Informatieclassificatie Vlaamse overheid (Vo-ICR)

Ontwikkeling en gebruik van toepassingen

Minimale maatregelen

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

Situering van het document

Dit document maakt deel uit van de begeleidende documentatie in context van het generieke informatieclassificatieraamwerk (ICR) van de Vlaamse overheid (Vo) op initiatief van het Stuurorgaan Vlaams Informatie- en ICT Beleid.

Doel van het document

Dit document beschrijft de kwaliteitseisen van de minimale maatregelen die moeten afgedwongen worden in het kader van de deelprocessen ontwikkeling en gebruik van toepassingen. Deze kwaliteitseisen worden verbonden aan de informatieklassen zoals deze zijn beschreven in het ICR van de Vo.

Werkprincipe van het document

Het huidige document bestaat uit 2 delen. Eerst worden de minimale maatregelen besproken, alvorens in het 2de deel al de nodige aanvullende informatie ter beschikking wordt gesteld.

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

Verspreiding van het document

Dit document is voornamelijk voor intern gebruik en bevat informatie die mag gedeeld worden met personen verbonden aan de Vo en zijn diensten leveranciers.

Het document mag gedeeld worden met derden onder de richtlijnen openbaarheid van bestuur van de Vlaamse regering.

Vrijwaring

Dit document geeft de huidige status en daaraan gerelateerde informatie binnen het project weer. Gelieve de auteur of de bevoegde project begeleiders te contacteren om zich ervan te vergewissen dat u de laatst gevalideerde versie van dit document in handen heeft.

Eigenaar

Voorzitter werkgroep informatieveiligheid | Digitaal Vlaanderen

security@vlaanderen.be

Classificatie

Dit document valt onder de vertrouwelijkheidsklasse 1 (Publiek) en mag toegankelijk zijn voor iedereen.

Dit document valt onder integriteitsklasse 2. De organisatie heeft **geen directe hinder** indien de informatie gewijzigd wordt door onbevoegden en de **dienstverlening blijft gegarandeerd**. Maar bijsturing van de criteria en/of maatregelen is aangewezen.

Historiek

	Datum	Auteur	Opmerkingen
v.0.1	3 december 2019	Beau JANSSEN	Eerste versie
v.0.2	29 juni 2020	Beau JANSSEN	Tweede versie, na input van Johan Smekens en Kristel Van Aken
v.0.3	13 juli 2020	Beau JANSSEN	Bijkomende input van Kristel Van Aken
v.1.0	20 augustus 2020	Beau JANSSEN	Finale versie na review Johan Smekens/Kristel Van Aken
v.1.1	28 augustus 2020	Beau JANSSEN	Toevoegingen en preciseringen na Taakgroep 27/08/2020
v.1.2	24 september 2020	Beau JANSSEN	Toevoegingen na de Werkgroep Informatieveiligheid 22/09/2020
v.1.3	6 augustus 2021	Beau JANSSEN	Aanpassingen voor integratie van kwaliteitskenmerk “Beschikbaarheid”
v.2.0	22 juli 2022	Kristel VAN AKEN	Verbeteren leesbaarheid Geen inhoudelijke wijzigingen
V.2.1	17 oktober 2023	Nele Lowet	Update KSZ

Bronnen en verwijzingen

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

Documentverwijzingen:

- https://raygun.com/blog/software-development-life-cycle/#sdlc-infographic
- https://en.wikipedia.org/wiki/Software_development_process
- “Application Level Security Management”, Michael Neuhaus
- https://www.norea.nl/download/?id=3636

Inhoudsopgave

INLEIDING

Dit document beschrijft de rol van integriteit van en in toepassingen. We bekijken dit vanuit twee perspectieven:

1. De integriteit van de toepassing (software, applicatie) zelf
2. De data die deze toepassing gebruikt

Als we controles beschrijven die de toepassing in haar geheel beschermen, impliceert dat dikwijls dat de data erin dat ook is. Omgekeerd geldt hetzelfde: maatregelen die de data beschermen, beschermen indirect ook de gehele toepassing.

We beschrijven in dit document met name maatregelen rond integriteit omdat dit aspect in het ICR onderbelicht is geweest. In andere Beleidsdocumenten (Organisatie, Cryptografie, *Software Life Cycle*, etc.) staan voldoende maatregelen beschreven om de vertrouwelijkheid van een toepassing te borgen. Vandaar dat dat aspect in dit Beleidsdocument niet aan bod komt.

De focus van het hele proces ligt op de concepten “Security by Design” en “Privacy by Design”. Deze concepten zorgen ervoor dat je de kosten voor het bouwen, onderhouden en omgaan met toepassingen en systemen een pak goedkoper, veiliger en duurzamer kunt inregelen.

We bekijken deze integriteitsrol in de verschillende fases van deze cyclus. In dit document onderscheiden we 7 stappen:

1. Planning
2. Behoefteanalyse
3. Design
4. Ontwikkeling
5. Testing
6. Uitrol
7. Onderhoud

In elk van deze fases geven we aan welke informatierisico’s je moet overwegen en hoe je deze kunt mitigeren.

