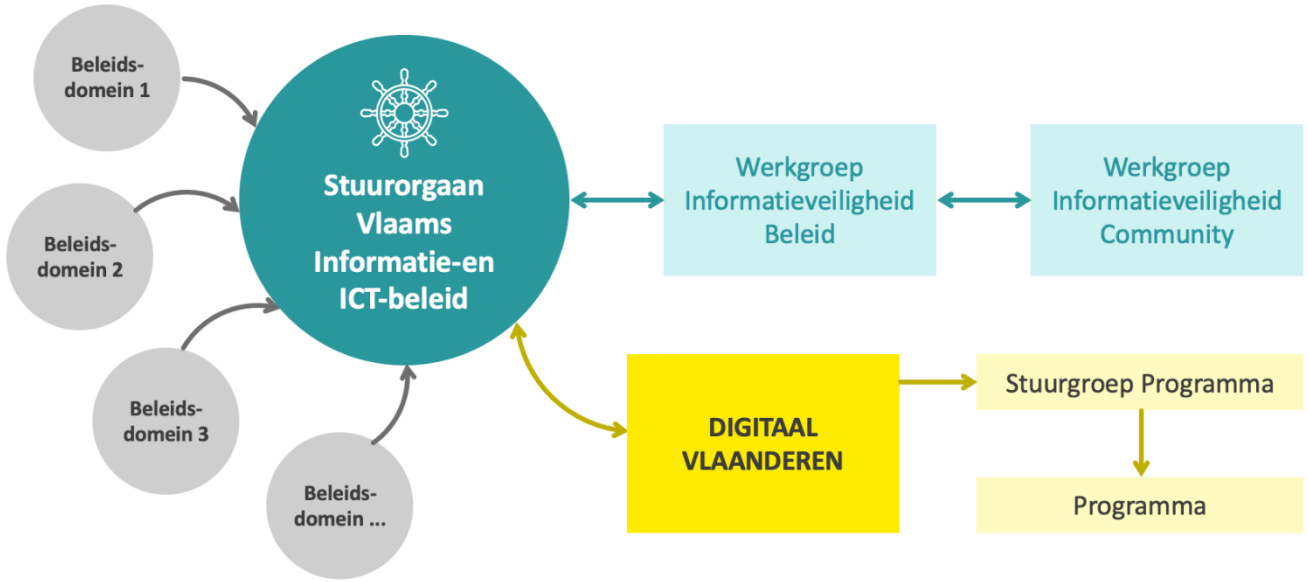
5.1 PROJECTSTURING

Detaillering en aanvullende rollen worden in onderstaande tabel weergegeven.

Rol	Omschrijving
Stuurorgaan Vlaams Informatie-en ICT-beleid	Afstemming met entiteiten in scope
Stuurgroep programma	Operationele aansturing programma met klantenvertegenwoordiging via CISO Digitaal Vlaanderen
Klantenfora	Werkgroep Informatieveiligheid Beleid, Werkgroep Informatieveiligheid Community, workshops met verandermanagers van betrokken entiteiten
Eindverantwoordelijke	Digitaal Vlaanderen

Rol	Omschrijving
Betrokken partijen	Entiteiten van de Vlaamse Administratie (66 entiteiten)

Aansturing van het programma en klantenvertegenwoordiging:



5.2 PROJECTPLAN 2023

De deliverables worden opgeleverd op incrementele wijze. We starten met een minimum viable product en verbeteren de deliverable in de loop van het programma. Op deze manier leveren de deliverables snel toegevoegde waarde.

PR120 - VO Informatieveiligheidsbeleid

Actie	startdatum	einddatum	Betrokken partij(en)
Het informatieclassificatieraamwerk is actueel en erkend door toezichthouders en regelgevers	01/01/23	31/12/23	Digitaal Vlaanderen
De transversale en overkoepelende coördinatie van informatieveiligheid is versterkt	01/01/23	31/12/23	Digitaal Vlaanderen
Communicatie -en bewustmaking campagne met betrekking tot informatieveiligheid	01/01/23	31/12/23	Digitaal Vlaanderen
Opbouw en verdere ontwikkeling van standaardrapportering en centraal dashboard voor veiligheidsrisico's	01/01/23	30/09/23	Digitaal Vlaanderen

