Vlaamse overheid

Thema-audit IT-beveiliging Vlaamse overheid

Globaal rapport | 5 november 2021

AUDIT VLAANDEREN

Auditteam

Jens Baetens, Senior Auditor (Deloitte)
Liese De Proost, Senior Auditor (Deloitte)
Evert Koks, Manager-Auditor (Deloitte)
Jan Vanhaecht, Partner (Deloitte)
Karel Bruneel, Senior Auditor
Gunter Schryvers, Manager-Auditor

Deze opdracht is uitgevoerd in overeenstemming met de internationale standaarden van het Institute of Internal Auditors (IIA).
Elke vijf jaar evalueert een externe instantie of Audit Vlaanderen deze standaarden naleeft.

Inhoudsopgave

I. Inleiding

Vlaamse overheid

AUDIT VLAANDEREN

Context van de thema-audit IT-beveiliging 2020-2021

- Zowel wereldwijd als binnen de Vlaamse administratie neemt het belang van ICT en bijgevolg van cybersecurity almaar toe. Dit wordt o.a. geïllustreerd door:
  - de ICT-risicoanalyse voor de Vlaamse administratie uit 2018;
  - de relevantie van cybersecurity-risico's volgens het Institute of Internal Auditors;
  - de incidenten bij de lokale besturen en de Vlaamse administratie met phishing en ransomware;
  - de bevindingen en langzame realisatie van de aanbevelingen van voorgaande thema-audits informatiebeveiliging bij de Vlaamse Administratie (2014-2015) en bij de lokale besturen (2017-2018).

- Bovenvermelde bevindingen en incidenten geven aanleiding tot bezorgdheid omtrent de beheersing van IT-beveiliging en IT-continuïteit binnen de Vlaamse administratie. Het auditcomité van de Vlaamse administratie keurde daarom op 4 juni 2020 de opstart van de thema-audit IT-beveiliging goed.

- Deze thema-audit beoogt een antwoord te formuleren op volgende vragen:

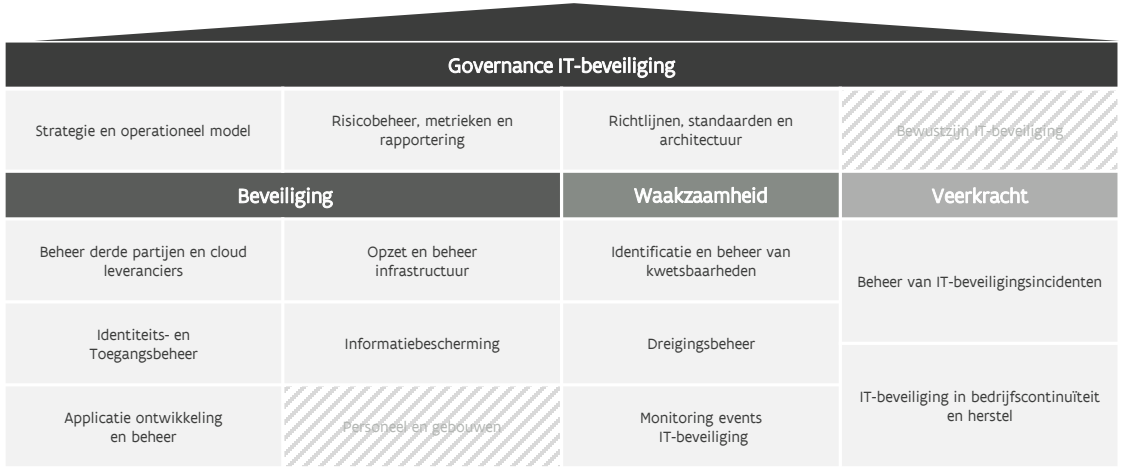
I.

In welke mate zijn de belangrijkste beheersmaatregelen aanwezig om de gewenste IT-beveiliging en IT-continuïteit te kunnen garanderen opdat de burger voldoende kan vertrouwen op (de werking van de kernprocessen van) de Vlaamse overheid? En hebben de betrokken entiteiten en de Vlaamse administratie overkoepelend daar voldoende zicht op?

- Om hierop een antwoord te formuleren, werkte Audit Vlaanderen een controleprogramma uit dat zowel focust op organisatorische als technische IT-beveiligingskwetsbaarheden en waarbij diverse types van entiteiten werden betrokken. Audit Vlaanderen liet zich tijdens deze thema-audit bijstaan door externen met de nodige gespecialiseerde kennis.

Auditaanpak en -reikwijdte

Verschillende elementen hebben een impact op de beheersing van IT-beveiligingsrisico's. De elementen die in deze thema-audit worden onderzocht om de auditdoelstellingen te beantwoorden, zijn geselecteerd uit internationaal gangbare normenkaders en goede praktijken. **Tijdens de audit is IT-beveiliging bekeken vanuit 4 delen met in totaal 13 elementen,** zoals rechts gevisualiseerd.



Voor de 13 elementen is respectievelijk nagegaan in welke mate:

- **Governance**
  - een adequate IT-beveiligingsstrategie en -beleid aanwezig is;
  - IT-beveiligingsrisico's geïdentificeerd, geëvalueerd, beheerd en opgevolgd worden;
  - rollen en verantwoordelijkheden inzake IT-beveiliging voldoende uitgewerkt en geconcretiseerd zijn;
- **Beveiliging**
  - de derde partijen m.b.t. IT-beveiliging worden aangestuurd en in welke mate deze derde partijen de voorziene maatregelen naleven;
  - het risico op ongeautoriseerde toegang wordt beheerst;
  - de infrastructuur veilig wordt gehouden;
  - bij de ontwikkeling en het beheer van systemen rekening wordt gehouden met IT-beveiliging; (Omdat dit element bij de GID veelal afzonderlijk wordt georganiseerd, is dit aspect enkel zijdelings meegenomen bij de evaluatie van de andere elementen.)
- **Waakzaamheid**
  - de updates tijdig worden doorgevoerd;
  - gebruik wordt gemaakt van testing, logging en monitoring;
  - de kwetsbaarheden en dreigingen tijdig worden geïdentificeerd en degelijk opgevolgd;
- **Veerkracht**
  - de nodige maatregelen getroffen zijn om incidenten goed te kunnen beheren;
  - voldoende maatregelen voor bedrijfscontinuïteit getroffen zijn.

Auditaanpak en -reikwijdte

- Voor de selectie van de entiteiten gevat door deze thema-audit, zijn de volgende criteria gehanteerd:
  - ingeschatte relevantie van het thema security in de ICT-risicoanalyse voor de Vlaamse administratie;
  - gevoeligheid van de verwerkte gegevens;
  - aanwezigheid van kernprocessen die gebruik maken van industriële controle systemen (ICS);
  - diversiteit in de opzet van het ICT-beheer (eigen beheer versus beheer door derden);
  - auditplanning van Audit Vlaanderen.

- Audit Vlaanderen auditeerde bij deze thema-audit de **volgende entiteiten:**
  - Vlaams Agentschap voor Innoveren en Ondernemen (VLAIO);
  - Vlaams Agentschap voor Personen met een Handicap (VAPH);
  - Agentschap Wegen en Verkeer (AWV);
  - De Vlaamse Waterweg (DVW);
  - De gemeenschappelijke ICT-dienstverlening (GID) met de regierol van Het Facilitair Bedrijf (HFB)/Digitaal Vlaanderen (*), en meer specifiek:
    - het algemeen beheer van IT-beveiliging voor de GID;
    - IT-beveiliging van de digitale werkplekdiensten;
    - IT-beveiliging van de netwerkdiensten.

(*) bij de start van de audit maakten de componenten in scope van deze GID-audit nog deel uit van het Facilitair Bedrijf. In de loop van de audit werden deze diensten opgenomen in de organisatie van Digitaal Vlaanderen.

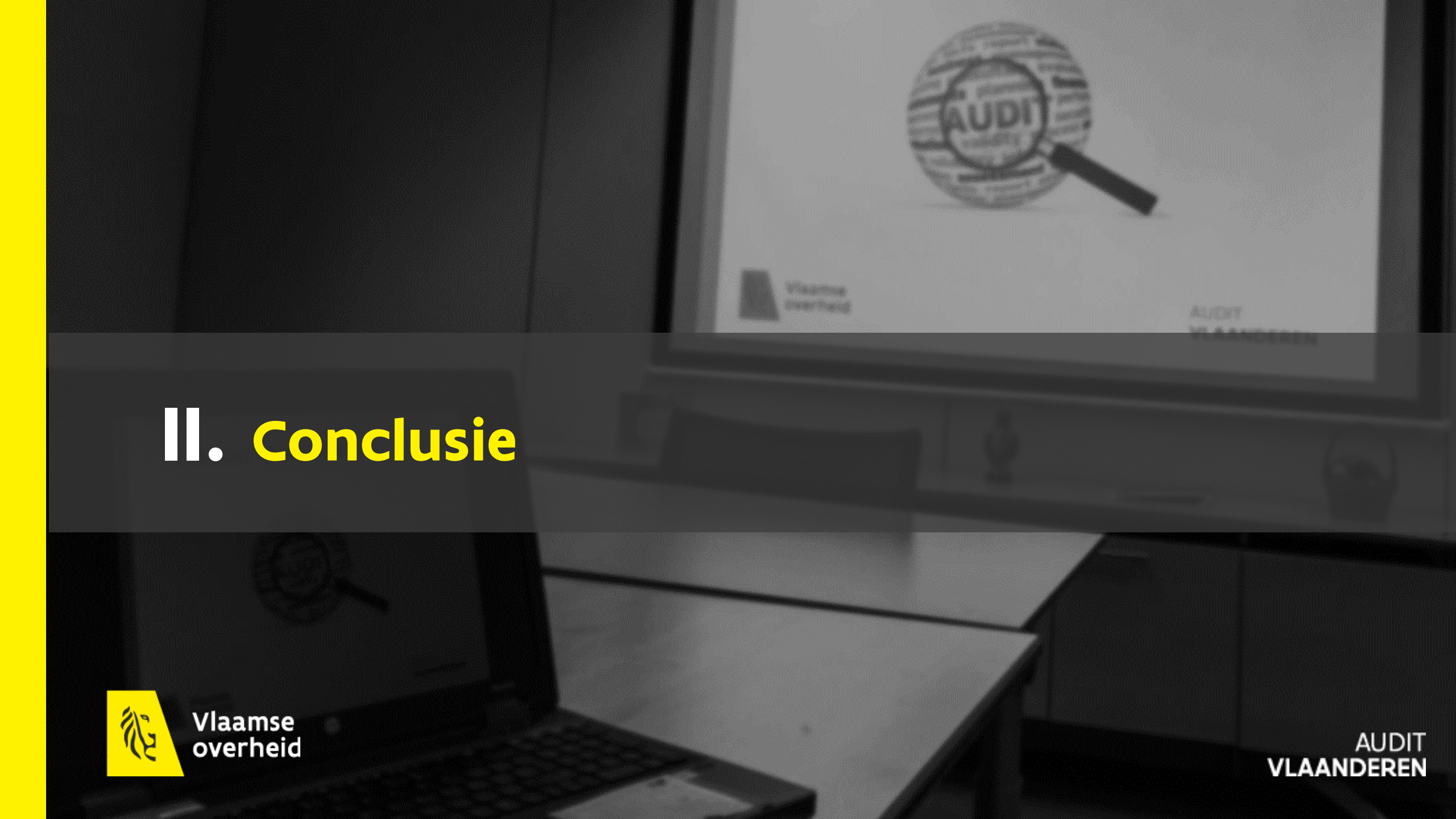
Auditaanpak en -reikwijdte

- De **kernprocessen** bij deze entiteiten werden geselecteerd op basis van:
  - hoge mate van automatisatie;
  - grote materialiteit of impact van de processen;
  - klantgerichte aard;
  - brede ontsluiting en veel informatie-uitwisseling met derde partijen.