De beschrijving van deze cyclus staat los van de gebruikte methode om code te ontwikkelen, bv. “Waterfall” of “Agile”. Waar er speciale aandacht nodig is voor ingekochte toepassingen, vermelden we dit expliciet.

1. MINIMALE MAATREGELEN

1.1 Minimale algemene maatregelen

Vertrouwelijkheid

Er zijn geen minimale maatregelen rond vertrouwelijkheid.

Integriteit

IC klasse	Minimale maatregelen
	〉 Uitvoeren van een risicoanalyse op nieuwe versie van een toepassing 〉 Werken volgens de "security by design" en "privacy by design" principes 〉 Kosten-baten-analyse 〉 Het uitvoeren van Veiligheidstesten, cf. het Beleidsdocument "Veiligheidstesten" 〉 Het uitvoeren van Security Monitoring-activiteiten, cf. het Beleidsocument "SIEM" 〉 Ondersteuning van de toepassing en haar onderliggende componenten, cf. het Beleidsdocument "*Software Lifecycle Management*"
	Alle maatregelen van Klasse 1 + 〉 Input validatie (manueel en automatisch) 〉 Output validatie op statische en niet-statische data 〉 Output validatie: controle op inputvelden
	Alle maatregelen van Klasse 1 + Klasse 2 + 〉 Expliciete garantie op betrouwbaarheid van de informatiebronnen 〉 Output validatie: controle op inputvelden via bijvoorbeeld "4-ogen-principe" 〉 Monitoring van ongeoorloofde wijzingen aan data 〉 Output verificatie door ontvangende toepassing/proces
	Alle maatregelen van Klasse 1 + Klasse 2 + Klasse 3 〉 Geen bijkomende maatregelen zijn gedefinieerd 〉 De uitvoering en *thresholding* ervan kan wel verschillen, gelet op de potentieel grotere impact van een gebrek aan integriteit
	Alle maatregelen van Klasse 1 + Klasse 2 + Klasse 3 + Klasse 4 + 〉 Geen bijkomende maatregelen zijn gedefinieerd 〉 De uitvoering en *thresholding* ervan kan wel verschillen, gelet op de potentieel grotere impact van een gebrek aan integriteit

Beschikbaarheid

Er zijn geen minimale maatregelen rond beschikbaarheid.

1.2 Minimale specifieke (GDPR) maatregelen

Er zijn op heden geen minimale specifieke maatregelen geïdentificeerd op basis van de criteria beschreven in de GDPR (en aanverwante) regelgeving.

1.3 Minimale specifieke (NISII) maatregelen

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

1.4 Minimale specifieke (KSZ) maatregelen

Volgens de Minimale Normen van de Kruispuntbank Sociale Zekerheid moeten volgende maatregelen in het kader van de ontwikkeling en gebruik van toepassingen toegepast worden:

Integriteit en vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: 〉 Logbeheer moet meegenomen worden vanaf het design tijdens de ontwikkeling of bij de bepalingen van aankoopcriteria van toepassingen of systemen om “security/privacy by design” te realiseren (Ref. KSZ 5.9.5). 〉 Elke organisatie moet een efficiënte en constructieve communicatie opzetten tussen de verschillende bij het project betrokken partijen (inclusief klanten en leveranciers), in het bijzonder met de veiligheidsconsulent(en). Dit moet een adequaat niveau van informatieveiligheid en privacy garanderen gekend door iedereen (Ref. KSZ 5.11.1). 〉 Wanneer een programma ontwikkeld wordt waarin de sociale zekerheidsinstelling een programmanummer overneemt in een bericht dat ze aan de KSZ richt, maar een natuurlijk persoon aan de basis van dit bericht ligt, in staat zijn zelf de relatie te leggen tussen dit programmanummer en de identiteit van de natuurlijke persoon die het bericht verstuurt (Ref. KSZ 5.11.2). 〉 Elke organisatie dient altijd een controlelijst te voorzien voor de projectleider zodat de projectleider er zich kan van vergewissen dat het geheel van de beleidslijnen informatieveiligheid en privacy correct geëvalueerd en indien noodzakelijk geïmplementeerd worden tijdens de ontwikkelingsfase van het project (Ref. KSZ 5.11.4). 〉 Elke organisatie moet zich via de verantwoordelijke van de opvolging, de project leider, en bij de in productiestelling van het project er van vergewissen dat de veiligheids- en privacy-vereisten die bij het begin van het project werden vastgelegd ook daadwerkelijk geïmplementeerd werden. (Ref. KSZ 5.11.5). 〉 Elke organisatie moet onder de supervisie van de projectleider de voorzieningen voor ontwikkeling, test en/of acceptatie en productie scheiden – inclusief de bijhorende scheiding der verantwoordelijkheden in het kader van het project. (Ref. KSZ 5.11.6).