Ontwikkeling van een Informatieveiligheid tool box met daarin onder andere sjablonen, richtlijnen en kennisbibliotheek ter ondersteuning van het team informatieveiligheid bij de invulling van haar transversale en overkoepelende rol, en ten behoeve van de dienst Information Security Officer as a Service. Deze dienst kan worden afgenomen door Vo-entiteiten ter ondersteuning van hun informatieveiligheidsbeleid	01/01/23	31/12/2023	Digitaal Vlaanderen
De modelclausules voor het afdekken van contractuele risico's op het gebied van informatieveiligheid zijn ontwikkeld en beschikbaar gesteld aan alle entiteiten via de aankoopcentrale	01/01/23	31/12/23	Digitaal Vlaanderen
Het informatieclassificatieraamwerk is verder uitgebouwd en aangevuld met compliance met federale en Europese regelgeving	01/01/23	31/12/23	Digitaal Vlaanderen
De instrumenten, tooling en het proces voor de self-assessments zijn ontwikkeld	01/01/23	30/06/23	Digitaal Vlaanderen

5.3 OVERHEIDSOPDRACHTEN

- ICT-raamovereenkomsten 2022-2029
- ICT-profielen raamovereenkomst 2022-2027

5.4 BUDGET

Het vereiste projectbudget 2023 wordt in onderstaande tabel opgesplitst per zelfstandig bruikbare component/deliverable.

Meer detail inclusief de exploitatiekost, is te vinden in het kosten- en financieringsmodel in bijlage 1.

Deliverable Nr	Deliverable	Budget (incl btw)
D.23.08.01	Het informatieclassificatieraamwerk is actueel en erkend door toezichthouders en regelgevers (D.23.08.1.1)	€ 34.999
D.23.08.02	De transversale en overkoepelende coördinatie van informatieveiligheid is versterkt (D.23.08.1.2.1)	€ 34.999
D.23.08.03	Communicatie -en bewustmaking campagne met betrekking tot informatieveiligheid (D.23.08.1.3.1)	€ 80.000.
D.23.08.04	Opbouw en verdere ontwikkeling van standaardrapportering en centraal dashboard voor veiligheidsrisico's (D.23.08.1.4.1)	€ 136.000
D.23.08.05	Ontwikkeling van een Informatieveiligheid tool box met daarin onder andere sjablonen, richtlijnen en kennisbibliotheek ter ondersteuning van het team informatieveiligheid bij de invulling van haar transversale en overkoepelende rol, en ten behoeve van de dienst	€ 25.002

Deliverable Nr	Deliverable	Budget (incl btw)
	Information Security Officer as a Service. Deze dienst kan worden afgenomen door Vo-entiteiten ter ondersteuning van hun informatieveiligheidsbeleid (D.23.08.2.1.2)	
D.23.08.06	De modelclausules voor het afdekken van contractuele risico's op het gebied van informatieveiligheid zijn ontwikkeld en beschikbaar gesteld aan alle entiteiten via de aankoopcentrale (D.23.08.2.3.1)	€ 50.000
D.23.08.07	Het informatieclassificatieraamwerk is verder uitgebouwd en aangevuld met compliance met federale en Europese regelgeving (D.23.08.3.2.3)	€ 40.002
D.23.08.08	De instrumenten, tooling en het proces voor de self-assessments zijn ontwikkeld (D.23.08.3.2)	€ 159.998
D.23.08.09	Algemeen overkoepelend projectmanagement (D.23.08.4)	€ 49.000
TOTAAL:		€ 610.000

5.5 RISICOREGISTER

Onderstaande tabel geeft een overzicht van de voornaamste geïdentificeerde projectrisico's en, in voorkomend geval, remediërende maatregelen om deze te beheersen.