- Hoewel de audit bij de diverse entiteiten focusten op de respectievelijke kernprocessen, werd telkens een holistische aanpak gehanteerd waarbij ook aandacht ging naar de kwetsbaarheid van verbonden of verwante systemen die een impact kunnen hebben op de veiligheid van het desbetreffende kernproces.

- De bevindingen van de audits bij de 5 voornoemde entiteiten kregen hun neerslag in 5 individuele rapporten die overgemaakt werden aan de betrokken bestemmelingen.

- Het voorliggende **globaal rapport** is opgemaakt op basis van de bevindingen uit de individuele auditopdrachten en van de gemaakte vaststellingen op niveau van de Vlaamse overheid.



II. Conclusie

Vlaamse overheid

AUDIT VLAANDEREN

Managementsamenvatting

- De Vlaamse overheid zet volop in op een digitale werking en dienstverlening voor haar burgers. Dat biedt vele voordelen maar brengt ook uitdagingen met zich mee. Cybercriminaliteit neemt alsmaar toe en vormt een steeds grotere bedreiging voor de dienstverlening.

- Uit deze thema-audit blijkt dat de Vlaamse overheid zich bewust is van het belang van IT-beveiliging, maar dat ze die beveiliging onvoldoende gestructureerd, consistent en kwalitatief aanpakt. Daardoor:
  - heeft de Vlaamse overheid onvoldoende zicht op de risico's die ze met betrekking tot IT-beveiliging en IT-continuïteit loopt;
  - worden keuzes gemaakt die afwijken van de vooropgestelde minimale maatregelen zonder dat transparant is waarom;
  - is de Vlaamse overheid nauwelijks voorbereid om snel en adequaat te kunnen reageren bij grootschalige IT-veiligheidsincidenten.

- De Vlaamse overheid nam niettemin al goede initiatieven en kan op relatief korte termijn significante stappen vooruit zetten. Zo is bij de geauditeerde kernprocessen meermaals vastgesteld dat de technologie waarin de Vlaamse overheid investeert het potentieel bezit om een betere IT-beveiliging te garanderen. De ingezette leveranciers van ICT-diensten zijn veelal ook in staat beter beveiligde diensten te leveren wanneer dat uitdrukkelijk wordt gevraagd. Bovendien ligt momenteel een strategie voor informatieveiligheid voor dat potentieel de basis kan vormen voor een sterke vooruitgang op het vlak van IT-beveiliging bij de Vlaamse overheid. De transitieprojecten in het kader van de nieuwe ICT-raamovereenkomsten 2022 en de relanceprojecten omtrent "Cybersecurity en uitrol SIEM" en "Ondersteuning Digitale Transformatie" bieden opportuniteiten om die strategie, eens bekrachtigd, verder te concretiseren en in te vullen. De volledige realisatie van de strategie voor informatieveiligheid vereist wel een volgehouden inspanning op langere termijn.

- In het globaal rapport van de thema-audit informatiebeveiliging 2015 signaleerde Audit Vlaanderen dat de Vlaamse overheid te kwetsbaar was voor de bedreigingen op het vlak van IT-beveiliging. De realisatie van de aanbevelingen van dat globaal rapport zijn lange tijd te weinig ter harte genomen. Voor verschillende elementen blijkt de IT-beveiliging nog steeds te kwetsbaar. De aanbevelingen in het onderhavige rapport vervangen de eerder geformuleerde aanbevelingen of vullen ze aan. Het is van belang om zowel op korte als langere termijn actief stappen te zetten ter verbetering van de IT-beveiliging en IT-continuïteit opdat de burger voldoende kan vertrouwen op (de werking van de kernprocessen van) de Vlaamse overheid.

Duiding van de aanbevelingen (1/3)

- In 2020 valideerde het Stuurorgaan Vlaams Informatie- en ICT-beleid een strategie voor informatieveiligheid, in afwachting van een nog verder uit te werken nota voor de Vlaamse Regering. Deze strategie bouwt verder op het in 2018 gevalideerde raamwerk voor informatieclassificatie en de sindsdien uitgewerkte richtlijnen omtrent de concretisering daarvan in minimale maatregelen. Hoewel de huidige strategie voor informatieveiligheid verschillende goede principes en mogelijkheden aanreikt, is onder meer een verdere concretisering en invulling ervan nodig (aanbeveling 1).

- De ICT-omgeving van de Vlaamse overheid is een uitgebreid en complex geheel met verschillende onderlinge afhankelijkheden. Zowel tussen de verschillende actoren als bij elke actor zelf zijn rollen, taken, bevoegdheden en verantwoordelijkheden veelal onvoldoende duidelijk afgebakend en toegewezen. In de praktijk blijkt de Vlaamse overheid momenteel blootgesteld aan verschillende IT-beveiligingsrisico's waarvoor niemand aansprakelijkheid opneemt en worden andere IT-beveiligingsrisico's onvoldoende en/of laattijdig opgenomen. Zelfs het actief uitwisselen van informatie en kennis omtrent IT-beveiliging tussen en binnen actoren alsook het voeren van een dialoog over de risico's en de risicobeheersing is geen evidentie. Om de IT-beveiliging beter te garanderen, moeten rollen en verantwoordelijkheden zo snel mogelijk worden scherp gesteld (aanbeveling 2). De strategie voor informatieveiligheid bevat verschillende voorstellen hieromtrent.

- Om de IT-beveiliging effectief en kostenefficiënt aan te pakken, dient dit risicogebaseerd te gebeuren. De Vlaamse overheid en de individuele entiteiten hebben momenteel echter zowel overkoepelend als individueel onvoldoende zicht op de belangrijkste risico's die ze lopen met betrekking tot hun IT-beveiliging, noch op de mate waarin de belangrijkste beheersmaatregelen aanwezig zijn om de gewenste IT-beveiliging te kunnen garanderen.

Duiding van de aanbevelingen (2/3)

- Wanneer individuele entiteiten of aanbieders van gemeenschappelijke ICT-diensten initiatieven nemen om IT-beveiligingsrisico's in kaart te brengen en te beheersen, dan verlopen die eerder op ad-hocbasis. De entiteiten gebruiken de centraal ontwikkelde risicomethodiek voor het beheer van IT-beveiligingsrisico's niet of nauwelijks. Tijdens deze thema-audit zijn verscheidene IT-beveiligingsrisico's geïdentificeerd die, hoewel ze vaak reeds gekend waren bij betrokkenen, onvoldoende worden aangepakt. Hoewel de nieuwe strategie de risico-eigenaars aansprakelijk stelt voor hun IT-beveiliging, is er geen beperking op het aanvaarden van residuele risico's, dienen entiteiten hier niet over te rapporteren en kunnen ze in de praktijk zonder argumentatie afwijken van de richtlijnen inzake minimale maatregelen (aanbeveling 4).

- Een overkoepelend zicht op de belangrijkste IT-beveiligingsrisico's is noodzakelijk om indien nodig bijkomende maatregelen te kunnen nemen. Dit is zeker het geval bij incidenten die een impact kunnen hebben op andere entiteiten. Momenteel beschikt de Vlaamse overheid niet over een mechanisme om de entiteiten inzake IT-beveiliging op te volgen, te evalueren en zo nodig bij te sturen. De strategie voor informatieveiligheid stelt hiervoor een overkoepelende informatieveiligheidsdienst voorop die kan instaan voor een actieve opvolging in samenspraak met de entiteiten en het stuurorgaan. Het mandaat, de opdrachten, de praktische aanpak en de wisselwerking met de verschillende entiteiten moeten evenwel nog worden bepaald (aanbeveling 5).

- Met het raamwerk voor informatieclassificatie en de uitgewerkte richtlijnen inzake minimale maatregelen, zet de Vlaamse overheid al enkele jaren degelijke stappen om te anticiperen op de bedreigingen van haar informatieverwerking. Uit de auditwerkzaamheden blijkt dat de vertrouwdheid met en toepassing van het raamwerk voor informatieclassificatie evenwel te gering is, zowel bij individuele entiteiten als bij aanbieders van gemeenschappelijke ICT-diensten. Om te vermijden dat het raamwerk en de richtlijnen inzake minimale maatregelen een theoretisch model blijven met een beperkte impact op de IT-beveiliging in de praktijk, zijn meer inspanningen nodig om het raamwerk en de richtlijnen uit te dragen binnen de Vlaamse overheid en om de diverse entiteiten te ondersteunen bij hun toepassing ervan (aanbeveling 3).

Duiding van de aanbevelingen (3/3)

De noodzaak om verdere stappen te zetten ter verbetering van de IT-beveiliging uit zich niet enkel op het vlak van de governance van de IT-beveiliging, maar ook op het vlak van preventie (beveiliging), detectie (waakzaamheid) en reactie (veerkracht) :

- **Preventie (beveiliging)**

  Uit de deelaudits blijkt dat het voor individuele entiteiten niet eenvoudig is om autonoom de benodigde IT-beveiligingsmaatregelen te treffen. Het ontbreekt vaak aan de benodigde tijd en de kennis. Anderzijds blijkt dat de entiteiten wanneer ze beroep doen op - al dan niet gemeenschappelijk georganiseerde - uitbesteding, ook nog enkele stappen moeten zetten om tot een uitbesteding te komen die voldoende garanties en transparantie biedt op het vlak van IT-beveiliging. Zo ontbreken soms duidelijke verwachtingen ten aanzien van de leveranciers omtrent de te voorziene IT-beveiligingsmaatregelen en schiet het toezicht op de leveranciers hieromtrent tekort.