	〉 Elke organisatie moet: o a) Elke toegang tot persoonlijke en vertrouwelijke gegevens die sociaal of medisch van aard zijn, loggen in overeenstemming met de beleidslijnen "logging" en de toepasselijke wetgeving en regelgeving. o b) In de specificaties van een project opnemen hoe de toegang tot en het gebruik van systemen en applicaties gelogd zal worden om bij te dragen tot de detectie van afwijkingen van de beleidslijnen informatieveiligheid en privacy. Het logbeheer moet minimaal beantwoorden aan de volgende doelstellingen : ▪ a. Glashelder, snel en eenvoudig kunnen bepalen wie, wanneer en op welke manier toegang heeft verkregen tot welke informatie ▪ b. De identificatie van de aard van de geraadpleegde informatie ▪ c. De duidelijke identificatie van de persoon o c) rekening houden met reeds bestaande logbeheersystemen bij de evaluatie van logbehoeften in het kader van het project. o d) De noodzakelijke tools ter beschikking hebben of ontwikkelen om toe te laten deze log gegevens uit te baten door de geautoriseerde personen. o e) De algemene regel toepassen dat de transactionele/functionele log gegevens minimaal 10 jaar en de technische/infrastructurele log gegevens minimaal 2 jaar moeten bewaard blijven (Ref. KSZ 5.11.7). 〉 Elke organisatie moet: a. In de loop van de ontwikkeling van een project de procedures met betrekking tot het incidentbeheer formaliseren en valideren. Dit moet toelaten het ontwikkelde systeem te integreren in het standaard incident beheerssysteem van de organisatie. b. ervoor zorgen dat de veiligheidsconsulent op de hoogte wordt gesteld van de veiligheids- en privacy-incidenten in de loop van de ontwikkeling van een project. (Ref. KSZ 5.11.10) 〉 Elke organisatie moet de 'secure project lifecycle' toepassen zoals beschreven in de bijlage C van de beleidslijn 'Aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen'(Ref. KSZ 5.11.14). 〉 Bijlage C van de beleidslijn 'Aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen' omvat volgende stappen: o Initiatie o Planning o Realisatie ▪ Ontwikkeling en test ▪ In productiestelling o Afsluiting 〉 Elke organisatie moet de nodige maatregelen treffen om de veiligheid te garanderen op toepassingsniveau teneinde eventuele informatieveiligheidsinbreuken te vermijden (vertrouwelijkheid, integriteit, beschikbaarheid) (Ref. KSZ 5.11.15).

Beschikbaarheid

IC klasse	Minimale maatregelen

Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen:

〉 Logbeheer moet meegenomen worden vanaf het design tijdens de ontwikkeling of bij de bepalingen van aankoopcriteria van toepassingen of systemen om “security/privacy by design” te realiseren (Ref. KSZ 5.9.5).

〉 Elke organisatie moet een efficiënte en constructieve communicatie opzetten tussen de verschillende bij het project betrokken partijen (inclusief klanten en leveranciers), in het bijzonder met de veiligheidsconsulent(en). Dit moet een adequaat niveau van informatieveiligheid en privacy garanderen gekend door iedereen (Ref. KSZ 5.11.1).

〉 Wanneer een programma ontwikkeld wordt waarin de sociale zekerheidsinstelling een programmanummer overneemt in een bericht dat ze aan de KSZ richt, maar een natuurlijk persoon aan de basis van dit bericht ligt, in staat zijn zelf de relatie te leggen tussen dit programmanummer en de identiteit van de natuurlijke persoon die het bericht verstuurt (Ref. KSZ 5.11.2).

〉 Elke organisatie dient altijd een controlelijst te voorzien voor de projectleider zodat de projectleider er zich kan van vergewissen dat het geheel van de beleidslijnen informatieveiligheid en privacy correct geëvalueerd en indien noodzakelijk geïmplementeerd worden tijdens de ontwikkelingsfase van het project (Ref. KSZ 5.11.4).

〉 Elke organisatie moet zich via de verantwoordelijke van de opvolging, de project leider, en bij de in productiestelling van het project er van vergewissen dat de veiligheids- en privacy-vereisten die bij het begin van het project werden vastgelegd ook daadwerkelijk geïmplementeerd werden. (Ref. KSZ 5.11.5).

〉 Elke organisatie moet onder de supervisie van de projectleider de voorzieningen voor ontwikkeling, test en/of acceptatie en productie scheiden – inclusief de bijhorende scheiding der verantwoordelijkheden in het kader van het project. (Ref. KSZ 5.11.6).