Risico	Ernst	Kans	RPN	Beheersmaatregel
Onvoldoende externe resources	5	4	20	Voldoende tijd investeren in aanwervingsproces Resources begeleiden bij onboarding
Onvoldoende interne resources	5	3	15	Regelmatig overleg met Team Informatieveiligheid over prioriteiten en planning
Onvoldoende breed draagvlak	5	4	20	Stakeholder management dmv workshops met pilot-entiteiten Voldoende communicatie
Onvoldoende rekening houden met de eigenheden van de entiteiten	3	3	9	Tweerichtingscommunicatie (doorgeven van informatie én luisteren naar bezorgdheden)
Onrealistische verwachtingen van het programma	3	3	9	Management van verwachtingen door proactieve communicatie naar stuurorganen
Niet gericht op praktijk, waardoor entiteiten toch kiezen voor een individuele aanpak	4	3	12	Deliverables bijsturen obv feedback van piloot-entiteiten

[Ernst: 0-5 Kans: 0-5 RPN: risico prioriteit nummer = ernst x kans
Beheersmaatregel noodzakelijk vanaf RPN > 9]

BIJLAGE 1: KOSTEN- EN FINANCIERINGSMODEL

KOSTEN- EN FINANCIERINGSMODEL 2023-2024

Onderstaande tabel geeft per product en per deliverable een detaillering van de investeringskost in 2023 en de gerelateerde exploitatiekost in 2024.

Bedrag Product	Deliverable	Aankooptype detail	Financiering	JAAR 2023	2024
VO informatieveiligheidsbeleid	D.1 Erkenning ICR (1.1)	Externe medewerkers	VRD 2 Exploitatie	34.999	
	D.2 Beleidsafspraken eigenaarschap (1.2.1)	Externe medewerkers	VRD 2 Exploitatie	34.999	
	D.3 Communicatie & training (1.3.1)	Nog te bepalen IT	VRD 2 Exploitatie	80.000	
	D.4 Dashboard & statusrapportage (1.4.1)	Externe medewerkers	VRD 2 Exploitatie	136.000	
	D.5 Uitbouwen ISOaaS (2.1.2)	Externe medewerkers	VRD 2 Exploitatie	25.002	
	D.6 Afdekken contractuele risico's (2.3.1)	Externe medewerkers	VRD 2 Exploitatie	50.000	
	D.7 Compliance (3.2.3)	Externe medewerkers	VRD 2 Exploitatie	40.002	
	D.8 Self-assessments (3.2.1)	Externe medewerkers	VRD 2 Exploitatie	109.998	
	D.8 Tool voor ICR & self-assessments (3.2.2)	Nog te bepalen IT	VRD 2 Exploitatie	50.000	
	Exploitatiekost 2024	Externe medewerkers	VRD 2 Exploitatie		100.000
Projectregie	D.9 Overkoepelend programmamanagement (4)	Projecten	VRD 2 Exploitatie	49.000	
Eindtotaal				**610.000**	**100.000**

Aankooptype Externe Medewerkers: Aantal mandagen per ingezet profiel in 2023

Aantal MD Product	Profiel	Total
VO informatieveiligheidsbeleid	ICT Business analist - Consultant SR	283
VO informatieveiligheidsbeleid	Security Consultant (ML)	160
VO informatieveiligheidsbeleid	ICT - Architect (SR)	29
VO informatieveiligheidsbeleid	Security Expert CISO	27

VAK- EN VEK-KALENDER 2023 - 2024

Onderstaande tabel geeft voor het projectvoorstel een samenvatting en uitsplitsing op jaarbasis in de periode 2023 - 2024 van de nodige vastleggingskredieten (VAK) en vereffeningskredieten (VEK) per financieringsbron.

Budget Product	Financiering	VAK/VEK 2023	2024
VO informatieveiligheidsbeleid	VRD 2 Exploitatie	561.000	100.000
Projectregie	VRD 2 Exploitatie	49.000	
Eindtotaal		**610.000**	**100.000**

PROGNOSE VEK EERSTE UITVOERINGSJAAR

Onderstaande tabel geeft voor het relancebudget, per projectresultaat, een prognose voor de vereffeningskalender van het eerste uitvoeringsjaar.