- **Detectie (waakzaamheid)**

  De individuele entiteiten doen te weinig aan logging, monitoring en opvolging om gebeurtenissen op het gebied van IT-beveiliging te detecteren. Het centraal systeem dat gemeenschappelijke ICT-dienstverlening inzet voor het beheer van veiligheidsgebeurtenissen en -informatie (SIEM), detecteert vooralsnog slechts een beperkt aantal bedreigingen, kwetsbaarheden en veiligheidsincidenten. De Vlaamse overheid plant via het perceel Service-Integratiediensten van de nieuwe ICT-raamovereenkomst 2022 om hierin verbetering te brengen en dergelijke beheersmaatregelen ook ruimer in te (laten) zetten. Wat dit concreet inhoudt, zowel overkoepelend, voor de gemeenschappelijke ICT-dienstverlening als voor de individuele entiteiten, moet nog worden bepaald.

- **Reactie (veerkracht)**

  Hoewel binnen de Vlaamse overheid op verschillende niveaus initiatieven voor bedrijfscontinuïteit zijn genomen, is de continuïteit van de diensten geleverd aan de burger in geval van grootschalige incidenten en calamiteiten op dit moment onvoldoende gegarandeerd. De respectievelijke entiteiten, Digitaal Vlaanderen en het CCVO hebben voor IT-beveiligingscrisissen te weinig specifieke voorbereidingen getroffen. Maatregelen die wel al voorzien zijn, zijn veelal onvoldoende getest.

Visueel overzicht

Audit Vlaanderen formuleert 5 aanbevelingen.

Legende

M.b.t. dit subproces werden één of meerdere risico's die de realisatie van de doelstellingen van het proces kunnen belemmeren. Bijkomende maatregelen dringen zich op om het risico tot een aanvaardbaar niveau te herleiden. Voor deze procesfase werden aanbevelingen geformuleerd met hoge prioriteit.

M.b.t. dit subproces werden één of meerdere risico's geïdentificeerd die de realisatie van één van de doelstellingen van het proces kunnen belemmeren. Bijkomende maatregelen kunnen overwogen worden om het huidige risiconiveau te kunnen handhaven of om het risico verder terug te dringen. Voor deze procesfase werden verbeterpunten geformuleerd met gemiddelde prioriteit.

M.b.t. dit subproces werden één of meerdere risico's geïdentificeerd die de realisatie van de doelstellingen van het proces niet belemmeren. Voor deze procesfase werden geen verbeterpunten geformuleerd of enkel verbeterpunten met lage prioriteit.

Aanbevelingen

Referentie	Omschrijving
A1 – Strategie	Versterk de slagkracht van de strategie voor informatieveiligheid om een antwoord te bieden op de toenemende uitdagingen op het vlak van IT-beveiliging. Dit door: • de formele bekrachtiging van de strategie door de Vlaamse Regering; • het verder concretiseren en invullen van de strategie, zowel overkoepelend voor de gemeenschappelijke ICT-diensten als bij de respectievelijke entiteiten; • de periodieke opvolging, beoordeling en bijsturing van de operationele uitvoering van de strategie, door middel van het periodiek rapporteren van de concrete en meetbare doelstellingen naar het stuurorgaan; • de communicatie na de goedkeuring door de Vlaamse Regering van het bindend karakter van de strategie en de bijhorende verwachtingen ten aanzien van de entiteiten en aanbieders van gemeenschappelijke ICT-diensten.
A2 – Rollen en verantwoordelijkheden	Om de IT-beveiliging op het niveau van de Vlaamse overheid beter te garanderen, behoort: • elke entiteit de verdeling van de rollen en verantwoordelijkheden voor de identificatie, de evaluatie en het proactief beheer van, alsook de rapportering over de IT-beveiligingsrisico's helder in kaart te brengen, met de focus op eenduidige aansprakelijkheden en duidelijke verwachtingen; • elke entiteit de samenwerking met andere entiteiten en actoren te verduidelijken en verder scherp te stellen (bv. samenwerking met GID, overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen en leveranciers); • de Vlaamse overheid een formeel proces te bepalen dat de finale en overkoepelende aansprakelijkheid toewijst aan één partij wanneer er een overlap bestaat tussen de verantwoordelijkheid voor IT-beveiligingsrisico's van meerdere partijen.

Referentie	Omschrijving
A3 – Raamwerk voor informatieclassificatie	Opdat de gewenste prioriteiten, doelstellingen en minimale maatregelen voor IT-beveiliging binnen de Vlaamse overheid zouden worden gerespecteerd, is het aangewezen om de vertrouwdheid met en toepassing van het raamwerk voor informatieclassificatie te bevorderen. Dit kan onder meer door: • de verdere uitbouw van het raamwerk concreet af te lijnen en te vervolledigen voor alle kwaliteitskenmerken (vertrouwelijkheid, integriteit en beschikbaarheid), minimale maatregelen (ook omtrent bedrijfscontinuïteit) en specifieke domeinen (bv. NIS en ICS); • de finale stukken telkens formeel te laten valideren, minstens door het stuurorgaan, en als zodanig met een duidelijke versiegeschiedenis te markeren in het documentbeheer; • het raamwerk periodiek te evalueren in functie van de nieuwe en evoluerende technologieën en regelgeving; • de communicatie en bewustmaking rond het raamwerk voor informatieclassificatie binnen de Vlaamse overheid te verhogen; • ondersteuning beschikbaar te stellen om de uitrol van het raamwerk door de individuele entiteiten te ondersteunen, te begeleiden en op te volgen; • de toepassing van de methodiek gefaseerd uit te rollen over de volledige Vlaamse overheid (bv. middels een programma).
A4 – Opvolging van IT-beveiliging en bijhorende risico's	De Vlaamse overheid beheert en verwerkt tal van gevoelige en vertrouwelijke gegevens van burgers, ondernemingen en personeelsleden. Om zicht te krijgen op het niveau van integriteit, beschikbaarheid en vertrouwelijkheid van deze informatieverwerking dienen de individuele entiteiten en aanbieders van gemeenschappelijke ICT-diensten het beheer van IT-beveiligingsrisico's op een meer gestructureerde, consistente en kwalitatieve wijze aan te pakken. Daartoe is het aangewezen om: • de verplichtingen van de risico-eigenaren inzake de rapportering over hun IT-beveiligingsrisico's en over hun compliance met de minimale maatregelen eenduidig te bepalen en af te dwingen; • een begrenzing te stellen aan de residuele risico's waaraan individuele entiteiten en aanbieders van gemeenschappelijke ICT-diensten de eigen informatiebeveiliging en die van de Vlaamse overheid in haar geheel kunnen blootstellen zonder escalatie en periodieke expliciete acceptatie op overkoepelend niveau; • voor de omgang met uitzonderingen rond risico's die de begrenzing overschrijden of afwijkingen op de minimale maatregelen, een formeel proces uit te werken gebaseerd op het principe "pas toe of leg uit" (comply or explain).

Referentie	Omschrijving
A5 – Opvolging van IT-beveiliging en bijhorende risico's	Verkrijg en onderhoud een overkoepelend zicht op de IT-beveiligingsrisico's en de mate waarin de belangrijkste beheersmaatregelen aanwezig zijn om de gewenste IT-beveiliging en IT-continuïteit te kunnen garanderen voor de hele Vlaamse overheid. Zorg daarnaast voor een actieve opvolging van de huidige en toekomstige bedreigingen voor de IT-beveiliging van de kernprocessen. Dit door: • het mandaat en de opdracht van de overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen te bepalen en te laten goedkeuren door de Vlaamse overheid. • zo snel mogelijk een overzicht te creëren van de overkoepelende risico's met formele taxonomie en centrale escalatie volgens specifieke richtlijnen • te bepalen hoe de overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen waakzaam zal blijven voor IT-beveiligingsincidenten in de (kern-)processen van de Vlaamse overheid (mogelijks via een planning voor de koppeling van de kernprocessen met de SIEM te bepalen, opvolging van nieuwe kwetsbaarheden, de IT-beveiliging – minstens van kernprocessen – actief opvolgen bij entiteiten en escaleren indien nodig) • een kader uit te werken voor hoe de overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen de Vo-brede coördinatie zal vervullen met betrekking tot informatieveiligheid (o.m. in geval van kritieke incidenten) • vast te leggen hoe de overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen zal rapporteren aan en afstemmen met het Stuurorgaan Vlaams Informatie- en ICT-beleid; • de nodige recurrente werkingsmiddelen voor de overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen te voorzien.

III. Managementreactie

Vlaamse overheid

AUDIT VLAANDEREN

Managementreactie (1/2)

Het Stuurorgaan kan zich vinden in de conclusies die Audit Vlaanderen geformuleerd heeft naar aanleiding van de thema-audit over de IT-beveiliging binnen de Vlaamse overheid.

Het is positief dat de in december 2020 door het Stuurorgaan **goedgekeurde strategie** aangaande het VO Informatieveiligheidsbeleid erkenning in de aanbevelingen van Audit Vlaanderen krijgt. Het Stuurorgaan ziet deze audit dan ook als een validatie van de ingeslagen weg. In de volgende slide wordt concreet aangegeven hoe deze strategie de geformuleerde aanbevelingen zal invullen.

Met de implementatie van de strategie werd inmiddels al aanvang genomen. Digitaal Vlaanderen richt hiervoor een **programma** in, dat onder meer zal instaan voor het promoten van informatieclassificaties, doorvoeren van risicobeheer, het opzetten van rapporteringsmechanismen over de voortgang van veiligheidsmaatregelen en het opvolgen van veiligheidsincidenten. Dit is geen eenmalig project, de praktische realisatie zal zich over een aantal jaren uitstrekken.

De **nieuwe raamcontracten,** die begin 2022 in werking treden, versterken het kader m.b.t. informatieveiligheid verder. De lessen uit het verleden en uit de resultaten van eerdere veiligheidsaudits, hebben geleid tot de introductie van nieuwe processen en governance, naast specifieke dienstverlening m.b.t. security.

De combinatie van het implementeren van de VO Informatieveiligheidsbeleid enerzijds, en de nieuwe aanpak via de nieuwe contracten anderzijds, vormt een **sterke basis om de hele VO bij te staan** bij het realiseren van een sterke IT-beveiliging. Het Stuurorgaan engageert zich om dit proces te ondersteunen vanuit haar opdracht.