〉 Elke organisatie moet:

- a) Elke toegang tot persoonlijke en vertrouwelijke gegevens die sociaal of medisch van aard zijn, loggen in overeenstemming met de beleidslijnen “logging” en de toepasselijke wetgeving en regelgeving.
- b) In de specificaties van een project opnemen hoe de toegang tot en het gebruik van systemen en applicaties gelogd zal worden om bij te dragen tot de detectie van afwijkingen van de beleidslijnen informatieveiligheid en privacy. Het logbeheer moet minimaal beantwoorden aan de volgende doelstellingen :
  - a. Glashelder, snel en eenvoudig kunnen bepalen wie, wanneer en op welke manier toegang heeft verkregen tot welke informatie
  - b. De identificatie van de aard van de geraadpleegde informatie
  - c. De duidelijke identificatie van de persoon
- c) rekening houden met reeds bestaande logbeheersystemen bij de evaluatie van logbehoeften in het kader van het project.
- d) De noodzakelijke tools ter beschikking hebben of ontwikkelen om toe te laten deze log gegevens uit te baten door de geautoriseerde personen.
- e) De algemene regel toepassen dat de transactionele/functionele log gegevens minimaal 10 jaar en de technische/infrastructurele log gegevens minimaal 2 jaar moeten bewaard blijven (Ref. KSZ 5.11.7).

〉 Elke organisatie moet de deliverables van het project integreren in het backup beheersysteem van de organisatie zoals opgelegd in de beleidslijnen. Dit omvat

	niet alleen de gegevens die verwerkt worden maar ook de documentatie die hierop betrekking heeft (broncode, programma's, technische documenten, …). De backup dient regelmatig getest te worden via een herstel ("restore") oefening om na te gaan of de informatie überhaupt wel recupereerbaar is en hoelang dergelijke herstel opdracht duurt (Ref. KSZ 5.11.8). 〉 Elke organisatie moet: a. In de loop van de ontwikkeling van het project de behoeften met betrekking tot continuïteit van de dienstverlening formaliseren, conform met de verwachtingen van de organisatie. ○ b. In de programma's de te definiëren herstartpunten duidelijk integreren om het hoofd te bieden aan operationele problemen. Deze informatie maakt deel uit van het exploitatie dossier. ○ c. Tijdens de ontwikkeling van een project bijzondere aandacht besteden aan backup en herstel ("restore") van informatie d. In de productie omgeving rekening houden met de eisen van de instelling met betrekking tot probleemtolerantie en redundantie van de infrastructuur e. Het continuïteitsplan en de bijhorende procedures actualiseren in functie van de projectevolutie, met inbegrip van continuïteitstesten ○ f. een risico analyse in het begin van het project uitvoeren om de noodprocedures te definiëren. Deze moeten bevatten : ▪ De werking bij verminderde beschikbaarheid van informatie systemen ▪ De beschrijving van alternatieve informatie systemen met inbegrip van de uitrol, de exploitatie modaliteiten en de eventuele ontwikkeling van noodsystemen ▪ De kerntaken en kernprocedures in geval van systeemonderbreking ▪ • De taken, de sleutelrollen en de in te zetten middelen om tot een optimale beschikbaarheid te komen (Ref. KSZ 5.11.9). 〉 Elke organisatie moet: ○ a. In de loop van de ontwikkeling van een project de procedures met betrekking tot het incidentbeheer formaliseren en valideren. Dit moet toelaten het ontwikkelde systeem te integreren in het standaard incident beheerssysteem van de organisatie(Ref. KSZ 5.11.10). ○ b. ervoor zorgen dat de veiligheidsconsulent op de hoogte wordt gesteld van de veiligheids- en privacy-incidenten in de loop van de ontwikkeling van een project (Ref. KSZ 5.11.10). 〉 Elke organisatie moet de 'secure project lifecycle' toepassen zoals beschreven in de bijlage C van de beleidslijn 'Aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen'(Ref. KSZ 5.11.14). 〉 Bijlage C van de beleidslijn 'Aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen' omvat volgende stappen: ○ Initiatie ○ Planning ○ Realisatie ▪ Ontwikkeling en test ▪ In productiestelling ○ Afsluiting 〉 Elke organisatie moet de nodige maatregelen treffen om de veiligheid te garanderen op toepassingsniveau teneinde eventuele informatieveiligheidsinbreuken te vermijden (vertrouwelijkheid, integriteit, beschikbaarheid) (Ref. KSZ 5.11.15).

Met opmerkingen [NL1]: beschikbaarheid

2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1. De stappen in de *Software Development Lifecycle*

In dit overzicht schetsen we kort de 7 stappen in de *Software Development Lifecycle*.

Planning

Dit deel van de levenscyclus bevat de praktische aspecten van de te plannen taken:

- Welke resources heb je nodig (mensen en materiaal)?
- Wat is de geraamde kost?
- Binnen welke timing wil ik live zijn?
- Etc.

Behoefteanalyse

Je moet tot een volledig beeld komen van alle behoeftes. Deze kunnen zowel functioneel als niet-functioneel zijn. Hiervoor ga je te raden bij alle relevante partijen bij de business- en de ICT-diensten, en bij experts in de materie.

In deze fase analyseer je ook de behoeftes rond privacy en informatieveiligheid om deze zo vroeg mogelijk te kennen en hun impact te kunnen inschatten. Dit noemen we ook wel *security by design* en *privacy by design* (zie ook later in het document voor meer details).