	Waarden											
Deliverable	01/23	02/23	03/23	04/23	05/23	06/23	07/23	08/23	09/23	10/23	11/23	12/23
D.1 Erkenning ICR (1.1)	2.923	2.916	2.916	2.916	2.916	2.916	2.916	2.916	2.916	2.916	2.916	2.916
D.2 Beleidsafspraken eigenaarschap (1.2.1)	2.923	2.916	2.916	2.916	2.916	2.916	2.916	2.916	2.916	2.916	2.916	2.916
D.3 Communicatie & training (1.3.1)	6.667	6.667	6.667	6.667	6.667	6.667	6.667	6.667	6.667	6.667	6.667	6.667
D.4 Dashboard & statusrapportage (1.4.1)	11.365	11.331	11.331	11.331	11.331	11.331	11.331	11.331	11.331	11.331	11.331	11.331
D.5 Uitbouwen ISOaaS (2.1.2)	2.034	2.088	2.088	2.088	2.088	2.088	2.088	2.088	2.088	2.088	2.088	2.088
D.6 Afdekken contractuele risico's (2.3.1)	4.487	4.593	4.593	4.593	4.593	4.593	2.088	4.593	4.593	4.593	4.593	2.088
D.7 Compliance (3.2.3)	3.534	3.588	3.588	3.588	3.588	3.588	2.088	3.588	3.588	3.588	3.588	2.088
D.8 Self-assessments (3.2.1)	11.046	11.004	11.004	10.992	10.992	10.992	0	10.992	10.992	10.992	10.992	0
D.8 Tool voor ICR & self-assessments (3.2.2)	4.167	4.167	4.167	4.167	4.167	4.167	4.167	4.167	4.167	4.167	4.167	4.167
D.9 Overkoepelend programmamanagement (4)	4.083	4.083	4.083	4.083	4.083	4.083	4.083	4.083	4.083	4.083	4.083	4.083
Eindtotaal	**53.228**	**53.352**	**53.352**	**53.340**	**53.340**	**53.340**	**38.343**	**53.340**	**53.340**	**53.340**	**53.340**	**38.343**

BIJLAGE 2: BIJKOMENDE PROJECTINFORMATIE

Beschrijving programma in de vorm van epics

ProjectNr-Resultaat	Specifieke gebruiker	EPIC beschrijving
VV065.01 - A1.1 Verankering regelgeving	Entiteiten Vlaamse overheid	Als gebruiker wil ik dat de strategie informatieveiligheid in de regelgeving verankerd is door middel van een beslissing erover van de Vlaamse Regering via een gepubliceerde nota zodat ik deze kan gebruiken voor de invulling van het informatieveiligheidsbeleid binnen mijn eigen entiteit
DOT – C2.2 Vo-breed Crisis Inc. mgmt proces	Entiteiten Vlaamse overheid	Als gebruiker wil ik een afgestemd, efficiënt en centraal gecoördineerd overkoepelend incident management proces, in samenwerking met CCVO, zodat ik in geval van een ernstige informatieveiligheidsincidentweet wie waarvoor verantwoordelijk is en ik kan rekenen op ondersteuning en de tijdige afhandeling ervan
VV065.01- A1.2 Beleidsafspraken Eigenaarschap	Stuurorgaan Informatie en ICT-Beleid	Als gebruiker wil ik dat de rollen en verantwoordelijkheden mbtinformatieveiligheid goed vastgelegd en afgestemd zijn zodat ik weet wie binnen de entiteiten aansprakelijk is voor de uitvoering van het informatieveiligheidsbeleid en dat dit door de entiteiten onderschreven wordt
VV065.01.01-A1.4 Dashboard 1.0	Stuurorgaan Informatie en ICT-Beleid	Als gebruiker wil ik de ontwikkeling en implementatie van de eerste versie van een dashboard Informatieveiligheid en bescherming van persoonsgegevens zodat ik inzicht heb in de stand van zaken en de risico's die ik loop en zodat ik kan bijsturen als dat nodig is
VV065.01.02-A3.1 ICR 2.0	Entiteiten Vlaamse overheid	Als gebruiker wil ik dat de leesbaarheid, toegankelijkheid en de gebruiksvriendelijkheid van het Informatieclassificatieraamwerk(ICR) verbeterd wordt zodat ik dit ICR kan toepassen bij de invulling van informatieveiligheidsbeleid van mijn entiteit
VV065.01.03- A3.2 Self-assessment 1.0	Entiteiten Vlaamse overheid	Als gebruiker wil dat een self-assessment, inclusief bijbehorend proces, ontwikkeld wordt zodat ik deze kan gebruiken om de maturiteit van mijn entiteit te bepalen en deze kan vergelijken met het ambitieniveau van mijn entiteit en met een benchmark
VV065.01- A3.2 Compliance	Entiteiten Vlaamse overheid	Als gebruiker wil ik dat inzichtelijk is welke andere raamwerken relevant zijn om toe te voegen aan het ICR zodat ik na uitbreiding van het ICR met de minimale normen van deze relevante raamwerken er op

		kan rekenen dat ik door te voldoen aan de criteria van het ICR tegelijk ook aantoonbaar voldoe aan de opgenomen raamwerken