Managementreactie (2/2)

Aanbevelingen

1 **Aanbeveling 1: Strategie**
Versterk de slagkracht van de strategie voor informatieveiligheid, om een antwoord te bieden op de toenemende uitdagingen op het vlak van IT-beveiliging

2 **Aanbeveling 2: Rollen en verantwoordelijkheden**
De verdeling van de rollen en verantwoordelijkheden voor de identificatie, de evaluatie en het proactief beheer van, alsook de rapportering over de IT-beveiligingsrisico's

3 **Aanbeveling 3: Informatieclassificatie**
Vertrouwdheid met en toepassing van het raamwerk voor informatieclassificatie te bevorderen

4 **Aanbeveling 4: Geintegreerd risico-beheer**
Het beheer van IT-beveiligingsrisico's op een meer gestructureerde, consistente en kwalitatieve wijze aan te pakken

5 **Aanbeveling 5: Opvolging ICT-beveiliging**
Verkrijg en onderhoud een overkoepelend zicht op de IT-beveiligingsrisico's en de mate waarin de belangrijkste beheersmaatregelen aanwezig zijn

Waarom draagt onze strategie hier aan bij?

In 2020 valideerde het stuurorgaan vervolgens een eerste keer een strategie voor informatieveiligheid. Het gevalideerde document "Strategie Informatieveiligheid" voorziet doelen, strategische principes en een aanpak voor informatieveiligheid binnen de Vlaamse overheid. Een **nota voor de Vlaamse Regering** is in opmaak is en zal binnenkort op de Vlaamse regering worden geagendeerd.

De strategie voor Informatieveiligheid bevat een **beschrijving van de rollen en verantwoordelijkheden** op hoog niveau. Het strategisch plan voorziet in verdere concretisering en invulling van de strategie, bv. met betrekking tot de samenwerking tussen de individuele entiteiten en Digitaal Vlaanderen.

De **verdere ontwikkeling van het informatieclassificatiemodel** is gepland en gebudgetteerd binnen het strategisch plan, met extra aandacht voor overzicht en communicatie. Er wordt eveneens voorzien in het bindend karakter van deze methodologie in de nota aan de Vlaamse regering.

Digitaal Vlaanderen naar een ICT-regieorganisatie evolueren binnen de kaders van de vernieuwde ICT-dienstverlening waarbij ze de **integratie- en regierol** opneemt m.b.t. informatieveiligheid. Samen met onze ICT-partner Atos staan we o.m. in voor de borging van de naleving van de veiligheidsmaatregelen, het coördineren, opvolgen en rapporteren van risico's en acties en het inrichten van de Integrated Risk Management (IRM) oplossing.

Binnen de strategie voor informatieveiligheid is een **standaardrapportering** aan het stuurorgaan voorzien om inzicht te geven in de belangrijkste beveiligingsrisico's via een halfjaarlijks cybersecurity dashboard en statusrapport.

Binnen de strategie voor informatieveiligheid is een proces voorzien waarbij nagegaan wordt of/in hoeverre de entiteit (of een individuele toepassing) voldoet aan het Vo informatieclassificatie raamwerk via een **self-assessment.** We introduceren daarnaast een optionele conformiteitstoets binnen de Vlaamse overheid.

IV. Belangrijkste bevindingen

Vlaamse overheid

AUDIT VLAANDEREN

1. Governance: strategie

- Een strategie voor informatiebeveiliging opmaken is voor elke organisatie belangrijk om aan te geven hoe ze informatiebeveiliging wil aanpakken en welke principes en doelstellingen ze daarbij vooropstelt. Het globaal rapport van de thema-audit informatiebeveiliging 2015 van Audit Vlaanderen wees op het gebrek aan een strategie voor informatiebeveiliging op het niveau van de Vlaamse overheid. In 2018 keurde het Stuurorgaan Vlaams Informatie- en ICT-beleid een raamwerk voor informatieclassificatie goed dat sindsdien helpt om meer gestructureerd over informatiebeveiliging na te denken. In 2020 valideerde het stuurorgaan vervolgens een strategie voor informatieveiligheid, in afwachting van een nog verder uit te werken nota hieromtrent voor de Vlaamse Regering. Het gevalideerde document “Strategie Informatieveiligheid” voorziet doelen, strategische principes en een aanpak voor informatieveiligheid binnen de Vlaamse overheid. Hoewel een nota voor de Vlaamse Regering in opmaak is, ontbreekt tot op heden de goedkeuring door de Vlaamse Regering van een formele en voor de Vlaamse administratie afdwingbare strategie voor informatieveiligheid.

- De strategie voor informatieveiligheid vermeldt een plan van aanpak met drie prioriteiten:
  - een Vlaamse overheid-brede aanpak van informatieveiligheid,
  - versterking van de digitale competenties en
  - verhoging van het IT-beveiligingsniveau door weerbare digitale processen en robuuste infrastructuur.

- Het door de Vlaamse Regering goedgekeurde relanceproject ‘Cybersecurity en uitrol SIEM’ (VV065) anticipeert op de nieuwe strategie voor informatieveiligheid. In het kader van het relanceplan “Vlaamse Veerkracht” stelde de Vlaamse Regering in juni 2021 met dit project middelen ter beschikking om reeds een deel van deze prioriteiten te realiseren. Ook de nieuwe ICT-raamovereenkomsten 2022 bieden hiervoor opportuniteiten.

- Hoewel de huidige strategie voor informatieveiligheid verschillende goede principes en mogelijkheden aanreikt, is verdere concretisering en invulling ervan nodig. Zo bijvoorbeeld wordt wel rapportage naar het stuurorgaan voorzien, maar is nog niet duidelijk wat moet gerapporteerd worden, wat het doel daarvan is, wie signalen daaruit moet capteren en wie escalaties en/of acties kan initiëren.

1. Governance: strategie

- De volledige realisatie van de voornoemde strategie vereist een structurele langetermijnaanpak. Het Stuurorgaan Vlaams Informatie- en ICT-beleid houdt zichzelf verantwoordelijk voor de opvolging van de initiatieven die in het kader van de uitvoering van de strategie worden getroffen. Er zijn echter nog geen concrete doelstellingen geformuleerd op basis waarvan de implementatie adequaat kan worden opgevolgd, beoordeeld en indien nodig bijgestuurd. Ook de beoogde resultaten van het relanceproject “Cybersecurity en uitrol SIEM” zijn alleen op hoog niveau geformuleerd. Dit maakt het moeilijk om zich te verzekeren van de verdere uitwerking en de operationele uitvoering van de strategie.

Aanbeveling 1

Versterk de slagkracht van de strategie voor informatieveiligheid, om een antwoord te bieden op de toenemende uitdagingen op het vlak van IT-beveiliging, door:

- de formele bekrachtiging van de strategie door de Vlaamse Regering;
- het verder concretiseren en invullen van de strategie, zowel overkoepelend, voor de gemeenschappelijke ICT-diensten als bij de respectievelijke entiteiten;
- de periodieke opvolging, beoordeling en bijsturing van de operationele uitvoering van de strategie, door middel van het periodiek rapporteren van de concrete en meetbare doelstellingen naar het stuurorgaan;
- de communicatie na de goedkeuring door de Vlaamse Regering van het bindend karakter van de strategie en de bijhorende verwachtingen ten aanzien van de entiteiten en aanbieders van gemeenschappelijke ICT-diensten.

2. Governance: rollen en verantwoordelijkheden

- De ICT-omgeving van de Vlaamse overheid is een uitgebreid en complex geheel met veel onderlinge afhankelijkheden. De diverse rollen en verantwoordelijkheden voor IT-beveiliging zitten verspreid over verschillende actoren, zoals bijvoorbeeld het Stuurorgaan voor Informatie -en ICT-beleid en de onderliggende werkgroep Informatieveiligheid, de overkoepelende informatieveiligheidsdienst georganiseerd door Digitaal Vlaanderen (ook naar verwezen als het 'Digital Security Office'), de diverse entiteiten die instaan voor en/of betrokken zijn bij de verschillende (kern- en andere) processen, de ICT-dienstleveranciers, de gemeenschappelijke ICT-dienstverlening en andere derde partijen.

- De verdeling van de rollen en verantwoordelijkheden voor IT-beveiliging tussen die respectievelijke actoren is vaak onvoldoende duidelijk afgebakend. Uit de diverse deelaudits blijkt dat hierdoor IT-beveiligingsrisico's blijven openstaan en de betrokken organisaties in het algemeen meer risico's lopen dan ze zich realiseren. De strategie voor informatieveiligheid probeert hier aan tegemoet te komen door:
  - de verantwoordelijkheden duidelijker toe te wijzen (met de entiteiten als eindverantwoordelijken);
  - een overkoepelende opvolging met actief toezicht door de informatieveiligheidsdienst van Digitaal Vlaanderen;
  - het Stuurorgaan Vlaams Informatie- en ICT-beleid naast haar decretale adviesbevoegdheden ook te mandateren voor het nemen van beslissingen bij escalaties en voor het afkondigen van en toezien op dwingende minimale beveiligingsmaatregelen.

  Een bekrachtiging van de strategie voor informatieveiligheid door de Vlaamse Regering zou zowel het raamwerk voor informatieclassificatie als de bijhorende minimale maatregelen een bindend karakter geven en de nog te concretiseren implementatie in de praktijk ruggensteunen.

- Het ontwerp van strategie voor Informatieveiligheid is een bondig document met beschrijvingen op hoog niveau. Veel zal dan ook afhangen van de concretisering en invulling van de strategie. Zo bijvoorbeeld zal moeten worden afgesproken hoe de samenwerking tussen de individuele entiteiten en Digitaal Vlaanderen moet worden bijgestuurd om de voorgestelde uitdrukkelijke aansprakelijkheid van de individuele entiteiten - ongeacht wie voor het operationeel beheer instaat - voldoende te kunnen opnemen.

2. Governance: rollen en verantwoordelijkheden

- Wanneer entiteiten keuzes maken en bestellingen plaatsen die een impact kunnen hebben op andere entiteiten, is onvoldoende duidelijk wie daaromtrent keuzes kan maken en de aansprakelijkheid draagt. Als er een overlap bestaat tussen verschillende activiteiten en de daaraan verbonden processen en ondersteunende infrastructuur, dienen de betrokkenen volgens de strategie onderling overeen te komen welke partij de aansprakelijkheid zal dragen. Tijdens de auditwerkzaamheden bleek dat dergelijke situaties in de praktijk veelvuldig voorkomen en vaak knelpunten vormen. In de praktijk blijkt de Vlaamse overheid blootgesteld aan verschillende IT-beveiligingsrisico's waarvoor niemand aansprakelijkheid opneemt. Zelfs het actief uitwisselen van informatie en kennis omtrent IT-beveiliging tussen en binnen actoren alsook het voeren van een dialoog over de risico's en de risicobeheersing is vaak geen evidentie.