Hier is het van belang dat je goed inschat welke informatieklasse de behandelde informatie in jouw toepassing/proces heeft. Deze is namelijk bepalend voor welke controles je kunt, of moet implementeren en hoe. Ook al zijn de meeste van deze *requirements* niet-functioneel, ze hebben ook een invloed op hoe de toepassing werkt en op de exploitatiekost.

Opmerking: *Hierbij verwijzen we naar de maatregelen die in alle andere Beleidsdocumenten beschreven staan, en ook samengevat zijn in het "Overzicht baseline maatregelen" beschikbaar op de site van het Security Office van Het Facilitair Bedrijf.*

Je komt tot een geconsolideerde en uniform geaccepteerde lijst van behoeftes (*requirements*) die je gaat implementeren. Afhankelijk van je ontwikkelmethode (bv. *Waterfall* of *Agile*), kan deze lijst een andere vorm aannemen.

Design

Een keer dat de behoeftes duidelijk zijn uitgelijnd, werk je het ontwerp uit. Hoe vertaal je die behoeftes concreet zodat je ze kunt inpassen in een operationele context? Hoe maak je maximaal gebruik van bestaande componenten?

De output is een ontwerp van de beoogde oplossing.

Ontwikkeling

In deze fase ga je effectief over tot de concrete ontwikkeling van de software. Dit kan op verschillende manieren gebeuren: ofwel in kleine stukken (*Agile*), ofwel in één keer (*Waterfall*).

Hierbij is het belangrijk om regelmatig af te stemmen met de personen die behoeftes hebben geformuleerd, zodat je zeker bent dat je een antwoord biedt op hun behoeftes.

Testing

De testfase is van belang om je ervan te vergewissen dat alles werkt zoals het hoort. Er zijn allerlei soorten tests die je best onderneemt om de juiste werking van je software te testen, zowel als programma op zichzelf als binnen de context waar de software terecht komt. Hierbij kan het gaan om (geen exhaustieve lijst):

- De kwaliteit van de code
- Unit testen
- Integratietesten
- Performantietesten
- Security testen

Een groot deel van deze testen kun je automatiseren. Dit vermindert de werklast en verlaagt ook de kans op fouten in de testen.
Ook in deze fase test je de geïmplementeerde controles die je in de analysefase hebt geïdentificeerd. Dit gaat om zowel puur procedurele controles als om de verificatie van de *security* en *privacy by design*-principes.
Deze testen laat je aftekenen door de toepassingseigenaar zodat je er zeker van bent dat de geplande implementatie de beoogde resultaten haalt.

Uitrol

De uitrol van de software is een proces op zich en gebeurt liefst zo automatisch mogelijk. Het controleniveau hiervoor staat beschreven in het document “Release en Deployment Beheer” beschikbaar op de SharePoint van het Security Office Team van het Facilitair Bedrijf.

Als de uitrol van een software functionele of proceswijzigingen bevat, moet je de eindgebruikers hiervan op de hoogte stellen en, indien nodig, opleiden.

Onderhoud

De levenscyclus stopt niet bij het opleveren en in productie zetten van de software. Eenmaal live, moet je continu monitoren dat de software naar behoren werkt. Als er problemen ontstaan of als er bugs voorkomen, moet je deze aanpakken en oplossen.

Dit geldt ook voor het up-to-date houden van de controles voor security en privacy. De evoluties in de gebruikte technieken en controles zelf moet je volgen. Het ICR evolueert ook: nieuwe controles kunnen er bijkomen en verwachtingen rond bestaande controles kunnen veranderen. Deze communiceert het Security Office uiteraard wel via de geijkte *governance* kanalen.

Door het eigenlijk gebruik van de software kunnen er ook nieuwe behoeftes naar boven komen. Deze kunnen dienen als input voor verdere verbeteringen.

Een uiteindelijke stap in het Onderhouds-proces is het afvoeren van een toepassing. Hierbij moet je analyseren in welke mate je de business of technische data nog nodig hebt. Denk hierbij aan wettelijke termijnen van opslag, bijvoorbeeld.

Als je toepassing een deel van een proces ondersteunt, moet je er zeker van zijn dat het proces in zijn geheel kan blijven werken zonder jouw toepassing. Dit kan door een vervangende toepassing, of met *work arounds*.

2.2. Het beheer van informatierisico en -veiligheid in deze cyclus

2.2.1. *Security/Privacy by Design*

Je betrekt de security en privacy teams zo snel mogelijk in de uitwerking van je software. Hoe vroeger je dit doet, hoe makkelijker je dit kunt integreren in het design of het ontwerp.

Hoe vroeger je dit doet, hoe goedkoper ook. Volgens een Gartner-rapport is "de kost om een security kwetsbaarheid in productie te verwijderen 30 tot 60 keer duurder is dan de kwetsbaarheid te verwijderen tijdens de ontwerpfase" (eigen vertaling). Kostenefficiënte ontwikkeling houdt dus zo snel mogelijk rekening met security vereisten.