ProjectNr-Resultaat	Specifieke gebruiker	EPICbeschrijving
VV065.02.01 – B1.3 Communicatie & training	Entiteiten & medewerkers Vlaamse overheid	Als gebruiker wil ik over informatieveiligheid geïnformeerd worden en bewustgemaakt worden van cybersecurity dreigingen en wat ik daaraan kan doen zodat ik minder blootgesteld word aan risico's met betrekking tot informatieveiligheid
VV065.02 – B1.2 Invoering drielijnenmodel	Entiteiten Vlaamse overheid	Als gebruiker wil ik dat de drie verdedigingslijnen zoals beschreven in het Drielijnen model voor de Vlaamse overheid gedefinieerd en geïmplementeerd worden zodat ik duidelijk weet wie welke verantwoordelijkheid heeft en ik deze kan inzetten als middel om aan risicobeheer te doen
VV065.02 – B2.1 Versterking TIV	Entiteiten Vlaamse overheid	Als gebruiker wil ik dat het TIV voldoende capaciteit en kennis heeft om haar taken en verantwoordelijkheden in te vullen zoals beschreven in de strategie informatieveiligheid zodat ik er op kan rekenen dat het TIV ondersteuning kan bieden aan de centrale dienstverlening en aan het Stuurorgaan IIB
VRD2.23.8– A1.1 Erkenning ICR	Entiteiten Vlaamse overheid	Als gebruiker wil ik dat het ICR erkend wordt door toezichthouders en regelgevers (ook buiten de Vlaamse overheid), welke daarmee aanvaarden dat aantoonbaar voldoen aan de Algemene Vo Norm ook conformiteit betekent met zijn vereisten, zodat ik door te voldoen aan het ICR in een keer gelijk voldoe aan de eisen van deze toezichthouders en regelgevers en daarmee minder administratieve lasten heb
VRD2.23.8 – A1.2 Vo-brede coördinatie	Stuurorgaan Informatie en ICT-Beleid	Als gebruiker wil ik dat er een Vo-brede coördinatie is van de invulling van de rollen en verantwoordelijkheden mbt informatieveiligheid zodat ik weet wie binnen de entiteiten aansprakelijk is voor de uitvoering van het informatieveiligheidsbeleid en dat dit door de entiteiten bevestigd wordt
VRD2.23.8 – A1.4 Dashboard 2.0	Stuurorgaan Informatie en ICT-Beleid	Als gebruiker wil ik dat het dashboard Informatieveiligheid en bescherming van persoonsgegevens verder uitgebreid wordt met aanvullende rapportages zodat ik meer inzicht heb in de stand van zaken en de risico's die ik loop en zodat ik kan bijsturen als dat nodig is