- Ook voor leveranciers zijn de richtlijnen vanuit de diverse entiteiten soms moeilijk te verzoenen en is daarbij te vaak onduidelijk wie uiteindelijk aansprakelijk is voor wat. In sommige gevallen probeert de gemeenschappelijke ICT-dienstverlener te werken met een Risico Acceptatie Formulier (=RAF) dat wordt voorgelegd aan de bestellende entiteit. Veel van deze formulieren worden uiteindelijk ongetekend in de applicatiedossiers opgenomen zonder dat er een overkoepelend zicht is op deze risico's en zonder dat de andere entiteiten die bij incidenten mogelijks geïmpacteerd kunnen worden hiervan op de hoogte (kunnen) zijn.

- Ook bij de respectievelijke actoren zijn de bevoegdheden en de taken op het vlak van IT-beveiliging veelal onvoldoende duidelijk afgelijnd en toegewezen. Vaak vult elke betrokkene de identificatie, de evaluatie en het proactief beheer van IT-beveiligingsrisico's naar eigen inzicht en noden in. Wie verantwoordelijk is voor de rapportering over de IT-beveiligingsrisico's naar het management en voor het opvolgen van de IT-beveiligingsrisico's op entiteitsniveau, is bijvoorbeeld niet altijd duidelijk. Door een gebrek aan eenduidige aansprakelijkheid worden ook binnen elke actor belangrijke rollen, taken, bevoegdheden en verantwoordelijkheden onvoldoende opgenomen. Dit draagt er toe bij dat de verwachtingen ten aanzien van IT-beveiliging onvoldoende worden gerealiseerd, dat de reële risicobeheersing onvoldoende duidelijk is, dat openstaande risico's en mogelijke keuzes daaromtrent onvoldoende gesignaleerd worden en dat gekende risico's en kwetsbaarheden te lang blijven sluimeren.

2. Governance: rollen en verantwoordelijkheden

Aanbeveling 2

Om de IT-beveiliging op het niveau van de Vlaamse overheid beter te garanderen, behoort:

- elke entiteit de verdeling van de rollen en verantwoordelijkheden voor de identificatie, de evaluatie en het proactief beheer van, alsook de rapportering over de IT-beveiligingsrisico's helder in kaart te brengen, met de focus op eenduidige aansprakelijkheden en duidelijke verwachtingen;
- elke entiteit de samenwerking met andere entiteiten en actoren te verduidelijken en verder scherp te stellen (bv. samenwerking met GID, overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen en leveranciers);
- de Vlaamse overheid een formeel proces te bepalen dat de finale en overkoepelende aansprakelijkheid toewijst aan één partij wanneer er een overlap bestaat tussen de verantwoordelijkheid voor IT-beveiligingsrisico's van meerdere partijen.

3. Governance: raamwerk voor informatieclassificatie

- Initieel via een decreet van 23 december 2016 en later via het Bestuursdecreet, kreeg het Stuurorgaan Vlaams Informatie- en ICT-beleid verschillende opdrachten toegewezen. Zo dient het stuurorgaan aan de Vlaamse Regering naast andere adviesopdrachten ook binnen de krijtlijnen van een strategisch plan van de Vlaamse Regering alle nuttige maatregelen voor te stellen die kunnen bijdragen tot een veilige en vertrouwelijke behandeling van persoonsgegevens. Deze maatregelen kunnen waar nodig door de Vlaamse regering als bindende afspraken vastgelegd worden. Op 26 juni 2020 keurde de Vlaamse Regering, teneinde de krijtlijnen te bepalen, een strategisch plan goed waarbij cybersecurity als één van de speerpunten werd aangeduid.

- Het stuurorgaan heeft ook de opdracht om binnen de krijtlijnen van het strategisch plan technische voorschriften en richtlijnen voor de Vlaamse administratie en de lokale overheden vast te leggen. In juli 2018 valideerde het Stuurorgaan Vlaams Informatie- en ICT-beleid een raamwerk voor informatieclassificatie. Het stuurorgaan beval bij deze validatie iedere betrokken instantie aan haar informatie in te delen in één van de 5 informatieklassen volgens de gevalideerde informatieclassificatie en om navenant minimale beveiligingsmaatregelen toe te passen. De werkgroep Informatieveiligheid van het stuurorgaan werkt sindsdien onder de noemer van ‘generieke informatieclassificatie’ gefaseerd richtlijnen omtrent de minimale maatregelen per informatieklasse uit om dat raamwerk te helpen concretiseren.

- Met het raamwerk voor informatieclassificatie en de uitwerking van een generieke informatieclassificatie, zette de Vlaamse overheid degelijke stappen om te anticiperen op de vele IT-bedreigingen voor haar informatieverwerking. Voor het bepalen van de concrete initiatieven die de individuele entiteiten in het kader van de informatieclassificatie dienen te ondernemen, wordt uitgegaan van de eigen inzichten. In de praktijk blijkt dat entiteiten zich soms beperken tot het op organisatieniveau collectief inschatten van de klasse van alle door hen verwerkte gegevens. Dit kan er toe leiden dat de bescherming voor sommige gevoeligere informatie tekortschiet, maar ook dat voor een deel van de informatie te hoge beveiligingskosten worden gemaakt en dat de werking soms onnodig wordt bemoeilijkt.

3. Governance: raamwerk voor informatieclassificatie

- De uitwerking van het raamwerk voor informatieclassificatie en van de generieke informatieclassificatie is nog in uitvoering. De werkgroep Informatieveiligheid beschrijft momenteel de richtlijnen voor het inrichten van de minimale maatregelen per informatieklasse voor de kwaliteitskenmerken vertrouwelijkheid, integriteit en beschikbaarheid. Deze werkzaamheden zijn nog niet beëindigd. Zo ontbreken bv. nog de minimale maatregelen voor beschikbaarheid en de gedetailleerde richtlijnen omtrent bijvoorbeeld de identificatie en het beheer van kwetsbaarheden. In het relanceproject “Cyber security en uitrol SIEM” (VV065) is de verdere uitbouw van het voornoemde raamwerk expliciet opgenomen. Wat die verdere uitbouw concreet omhelst en finaal nastreeft, is echter niet nader bepaald. In tegenstelling tot de aanpak voor bijvoorbeeld standaardbestekken, laat het versie- en documentbeheer van de reeds uitgewerkte richtlijnen bovendien niet eenvoudig toe om snel te achterhalen welke richtlijnen op welk moment gefinaliseerd werden.

- Bij de concretisering van het raamwerk voor informatieclassificatie werd de afgelopen jaren voornamelijk gefocust op de reguliere ICT-ondersteuning van de gemiddelde werkplek. Met Europees opgelegde verplichtingen (bv. in het kader van de Europese Structuurfondsen) en verstrengende Europese normen en regelgeving (bv. de Europese richtlijn houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie of afgekort de NIS-richtlijn) wordt daarbij vaak weinig rekening gehouden. Entiteiten die daar mee geconfronteerd worden, zijn dan ook genoodzaakt om hun IT-beveiliging in belangrijke mate zelf op te nemen. Mogelijke verstrengingen van de Europese regelgeving worden bovendien niet gezien als opportuniteiten of als richtinggevend om geleidelijk haalbare trajecten uit te werken, maar leiden eerder tot defensieve reacties en pogingen om de toepasselijkheid ervan uit te stellen. Ook op specifieke aspecten die van belang zijn voor apparaten die via internet met andere apparaten of systemen in contact staan, zoals “internet-of-things”-platformen, wordt vanuit het raamwerk voor informatieclassificatie weinig geanticipeerd. Nu industriële controlesystemen (ICS), bv. voor de bewaking en aansturing van tunnels en sluizen, door de technologische evolutie steeds meer opengesteld worden naar andere partijen en het internet en daarbij wordt geëvolueerd naar meer bediening van op afstand, blijken zich hieromtrent significante inspanningen op te dringen. De beoogde timing voor de stap naar verdere bediening van op afstand laat nog enige ruimte om de nodige inspanningen te kunnen leveren, mits onverwijld tot (bijkomende) actie wordt overgegaan.

3. Governance: raamwerk voor informatieclassificatie

- Volgens het raamwerk voor informatieclassificatie behoren eigenaars van informatie jaarlijks te evalueren of de door hen toegekende informatieklassen nog relevant en correct zijn. Onder auspiciën van het stuurorgaan zou Digitaal Vlaanderen het raamwerk voor informatieclassificatie ook jaarlijks moeten herzien in functie van de nieuwe en evoluerende technologieën en regelgeving. Als gevolg daarvan dienen informatie-eigenaren hun datasets mogelijk opnieuw te evalueren of getroffen maatregelen bij te sturen. Op dit moment vindt bij de entiteiten in de scope van deze thema-audit geen van de vermelde evaluaties jaarlijks plaats. Entiteiten blijven vertrouwen op een initiële inschatting en invulling, waardoor de voorziene bescherming voor sommige informatie intussen mogelijk niet langer adequaat is.

- Uit de auditwerkzaamheden blijkt dat de aanbeveling van het stuurorgaan en de uitgewerkte richtlijnen omtrent informatieclassificatie door alle betrokkenen onvoldoende zijn opgenomen, waardoor momenteel noch de individuele entiteiten, noch de aanbieders van gemeenschappelijke ICT-diensten de minimale maatregelen volledig respecteren. De Vlaamse Regering stelde de aanbeveling van het stuurorgaan tot op heden nog niet expliciet verplicht. Afwijkingen blijken veelal niet te worden opgevolgd en zijn momenteel ook niet te penaliseren.

- De uitgevoerde deelaudits van deze thema-audit tonen aan dat de verschillende entiteiten aan significante IT-beveiligingsrisico's voorbij gaan, waardoor ze in de realiteit hun informatieverwerking minder adequaat beschermen dan gedacht. De oorzaak hiervan is de vaak te beperkte kennis rond informatieveiligheid bij de entiteiten en de te schaarse aandacht die naar IT-beveiliging uitgaat. Om daaraan tegemoet te komen zijn meer inspanningen nodig om de het raamwerk voor informatieclassificatie en de uitgewerkte richtlijnen daaromtrent uit te dragen binnen de Vlaamse overheid en om de entiteiten te ondersteunen bij de toepassing ervan. Zoals de strategie voor informatieveiligheid terecht aangeeft, kan geen enkele entiteit de uitdagingen van informatieveiligheid individueel het hoofd bieden.