Hetzelfde geldt voor het privacy-aspect. Hoe sneller je een concreet zicht hebt op welke behoeften je moet beantwoorden, hoe makkelijker je ze kunt integreren. Ook hier geldt het kostenbesparend aspect.

Norea heeft specifiek voor het *privacy by design*-aspect adviezen gepubliceerd, waarin ze enkele principes aanbevelen om dit mogelijk te maken (zie link, vanaf slide 23).

Security en *Privacy by Design* helpen er ook voor zorgen dat gebruikers en beheerders de functionele eigenschappen van een toepassing op een veilige manier kunnen gebruiken. Het combineert én de functionaliteit, de privacy én de veiligheid.

2.2.2. Informatieclassificatie

Bij het ontwikkelen van (nieuwe) software, moet je nagaan in welke Informatieklasse je informatie valt. Dit is een oefening die je kunt doen aan de hand van het Beleidsdocument "Informatie Classificatie- Organisatie". Er staan ook andere tools ter beschikking via de website vlaanderen.be/informatieveiligheid.

Het resultaat van deze oefening valideer je samen met de Veiligheidsconsulent en/of *Data Protection Officer* binnen jouw entiteit.

Belangrijk hierbij is om te kijken naar de verschillende kwaliteitskenmerken van je toepassing: vertrouwelijkheid, integriteit en beschikbaarheid. De eisen en controles die je verwacht voor elk van deze kenmerken kunnen heel anders zijn.

Alle controles die hierbij noodzakelijk zijn, staan beschreven in het ICR. Ook over deze lijst met controles kun je advies vragen aan de persoon die binnen jouw entiteit verantwoordelijk is voor Informatieveiligheid en Privacy.

2.2.3. Risicoanalyse

Bij het *releasen* van (nieuwe) software, is het niet de bedoeling om nodeloze risico's te introduceren. Om een volledig beeld van je risicolandschap te krijgen, voer je een risicoanalyse uit.

Dit doe je in samenspraak met alle belanghebbenden, inclusief een Veiligheidsconsulent en een *Data Protection Officer*. Verandert het risicolandschap? Valideer dit met je leidend ambtenaar of hun gedelegeerde.

Opmerking: Dit proces staat beschreven in het document "Proces risicobeheer", beschikbaar op de site het Security Office.

Binnen datzelfde proces stelt het Security Office ook tooling ter beschikking (via de SharePoint van het team) die rekening houdt met alle requirements uit het gevalideerde proces.

2.3. Security per processtap

Planning

Tijdens de planningsfase is het vooral van belang dat je de kosten van en voor security in je budget meetelt. Dit zowel voor het ontwikkelen van of aansluiten op bestaande security bouwstenen, als het integreren van security in de business werking van je toepassing. Als je hiervoor geen budget voorziet vanaf het begin, kun je later in het proces in de problemen komen qua oplevertermijn of voorzien budget.

Hierbij hou je rekening met de verschillende kwaliteitskenmerken: vertrouwelijkheid, integriteit en beschikbaarheid. Elk kenmerk heeft specifieke noden waaraan je moet voldoen en die een invloed hebben op oplevertermijnen en budget.

Opmerking: Het Facilitair Bedrijf biedt enkele Veiligheidsbouwstenen aan om toepassingen te beveiligen. Deze zijn niet verplicht af te nemen. Wel leveren ze ontzorging: de ontwikkeling en het onderhoud ervan is altijd in mijn met de geldende normen binnen het ICR.

Deze bouwstenen hebben altijd als objectief de Vertrouwelijkheid, Integriteit en Beschikbaarheid van de betrokken toepassingen en hun data te borgen.

Behoefteanalyse

Nadat je de inschatting gemaakt hebt van je informatieklasse, kun je op basis van de klasse zien welke controles je effectief moet implementeren. Het hoe hiervan hangt uiteraard af van de context en technische invulling van je toepassing. Het is belangrijk dat je deze controles in je analyse opneemt als niet-functionele behoeftes en deze in de scope van je ontwikkeling opneemt.

Je verzamelt ook alle behoeften rond het naleven van de kwaliteitseisen rond vertrouwelijkheid en integriteit van de verantwoordelijke voor het proces en/of de toepassing. Deze behoeften vertalen zich dan naar controles die je implementeert, onder andere op basis van het ICR.

Controles die je kunt overwegen afhankelijk van het proces waarin de toepassing tussenkomt:

- Betrouwbaarheid van de informatiebronnen
- Hoe hoger de informatieklasse rond Integriteit, hoe hoger de noodzaak om een betrouwbare informatiebron te hebben. De betrouwbaarheid van een leverancier heeft een grote invloed op de waarde die deze data heeft.

- Vanaf Integriteit klasse 3 moet de betrouwbaarheid van de informatiebron gegarandeerd kunnen zijn.