ProjectNr-Resultaat	Specifieke gebruiker	EPIC beschrijving

VRD2.23.8 – A3.2 Self-assessment 2.0	Entiteiten Vlaamse overheid	Als gebruiker wil dat een self-assessment, inclusief bijbehorend proces, ontwikkeld wordt zodat ik deze kan gebruiken om de compliance van mijn entiteit met het ICR te bepalen en deze kan vergelijken met het ambitieniveau van mijn entiteit en met een benchmark
VRD2.23.8 – A3.2 Compliance ICR 3.0 – NIS2	Entiteiten Vlaamse overheid	Als gebruiker wil ik dat de minimale normen voor compliance voor de gekozen relevante raamwerken inzichtelijk zijn en toegevoegd zijn aan het ICR zodat ik door te voldoen aan de criteria van het ICR op het relevant classificatieniveau tegelijk ook aantoonbaar voldoe aan de opgenomen raamwerken
VRD2.23.8 – B1.3 Communicatie & training	Entiteiten & medewerkers Vlaamse overheid	Als gebruiker wil ik over informatieveiligheid geïnformeerd worden en bewustgemaakt worden van cybersecurity dreigingen en wat ik daaraan kan doen zodat ik minder blootgesteld word aan risico's met betrekking tot informatieveiligheid
VRD2.23.8 – B1.2 Versterking WIV 2023	Stuurorgaan Informatie en ICT-Beleid	Als gebruiker wil ik dat de Werkgroep Informatieveiligheid-Beleid versterkt wordt met externe experts om de capaciteit, expertise en slagkracht ervan te vergroten zodat ik er op kan rekenen dat de WIV-Beleid in staat is om mijn vragen te beantwoorden en om mij van onderbouwd advies te voorzien
VRD2.23.8 – B2.1 Uitbouw TIV & dienst	Entiteiten Vlaamse overheid	Als gebruiker wil ik dat Digitaal Vlaanderen haar de dienstverlening verder uitbouwt door de capaciteit, competentie -en kennisopbouw te verhogen zodat ik een informatieveiligheidscoördinator kan inhuren uit een pool van specialisten met brede inzetbaarheid en kennis die up to date is
VRD2.23.8 – B2.3 Modelclausules	Entiteiten Vlaamse overheid	Als gebruiker wil ik dat er modelclausules ontwikkeld worden met betrekking tot contractuele risico's op gebied van informatieveiligheid en dat deze beschikbaar worden gesteld aan alle entiteiten via de aankoopcentrale zodat ik deze kan gebruiken om op te nemen in bestekteksten voor contracten met externe partijen

ProjectNrResultaat	Specifieke gebruiker	EPICbeschrijving
A1.4 Dashboard 3.0	Stuurorgaan Informatie en ICT-Beleid	Als gebruiker wil ik dat het dashboard Informatieveiligheid en bescherming van persoonsgegevens verder uitgebreid wordt met aanvullende rapportages zodat ik meer inzicht heb in de stand van zaken en de risico's die ik loop en zodat ik kan bijsturen als dat nodig is
A3.1 ICR 4.0	Entiteiten Vlaamse overheid	Als gebruiker wil ik dat ICR 3.0 verder uitgebreid wordt op basis van nieuwe ontwikkelingen in de wet- en regelgeving op het gebied van informatieveiligheid zodat ik er op kan blijven rekenen dat ik door te voldoen aan de criteria van het ICR aantoonbaar blijf voldoen aan alle daarin opgenomen raamwerken en regelgeving
A3.2 Continuering Self-assessment 2024	Entiteiten Vlaamse overheid	Als gebruiker wil dat de bestaande self-assessments verder ontwikkeld worden zodat deze nog beter te gebruiken zijn om de ontwikkeling van de maturiteit en compliance van mijn

		entiteit met het ICR te volgen en deze te vergelijken met het ambitieniveau van mijn entiteit en met een benchmark
B1.3 Communicatie & training 2024	Entiteiten & medewerkers Vlaamse overheid	Als gebruiker wil ik over informatieveiligheid geïnformeerd worden en bewustgemaakt worden van cybersecurity dreigingen en wat ik daaraan kan doen zodat ik minder blootgesteld word aan risico's met betrekking tot informatieveiligheid
B1.2 Versterking WIV 2024	Stuurorgaan Informatie en ICT-Beleid	Als gebruiker wil ik dat de Werkgroep Informatieveiligheid-Beleid versterkt wordt met externe experts om de capaciteit, expertise en slagkracht ervan te vergroten zodat ik er op kan rekenen dat de WIV-Beleid in staat is om mijn vragen te beantwoorden en om mij van onderbouwd advies te voorzien
A3.2 Proces conformiteitstoetsing	Entiteiten Vlaamse overheid	Als gebruiker wil ik dat binnen de Vlaamse overheid een proces voor een optionele conformiteitstoets ontwikkeld wordt welke vervolgens door een onafhankelijke partij uitgevoerd kan worden zodat ik een bewijs heb dat ik voldoende controle maatregelen genomen heb om (deels) te voldoen aan de criteria zoals deze in het ICR beschreven zijn

-
- algemene roadmap van de producten (ruimere scope dan enkel dit relanceproject 2023 -2024)
- Conceptuele architectuur van voorgestelde functionaliteit(en)
- ...]