3. Governance: raamwerk voor informatieclassificatie

- De drie prioriteiten van de strategie kunnen wel tot oplossingen leiden:
  - een Vlaamse overheid-brede aanpak van informatieveiligheid;
  - versterking van de digitale competenties; en
  - verhoging van het IT-beveiligingsniveau door weerbare digitale processen en robuuste infrastructuur.

  Zoals reeds gesteld, is de concretisering en invulling daarbij belangrijk. Zo is momenteel onvoldoende duidelijk
  - welke opdrachten, mandaten en capaciteiten zullen worden toegekend aan de voorgestelde overkoepelende veiligheidsdienst en hoe daarnaast de nodige gespecialiseerde dienstverlening zal worden voorzien en/of ter beschikking gesteld om bij te dragen aan de entiteitsspecifieke (concretiseringen en) implementaties van het raamwerk voor informatieclassificatie;
  - welke keuzes de verschillende entiteiten zullen maken voor de versterking van de digitale competenties, naast de communicatie- en bewustmakingscampagnes die onder meer in het kader van het relanceproject Cyber security en uitrol SIEM (VV065) overkoepelend zijn voorzien;
  - welke inspanningen overkoepelend en voor gemeenschappelijke ICT-diensten zullen worden geleverd en welke inspanningen elk van de entiteiten en de entiteiten gezamenlijk zullen leveren om voor alle gegevens in functie van de toepasselijke klassen de IT-beveiliging voldoende te verhogen.

3. Governance: raamwerk voor informatieclassificatie

Aanbeveling 3

Opdat de gewenste prioriteiten, doelstellingen en minimale maatregelen voor IT-beveiliging binnen de Vlaamse overheid zouden worden gerespecteerd, is het aangewezen om de vertrouwdheid met en toepassing van het raamwerk voor informatieclassificatie te bevorderen. Dit kan onder meer door:

- de verdere uitbouw van het raamwerk concreet af te lijnen en te vervolledigen voor alle kwaliteitskenmerken (vertrouwelijkheid, integriteit en beschikbaarheid), minimale maatregelen (ook omtrent bedrijfscontinuïteit) en specifieke domeinen (bv. NIS en ICS);
- de finale stukken telkens formeel te laten valideren, minstens door het stuurorgaan, en als zodanig met een duidelijke versiegeschiedenis te markeren in het documentbeheer;
- het raamwerk periodiek te evalueren in functie van de nieuwe en evoluerende technologieën en regelgevingen;
- de communicatie en bewustmaking rond het raamwerk voor informatieclassificatie binnen de Vlaamse overheid te verhogen;
- ondersteuning beschikbaar te stellen om de uitrol van het raamwerk door de individuele entiteiten te ondersteunen, te begeleiden en op te volgen;
- de toepassing van de methodiek gefaseerd uit te rollen over de volledige Vlaamse overheid (bv. middels een programma).

4. Opvolging van IT-beveiliging en bijhorende risico's

- De Vlaamse overheid heeft momenteel geen zicht op de belangrijkste risico's die ze centraal en decentraal loopt met betrekking tot haar IT-beveiliging. Tijdens deze thema-audit zijn verscheidene IT-beveiligingsrisico's geïdentificeerd die, hoewel ze vaak reeds gekend waren bij enkele betrokkenen, door de entiteiten - en desgevallend door de actoren die instaan voor de organisatie van gemeenschappelijke ICT-dienstverlening - onvoldoende worden aangepakt. Entiteiten of aanbieders van gemeenschappelijke ICT-diensten die beveiligingsrisico's lopen met een potentiële impact op de gehele Vlaamse overheid, rapporteren daarover niet aan het overkoepelende niveau, ook niet wanneer bewust voor een risico-acceptatie wordt gekozen. Dit inzicht is nochtans noodzakelijk om, zowel op overkoepelend niveau als binnen de individuele entiteiten, de gepaste beleids- en investeringsbeslissingen te kunnen nemen. Momenteel zijn er geen grenzen bepaald aan welke risico's met mogelijke impact op andere delen van de Vlaamse overheid de entiteiten kunnen accepteren en welke escalaties hieromtrent eventueel mogelijk en/of nodig zijn.

- Het Stuurorgaan Vlaams Informatie- en ICT-beleid valideerde eind 2020 een set van beleidsdocumenten voor het beheer van de IT-beveiligingsrisico's bij individuele entiteiten. Zo werden onder meer de criteria, kwaliteitseisen en methodiek voor het beheer van IT-beveiligingsrisico's gevalideerd. Volgens de concretisering van het raamwerk voor informatieclassificatie door de werkgroep Informatieveiligheid is het gebruik van een risicomethodiek verplicht vanaf de verwerking van gegevens van informatieklasse 3. Tot nu toe bleef de beoogde communicatie omtrent deze methodiek en de begeleiding van risico-eigenaren bij de toepassing ervan uit. De entiteiten en de aanbieders van gemeenschappelijke ICT-diensten maken van het ontwikkelde risicobeheer voor IT-beveiliging dan ook nauwelijks gebruik.

- Wanneer individuele entiteiten of aanbieders van gemeenschappelijke ICT-diensten zelf initiatieven nemen om IT-beveiligingsrisico's in kaart te brengen en te beheersen, dan verlopen die eerder op ad-hoc basis. De risicoanalyses die wel worden uitgevoerd, zijn in veel gevallen onvolledig en eerder gebaseerd op theoretische oefeningen dan op empirische resultaten. De Algemene Verordening Gegevensbescherming of het algemene risicobeheer op entiteitsniveau vormen vaak de drijfveer voor de uitgevoerde risicoanalyses. De focus op de bescherming van persoonlijke gegevens is echter te eng om de volledige reikwijdte van IT-beveiliging af te dekken. Uit de deelaudits blijkt daarnaast dat de entiteitbrede organisatiebeheersing vaak onvoldoende rekening houdt met de concrete IT-beveiligingsrisico's die zich in praktijk voordoen. In de praktijk hebben de verschillende entiteiten een te beperkt zicht op hun IT-beveiligingsrisico's.

4. Opvolging van IT-beveiliging en bijhorende risico's

- Hoewel de strategie voor informatieveiligheid krijtlijnen voor een gestandaardiseerde rapportering aan een overkoepelend niveau uittekent, is op dit moment nog niet bepaald hoe en wanneer de entiteiten concreet over hun IT-beveiliging dienen te rapporteren.
- Hoewel de nieuwe strategie de risico-eigenaars aansprakelijk stelt voor hun IT-beveiliging, schept de vooropgestelde aanpak van informatieveiligheid binnen de Vlaamse overheid nog geen duidelijkheid over de omgang met uitzonderingen. Een formeel proces gebaseerd op het principe van comply-or-explain (pas toe of leg uit) kan hieraan tegemoet komen.

Aanbeveling 4

De Vlaamse overheid beheert en verwerkt tal van gevoelige en vertrouwelijke gegevens van burgers, ondernemingen en personeelsleden. Om zicht te krijgen op het niveau van integriteit, beschikbaarheid en vertrouwelijkheid van deze informatieverwerking dienen de individuele entiteiten en aanbieders van gemeenschappelijke ICT-diensten het beheer van IT-beveiligingsrisico's op een meer gestructureerde, consistente en kwalitatieve wijze aan te pakken. Daartoe is het aangewezen om:

- de verplichtingen van de risico-eigenaren inzake de rapportering over hun IT-beveiligingsrisico's en over hun compliance met de minimale maatregelen eenduidig te bepalen en af te dwingen;
- een begrenzing te stellen aan de residuele risico's waaraan individuele entiteiten en aanbieders van gemeenschappelijke ICT-diensten de eigen informatiebeveiliging en die van de Vlaamse overheid in haar geheel kunnen blootstellen zonder escalatie en periodieke expliciete acceptatie op overkoepelend niveau;
- voor de omgang met uitzonderingen rond risico's die de begrenzing overschrijden of afwijkingen op de minimale maatregelen, een formeel proces uit te werken gebaseerd op het principe "pas toe of leg uit" (comply or explain).

4. Opvolging van IT-beveiliging en bijhorende risico's

- De Vlaamse overheid mist niet alleen een overkoepelend zicht op de IT-beveiligingsrisico's maar ook op de mate waarin de belangrijkste beheersmaatregelen aanwezig zijn om de gewenste IT-beveiliging en IT-continuïteit te kunnen garanderen. In het globaal rapport van de thema-audit informatiebeveiliging 2015 adviseerde Audit Vlaanderen om de aanpak van de verschillende entiteiten ten aanzien van het beheer van informatiebeveiliging op te volgen, te beoordelen en zo nodig bij te sturen. De nieuwe strategie voor informatieveiligheid stelt het Stuurorgaan voor Informatie- en ICT-beleid hiervoor verantwoordelijk. In de praktijk zou de overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen instaan voor de opvolging die nodig is om die verantwoordelijkheid te kunnen invullen.

- De ontwerpnota voor de Vlaamse Regering omtrent deze strategie vermeldt dat de werkgroep Informatieveiligheid en het agentschap Digitaal Vlaanderen hiertoe een gestandaardiseerde rapportering en een proces van self-assessment zullen ontwikkelen. De ontwerpnota stelt de individuele entiteiten verantwoordelijkheid voor het aanleveren van de relevante informatie. Een overkoepelende informatieveiligheidsdienst zou volgens de nieuwe strategie voor informatieveiligheid de kwaliteit van de self-assessments bewaken en de entiteiten desgewenst ondersteunen. Verder kan blijkens de voornoemde ontwerpnota ook een onafhankelijke en optionele conformiteitstoets worden georganiseerd om na te gaan in hoeverre de getroffen IT-beveiligingsmaatregelen voldoen aan de criteria van het raamwerk voor informatieclassificatie. Ongeacht de vernoemde conformiteitsaudits, vereisen de door de werkgroep Informatieveiligheid uitgewerkte minimale maatregelen in het kader van het raamwerk voor informatieclassificatie een periodieke, onafhankelijke beoordeling van de informatiebeveiliging bij de verwerking van gegevens vanaf informatieklasse 4. Ook deze onafhankelijke beoordelingen zouden potentieel kunnen toelaten te evalueren in hoeverre de maatregelen genomen binnen een entiteit voldoen aan de criteria beschreven in raamwerk voor informatieclassificatie.

- In het relanceplan Vlaamse Veerkracht kende de Vlaamse Regering met het project "Cyber security en uitrol SIEM" (VV065) in juni 2021 middelen toe aan Digitaal Vlaanderen om een standaardrapportering, een centraal dashboard voor de overkoepelende veiligheidsrisico's en een instrument voor self-assessment en voor conformiteitstoetsing uit te werken. Hoewel de opvolging van de rapportering en van de self-assessments na de invoering ervan recurrente werkzaamheden zullen vergen, is momenteel onduidelijk welk recurrent budget hiervoor zal worden ingezet.