Opmerking: *Hoe je in deze context om kunt gaan met authentieke bronnen,* staat op pagina 14 beschreven.

- Integriteit van de aangeleverde data/input
- De verschillende methodes om input te genereren zijn: automatisch en manueel.
- Voor manuele input van data moet je bepaalde controles implementeren afhankelijk van de context van de toepassing
  - Het kan gaan om data input validatie van bepaalde velden (alfanumeriek, grenswaarden, preselectie van waarden, etc.)
    - Dit is relevant vanaf klasse 2
  - Bij automatische input van data definieer je welke data je nodig hebt en welk formaat deze moeten hebben. Als de bronformaten anders zijn dan de inputformaten die jouw toepassing nodig heeft, voorzie je een mechanisme om fouten te detecteren en remediëren
    - Dit is relevant vanaf klasse 2
- Validatie van de output van het proces
- Data kan statisch of niet-statisch zijn in een proces
- Statische data moet aantoonbaar niet-gewijzigd zijn door het proces. Dit kun je aantonen met:
  - Een audit trail
  - Checks op de data zelf, die verifieert dat de data inderdaad niet gewijzigd is
  - *Business tracking*, waarbij je een staal neemt van de data om manueel/automatisch te verifiëren dat er geen wijzigingen gebeurd zijn
  - Meta-validaties, bijvoorbeeld via *hash* functies, *total counts* op tabellen, etc.
    - Dit is relevant vanaf klasse 2
- Voor niet-statische data moet aantoonbaar zijn dat de wijzigingen legitiem zijn. Dit doe je door:
  - Een audit trail
  - Een validatie van het ontvangende proces dat de datakwaliteit aan de verwachtingen voldoet
  - *Business tracking*, waarbij je een staal neemt van de data om manueel/automatisch te verifiëren dat de gebeurde wijziging aan de verwachtingen voldoen
    - Dit is relevant vanaf klasse 2
- Operationele controles op de wijzigingen van de data
- Om fouten te vermijden, bouw je controles in om te verifiëren dat gebeurde wijzigingen correct zijn. Dit kan gaan om:
  - Controles op de inputvelden – denk hierbij aan het verifiëren van de *data requirements* (logische checks op naam, adres, rijksregisternummer, etc.)
    - Dit is relevant vanaf klasse 2
  - Controles op de invoer van data – denk hierbij bijvoorbeeld aan een “4-ogen principe” en dan bij voorkeur een “blind 4-ogen principe”, waarbij twee personen dezelfde input moeten ingeven, los van elkaar en er een automatische controle gebeurt op de juistheid ervan. Is er een verschil tussen beide *inputs*, gebeurt er een aparte controle
    - Dit is relevant vanaf klasse 3
  - Technische controles de wijzigingen van de data

- Je bepaalt vooraf welke data kan wijzigen en hoe. Als er een afwijking van deze normen gebeurt, stel je een waarschuwing in om verder te onderzoeken. De afhandeling gebeurt bijvoorbeeld volgens het incidentproces
  - Dit is relevant vanaf klasse 3
- Je kunt dit ook verifiëren met de toepassingen/processen die jouw output nodig hebben en laten nakijken of jouw output aan de verwachte kwaliteitseisen voldoet. Als dit aanpassingen in een andere toepassing vergt, moet je dit uiteraard in overleg met de toepassingseigenaar implementeren
  - Dit is relevant vanaf klasse 3

Dit zijn uiteraard enkel voorbeelden. Er zijn ook andere controles die de integriteit van data kunnen garanderen. Afhankelijk van je specifieke context, moet je andere controles implementeren.

Het objectief is wel altijd om tot een aanvaardbaar risiconiveau te komen. Als er controles gedefinieerd zijn in het ICR die geen risicovermindering opleveren, of die net risico toevoegen, breng je dit in kaart en valideer je dit met een Veiligheidsconsulent en/of *Data Protection Officer*.

Zijn er bepaalde controles die je niet opportuun zijn om in te voeren, dan moet je kijken in welke mate dit een risicoverhoging inhoudt en dit afchecken met een Veiligheidsconsulent en/of *Data Protection Officer*. Mogelijks moet de leidend ambtenaar of hun gedelegeerde dit ook goedkeuren.

Het gebruik van authentieke bronnen

Bij het gebruik van authentieke bronnen, moet je er als ontvangende toepassing van uitgaan dat de ontvangen informatie correct is. Blijkt uit objectieve feiten, waarnemingen of stukken dat de aangereikte informatie niet juist is, kun je deze in de toepassing wijzigen.

Zorg er wel voor dat je de bewijzen hiervoor opslaat, zodat je de gemaakte wijziging kunt staven.

Voorzie ook een feedback richting authentieke bron, waarbij de te corrigeren informatie vermeldt en de bewijzen meelevert die aantonen dat de geleverde data foutief is.

Als de authentieke bron zijn gegevens niet aanpast, zul je de manuele correctie in jouw toepassingen moeten blijven herhalen. Het is aan te raden deze fout telkens opnieuw te melden aan de authentieke bron.