4. Opvolging van IT-beveiliging en bijhorende risico's

- Daar waar de voorlopige nota aan de Vlaamse regering en het relanceplan een sterke aanzet geven voor de opzet van een overkoepelende informatieveiligheidsdienst, zijn het mandaat en de opdrachten daarvan echter nog onvoldoende bepaald. Een concretisering en bekrachtiging van het mandaat van de overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen door de Vlaamse Regering kan dat mandaat in de praktijk scherp stellen en verduidelijken ten aanzien van de diverse entiteiten.

Aanbeveling 5

Verkrijg en onderhoud een overkoepelend zicht op de IT-beveiligingsrisico's en de mate waarin de belangrijkste beheersmaatregelen aanwezig zijn om de gewenste IT-beveiliging en IT-continuïteit te kunnen garanderen voor de hele Vlaamse overheid. Zorg daarnaast voor een actieve opvolging van de huidige en toekomstige bedreigingen voor de IT-beveiliging van de kernprocessen. Dit door:

- het mandaat en de opdracht van de overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen te bepalen en te laten goedkeuren door de Vlaamse overheid;
- zo snel mogelijk een overzicht te creëren van de overkoepelende risico's met formele taxonomie en centrale escalatie volgens specifieke richtlijnen;
- te bepalen hoe het de overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen waakzaam zal blijven voor IT-beveiligingsincidenten in de (kern-)processen van de Vlaamse overheid (mogelijks via een planning voor de koppeling van de kernprocessen met de SIEM te bepalen, opvolging van nieuwe kwetsbaarheden, de IT-beveiliging – minstens van kernprocessen – actief opvolgen bij entiteiten en escaleren indien nodig);
- een kader uit te werken over hoe de overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen de VO-brede coördinatie zal vervullen met betrekking tot informatieveiligheid (o.m. in geval van kritieke incidenten);
- vast te leggen hoe de overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen zal rapporteren aan en afstemmen met het Stuurorgaan Vlaams Informatie- en ICT-beleid;
- de nodige recurrente werkingsmiddelen voor werkingsmiddelen voor de overkoepelende informatieveiligheidsdienst van Digitaal Vlaanderen te voorzien.

5. Beveiliging

- Om de verschillende onderdelen van de ICT-omgeving te beschermen tegen bedreigingen en kwetsbaarheden, is het van belang deze voldoende te beveiligen. Entiteiten kunnen zelf de beveiliging inregelen of dit uitbesteden aan derde partijen (bv. de gemeenschappelijke ICT-dienstverlening). Uit de deelaudits blijkt dat het voor individuele entiteiten niet eenvoudig is om autonoom de benodigde IT-beveiligingsmaatregelen te treffen. Het ontbreekt vaak aan de benodigde tijd en de kennis. Anderzijds blijkt dat de entiteiten wanneer ze beroep doen op - al dan niet gemeenschappelijk georganiseerde - uitbesteding, ook nog enkele stappen moeten zetten om tot een uitbesteding te komen die voldoende garanties en transparantie biedt op het vlak van IT-beveiliging.

- Zoals ook bleek tijdens de thema-audit ICT-organisatie, is IT-beveiliging veelal een bijkomende taak bovenop het takenpakket van operationele medewerkers. In de praktijk blijkt dat er hierdoor onvoldoende tijd overblijft om de noodzakelijke IT-beveiligingsaspecten op te nemen en dat mede hierdoor keuzes omtrent IT-beveiliging vaak moeten concurreren met allerlei andere operationele keuzes. Kwetsbaarheden en problemen zijn vaak gekend, maar blijven (te lang) open staan. Vaak ook is de kennis rond IT-beveiliging onvoldoende, waardoor controles op een gebrekkige wijze opgezet worden. Waar er externe controle is (bv. periodieke ISO 27001 audits), geven de entiteiten aan dat dit het bewustzijn en/of de maturiteit (samen met de kosten om deze maturiteit te bereiken) kunnen doen stijgen. Dit mede door de ingebouwde periodieke aandacht en de grotere betrokkenheid van het management.

- Wanneer entiteiten derde partijen inschakelen voor hun IT-beveiliging dan dienen daaromtrent de nodige afspraken gemaakt en geformaliseerd te worden. De desbetreffende overeenkomsten dienen dan ook de nodige IT-beveiligingsvereisten te bevatten. Daarnaast is het van belang de dienstverlening op regelmatige basis op te volgen om te verifiëren in welke mate de derde partijen deze IT-beveiligingsvereisten naleven. Na het in dienst nemen van nieuwe systemen of software verdwijnt de configuratie en het onderhoud immers al te vaak naar het achterplan, waardoor de IT-beveiliging niet langer gegarandeerd is.

- Tot voor kort werden na de acceptatie voor inproductiestelling veelal weinig tot geen verwachtingen gesteld omtrent periodieke evaluaties van de gerealiseerde mate van IT-beveiliging en/of omtrent de opvolging en certificering van de voorziene beheersmaatregelen (bv. ISAE) of van de alignering met industriestandaarden (zoals ISO27001). De overstap naar de nieuwe ICT-raamovereenkomsten 2022 biedt een opportuniteit om hier eventueel bijkomende afspraken over te maken.

5. Beveiliging

- In de praktijk doet een groot deel van de entiteiten in meerdere of mindere mate beroep op het aanbod van derde partijen voor het beheer van hun ICT-omgeving (bv. de gemeenschappelijke ICT-outsourcing en de gemeenschappelijke ICT-dienstverlening). De in het kader van het raamwerk voor informatieclassificatie door de werkgroep Informatieveiligheid uitgewerkte minimale maatregelen leggen voor wat betreft leveranciersrelaties op dat de vereisten rond IT-beveiliging opgenomen moeten worden in contractuele overeenkomsten. Dit gebeurt bv. via exploitatiedossiers, service portfolio's of modelcontracten. Hoewel afspraken voor de uitvoering van deze diensten tot op zekere hoogte in raamovereenkomsten zijn vastgelegd, ontbreken in veel specifieke gevallen duidelijke verwachtingen voor de IT-beveiliging. Bovendien zijn voor de operationele medewerkers die in de praktijk een rol spelen in het kader van de IT-beveiliging, bv. omtrent de opvolging van wat door derden geleverd wordt, de verwachtingen en bijgevolg ook het toezicht op de realisatie ervan vaak onvoldoende duidelijk.

- Uit de deelaudits blijkt dat ook entiteiten die gebruik maken van de gemeenschappelijke ICT-dienstverlening een grote verantwoordelijkheid hebben omtrent het maken van de juiste keuzes met betrekking tot IT-beveiliging. Uit de deelaudit bij de gemeenschappelijke ICT-dienstverlening blijkt dat het voor entiteiten niet altijd volstaat om blindelings de basisdienstverlening af te nemen om te voldoen aan de minimale maatregelen die door de werkgroep Informatiebeveiliging zijn vooropgesteld voor de informatieklassen 3, 4 en 5. De opties die de ontbrekende maatregelen kunnen invullen, worden in de praktijk weinig afgenomen.

- Naast het opnemen van de vereisten inzake IT-beveiliging in overeenkomsten met ICT-dienstenleveranciers, is het ook noodzakelijk deze vereisten geregeld op te volgen. Dit om na te gaan of de IT-beveiliging gegarandeerd blijft. In vele gevallen ontbreekt echter een structurele opvolging van de leveranciers met betrekking tot IT-beveiliging. Bij entiteiten leeft soms de perceptie dat ze de IT-beveiliging van de gemeenschappelijke ICT-dienstverlening minder dienen aan te sturen en op te volgen. Toch blijkt de gemeenschappelijke ICT-dienstverlening in verhouding tot de betrokken informatieklassen momenteel soms onvoldoende transparantie te bieden over de garanties die kunnen worden geboden en opgevolgd. Zo lang dit niet verbeterd, zijn bijkomende inspanningen van de klant-entiteiten nodig opdat deze hun finale verantwoordelijkheid en aansprakelijkheid voldoende kunnen invullen.

6. Waakzaamheid

- Om niet onnodig bloot te staan aan mogelijke IT-beveiligingsincidenten, dienen IT-systemen, applicaties, gebruikerstoestellen en netwerkcomponenten actueel gehouden te worden. Dit is een serieuze inspanning, maar van belang om te vermijden dat gekende kwetsbaarheden uitgebuit worden. Uit de deelaudits blijkt dat de Vlaamse overheid hier maar gedeeltelijk in slaagt en dat systemen kwetsbaar zijn voor gekende aanvallen.

- Daarnaast ontstaan steeds nieuwe kwetsbaarheden en bedreigingen door een continu wijzigend globaal technologisch landschap en worden aanvallen steeds complexer. Het is van belang die nieuwe kwetsbaarheden, en bedreigingen tijdig op te sporen, te analyseren en aan te pakken. De Vlaamse overheid neemt deze taken niet consequent op en is momenteel onvoldoende waakzaam hiervoor, waardoor de kans toeneemt dat deze zich in de praktijk voordoen. Ook van mogelijkheden om informatie uit te wisselen over nieuwe aanvalstechnieken en over indicatoren en evoluties m.b.t. cybercriminaliteit dan wel om hieromtrent samen te werken met andere overheidsinstaties (bv. ENISA meliCERTes of Cert.be) wordt weinig gebruik gemaakt.

- De gemeenschappelijke ICT-dienstverlening zet zelf al meerdere jaren een centraal systeem voor het beheer van veiligheidsgebeurtenissen en -informatie in (naar dergelijke systemen met hun bijhorende procedures wordt veelal verwezen met de term ‘Security Information & Event Management’ of afgekort ‘SIEM’). Momenteel verzamelt dit systeem hoofdzakelijk data afkomstig van kritieke netwerkcomponenten in het kader van de gemeenschappelijke netwerkdiensten. Doordat de afgedekte componenten en scenario’s beperkt zijn, schiet de SIEM in de praktijk vaak te kort en worden niet alle bedreigingen, kwetsbaarheden en beveiligingsincidenten gedetecteerd. Hoewel momenteel investeringen in de verdere uitbouw van de SIEM worden voorbereid, is de aanpak om op termijn meer van de gemeenschappelijke ICT-dienstverlening en mogelijks ook van de kernprocessen van de Vlaamse overheid te gaan monitoren nog niet bepaald.

- Individuele entiteiten doen tot op heden te weinig aan logging en monitoring om gebeurtenissen op het gebied van IT-beveiliging op te sporen en te analyseren. Met de nieuwe ICT-raamovereenkomst 2022 krijgen individuele entiteiten in de toekomst de mogelijkheid om zelf bijkomende logs en gebeurtenissen toe te voegen aan het SIEM platform van de gemeenschappelijke ICT-dienstverlening. Momenteel is nog niet geconcretiseerd hoe dit geïmplementeerd gaat worden.