Design

Tijdens de design-fase maak je de afweging tussen business functionaliteit en mogelijke risico's. Hierbij hou je ook rekening met de controles die je moet implementeren (zoals hierboven beschreven) en hoe je deze integreert in je toepassing en het daaraan verbonden proces.

Dit kan leiden tot verschillende uitkomsten:

- De functionaliteit kan primeren en je introduceert een risico. Dit moet je dan inschatten en aanvaarden in samenspraak met een Veiligheidsconsulent, een *Data Protection Officer* en/of een leidend ambtenaar of hun gedelegeerde;
- Security primeert en je wijzigt de functionaliteit. Hiervoor moet je uiteraard een akkoord krijgen van de belanghebbenden;
- Je vindt een evenwicht tussen beiden met een wijziging in functionaliteit en een vermindering in security. Hiervoor spreek je alle belanghebbenden aan, inclusief een Veiligheidsconsulent, *Data Protection Officer* en de leidend ambtenaar of hun gedelegeerde.

Dit is gelinkt aan het proces Risicobeheer. Het proces en de tools om hiermee aan de slag te kunnen staan beschreven op de site van het Security Office.

Ontwikkeling

Tijdens de ontwikkeling, specifiek tijdens het schrijven van de code, hou je rekening met gangbare praktijken van *secure coding*. Specifiek kijk je naar de OWASP-top 10 en verzeker je je ervan dat je geen van deze kwetsbaarheden introduceert in code. Gebruik hiervoor automatische tools.

Behalve de puur security aspecten, kijk je ook naar de uitwerking van de controles die je bepaald hebt. De vertrouwelijkheid en integriteit van de informatie die je behandelt, moet doorheen het hele proces gegarandeerd zijn. Het is enkel zo dat de input aan de verwachte kwaliteitseisen kan voldoen.

De exacte implementatie hiervan verschilt per toepassing en hangt uiteraard sterk af van de informatieklasse voor deze kwaliteitskenmerken.

Voor de specifieke eisen rond het testen van de veiligheid van een toepassing tijdens de ontwikkeling ervan, raadpleeg je het Beleidsdocument "Veiligheidstesten". Hierin zit ook een rechtstreekse link met de informatieclassificatie van een toepassing. Hoe hoger de klasse, hoe strenger het controleniveau.

Testing

Tijdens het testen, test je ook de veiligheid van je toepassing in de specifieke context waarbinnen die zal functioneren. Dit kun je doen in de Test&Integratie-omgeving en in de Acceptatie-omgeving. Dit soort oefening kijkt naar hoe de processen binnen de toepassing werken en hoe iemand binnen deze processen veiligheidslekken kan uitbuiten. Hiervoor gebruik je ook automatische tools.

Tegelijkertijd moet je erin deze fase zeker van zijn dat de toepassing geschikt en inzetbaar is.

Meer details hierover staan beschreven in het document "Life Cycle Management".

Uitrol

Specifieke controles die je binnen deze processtap moet uitvoeren, staan uitgelegd in het Beleidsdocument "Release en Deployment Beheer".

Onderhoud

Veiligheidstesten

Van zodra je toepassing in productie staat, moet je de veiligheid ervan blijven borgen. Dit kan op verschillende manieren:

- Via security monitoring: je definieert welke evenementen je wilt loggen en monitoren. Meer details hierover vind je in het Beleidsdocument "Informatieclassificatie – SIEM";
- Via penetratietests: je bepaalt de scope van de test en laat die regelmatig uitvoeren op je productie-omgeving;
- Via *bug bounty* of *responsible disclosure* programma's: je nodigt zogenaamde *white hat hackers* uit om kwetsbaarheden op je toepassingen te melden en beloont hen hiervoor.

Dit staat beschreven in het Beleidsdocument "Veiligheidstesten".

(*Extended*) *support*

Eenmaal een toepassing in productie staat, moet je als beheerder ervoor zorgen dat je deze voldoende kunt ondersteunen. Dit geldt voor de gebruikers en voor de infrastructuur – en zeker ook voor de diensten die afhangen van leveranciers. Het is aan de beheerder van de toepassing om ervoor te zorgen dat de toepassing altijd een gepaste ondersteuning geniet.

2.4. Rollen en verantwoordelijkheden

Volgende rollen en verantwoordelijkheden werden vastgelegd op basis van een klassiek RACI-model.

	Uitvoeder (Responsible)	**Aansprakelijke** (Accountable)	**Raadpleging** (Consultable)	**Informeren** (Informed)
Toepassen van maatregelen	Data-eigenaar, lid van de organisatie.	Leidend ambtenaar	DPO(*) CSO(*)	Leden van het Stuurorgaan Vlaams Informatie en ICT-beleid

DPO: Data Protection Officer
CSO: Chief Security Officer
(*) delegatie aan veiligheidsconsulent is mogelijk