6. Waakzaamheid

- Het raamwerk voor informatieclassificatie bepaalt minimale maatregelen voor veiligheidslogging en monitoring. Vanaf de verwerking van gegevens van klasse 1 dienen gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen te worden geregistreerd in logbestanden en geregeld te worden beoordeeld. De effectieve monitoring en scanning via een SIEM is een vereiste vanaf klasse 4. De minimale maatregelen preciseren niet wat gemonitord en opgevolgd dient te worden. Het is de verantwoordelijkheid van de entiteiten om dat te bepalen. Hoe entiteiten hun SIEM in de praktijk best opzetten, is voor veel entiteiten momenteel een groot vraagteken, waardoor mogelijk niet alle belangrijke IT-beveiligingsgebeurtenissen zullen worden gedetecteerd en/of meer zal worden opgevolgd dan wenselijk. Over hoe veiligheidsincidenten kunnen worden gedetecteerd die zich bij meerdere entiteiten tegelijk voordoen, moeten bovendien nog verdere afspraken worden gemaakt.

- Eén van de drie prioriteiten van de nieuwe strategie voor informatieveiligheid spitst zich toe op het uitwerken van weerbare digitale processen en een robuuste infrastructuur met als doel het veiligheidsniveau van de informatieverwerking op operationeel niveau te verhogen. Om dit te helpen verwezenlijken, kan onder meer worden ingezet op een permanent beschikbaar ‘Security Operations Center’ (SOC) en een verbeterd SIEM platform. De uitrol van deze mogelijkheden maakt deel uit van het perceel Service-Integratiediensten van de nieuwe ICT-raamovereenkomst 2022. Hoe deze dienstverlening voor de gemeenschappelijke ICT-Diensten precies zal worden ingericht, maakt deel uit van overleg tijdens de transitieperiode.

7. Veerkracht

- Elke entiteit staat in voor incident- en crisisbeheer binnen de dagelijkse werking van haar eigen diensten en behoort daartoe de nodige incident- en crisisbeheersprocessen op te stellen. Daarnaast besliste de Vlaamse Regering reeds op 6 mei 2011 dat de entiteiten dienen te bepalen of hun processen kritisch, essentieel of noodzakelijk zijn en in functie daarvan continuïteitsplannen dienen op te stellen.

- Het raamwerk voor informatieclassificatie legt minimale maatregelen voor het beheer van de bedrijfscontinuïteit vast. Voor alle informatieklassen is een volwaardig en periodiek getest continuïteitsplan vereist.

- Hoewel weinig tot niet geëxpliciteerd, impliceren de gevaren van moderne ransomware-aanvallen dat voldoende offline backups moeten worden bijgehouden. Daarnaast kunnen verschillende processen en omstandigheden ook aanleiding geven tot beschikbaarheidseisen waarbij ook de onderliggende IT-infrastructuur daarbij voldoende redundant moet zijn opgezet en de ondersteunende dienstverlening voldoende beschikbaar moet zijn.

- Uit de auditwerkzaamheden blijkt dat de geauditeerde entiteiten niet over voldoende uitgewerkte beheersprocessen voor IT-beveiligingsincidenten en -crisissen beschikken. De toevallig beschikbare medewerkers maken nog veel keuzes met betrekking tot de beheersing van de IT-beveiliging op het moment dat incidenten zich voordoen. De geauditeerde entiteiten voeren ook nagenoeg geen oefeningen uit om na te gaan of eventueel bestaande herstelplannen in de praktijk functioneren en de continuïteit van hun diensten garanderen.

- Als entiteiten voor hun werking afhankelijk zijn van derde partijen, dan moeten ze zich vergewissen van de garanties die deze organisaties op het vlak van bedrijfscontinuïteit bieden (SLA's, RTO, RPO). Zo rekenen verschillende entiteiten op de gemeenschappelijke ICT-dienstverlening voor de continuïteit van hun werking zonder dat hieromtrent concrete afspraken zijn gemaakt. Auditwerk toont aan dat voor de GID-diensten onvoldoende structureel wordt nagedacht over bedrijfscontinuïteit en –herstel in het kader van IT-beveiligingscrisissen. Daardoor kan onder meer de continuïteit in het geval van een gerichte grootschalige cyberaanval momenteel niet voldoende worden gegarandeerd.

7. Veerkracht

- Voor de centrale communicatie en aansturing van entiteitoverschrijdende crisissen richtte de Vlaamse Regering het Crisiscentrum van de Vlaamse Overheid (CCVO) op. Onvoldoende voorbereide communicatielijnen en een gebrekkige doorstroming van informatie over incidenten en crisissen m.b.t. IT-beveiliging bemoeilijken het CCVO echter om efficiënt en daadkrachtig op te treden.

- Bij IT-beveiligingsincidenten en crisissen die een impact hebben op de IT-beveiliging en -continuïteit van meerdere entiteiten binnen de Vlaamse overheid, dringt een gecentraliseerde strategie en aanpak zich op. Dit laat toe incidenten efficiënter aan te pakken en de verdere verspreiding tegen te gaan. In dat verband vermeldt de nieuwe strategie voor informatieveiligheid de oprichting van een team dat centrale coördinatie en sturing verleent bij ernstige informatieveiligheidsincidenten. Dit zogeheten CSIRT (Computer Security Incident Response Team) zou in voorkomend geval de crisiscoördinatie op zich nemen in samenwerking met het CCVO (CrisisCentrum van de Vlaamse Overheid). Het is de ambitie om daartoe een formeel proces op te zetten, echter zijn er nog geen concrete plannen gemaakt of stappen gezet.

- Hoewel binnen de Vlaamse overheid op verschillende niveaus initiatieven voor bedrijfscontinuïteit zijn genomen, is de continuïteit van de diensten geleverd aan de burger in geval van grootschalige incidenten en calamiteiten op dit moment niet altijd verzekerd. De respectievelijke entiteiten, Digitaal Vlaanderen en het CCVO hebben voor IT-beveiligingscrisissen te weinig specifieke voorbereidingen getroffen of concrete scenario's uitgewerkt en getest. Een structurele oplossing om op korte termijn expertise en mankracht beschikbaar te stellen in geval van grootschalige cyberaanvallen ontbreekt. Als gevolg daarvan is de Vlaamse overheid nauwelijks voorbereid om zulke aanvallen op afdoende wijze te coördineren en af te handelen.

V. Verzendlijst

Vlaamse overheid

AUDIT VLAANDEREN

Verzendlijst (1/2)

De voorzitter van het Voorzitterscollege

Mevrouw Julie Bynens	Secretaris-generaal van het Departement Kanselarij en Buitenlandse Zaken

De voorzitter van het Stuurorgaan Vlaams Informatie- en ICT-beleid

De heer Mark Andries	Administrateur-generaal van het Agentschap Innoveren en Ondernemen

De leidend ambtenaren van de entiteiten die gevat werden door deze thema-audit

De heer Mark Andries	Administrateur-generaal van het Agentschap Innoveren en Ondernemen
De heer James Van Casteren	Administrateur-generaal van het Vlaams Agentschap voor Personen met een Handicap
De heer Tom Roelants	Administrateur-generaal van het Agentschap Wegen en Verkeer
De heer Chris Danckaerts	Gedelegeerd Bestuurder van De Vlaamse Waterweg
Mevrouw Barbara Van Den Haute	Administrateur-generaal van Digitaal Vlaanderen

De betrokken decentrale auditdienst

De heer Filip Waghemans	Auditor van De Vlaamse Waterweg

De voorzitter van de betrokken raad van bestuur

Mevrouw Frieda Brepoels	Voorzitter Raad van Bestuur van De Vlaamse Waterweg

De voorzitter van het betrokken auditcomité

Mevrouw Annemie Baeyaert	Voorzitter van het Auditcomité van De Vlaamse Waterweg

De bevoegde ministers van de entiteiten die gevat werden door deze thema-audit

Mevrouw Hilde Crevits	Vlaams minister van Economie, Innovatie, Werk, Sociale economie en Landbouw
De heer Wouter Beke	Vlaams minister van Welzijn, Volksgezondheid, Gezin en Armoedebestrijding
Mevrouw Lydia Peeters	Vlaams minister van Mobiliteit en Openbare Werken
De heer Jan Jambon	Vlaams minister van Buitenlandse Zaken, Cultuur, Digitalisering en Facilitair Management

Verzendlijst (2/2)

De minister bevoegd voor interne audit	
De heer Bart Somers	Viceminister-president van de Vlaamse Regering, Vlaams minister van Binnenlands Bestuur, Bestuurszaken, Inburgering en Gelijke Kansen
De minister-president en viceminister-presidenten	
De heer Jan Jambon	Minister-president van de Vlaamse Regering, Vlaams minister van Buitenlandse Zaken, Cultuur, Digitalisering en Facilitair Management
De heer Ben Weyts	Viceminister-president van de Vlaamse Regering, Vlaams minister van Onderwijs, Sport, Dierenwelzijn en Vlaamse Rand
Mevrouw Hilde Crevits	Viceminister-president van de Vlaamse Regering, Vlaams minister van Economie, Innovatie, Werk, Sociale economie en Landbouw
De leden van het auditcomité van de Vlaamse administratie	
De heer Jean-Pierre Garitte	Voorzitter van het auditcomité van de Vlaamse administratie en onafhankelijk deskundige
Mevrouw Iwona Muchin	Onafhankelijk deskundige
De heer Johan Christiaens	Onafhankelijk deskundige
Mevrouw Lieze Moeyersons	Onafhankelijk deskundige
Mevrouw Miet Vandersteegen	Vertegenwoordiger van de Vlaamse Regering
De heer Martin Ruebens	Vertegenwoordiger van de Vlaamse Regering
Mevrouw Myriam Parys	Vertegenwoordiger van de Vlaamse Regering
De secretaris van het auditcomité van de Vlaamse administratie	
Dieter Vanhee	Afdelingsverantwoordelijke Strategie, Coördinatie en Communicatie bij het Departement Kanselarij en Buitenlandse Zaken
Rekenhof	
Mevrouw Hilde François	Voorzitter van het Rekenhof

COLOFON

VERANTWOORDELIJKE UITGEVER
Mark Vandersmissen
Administrateur-generaal
Audit Vlaanderen

CONTACT
Audit Vlaanderen
Havenlaan 88, bus 24
1000 Brussel
02 553 45 55
Deze publicatie is ook beschikbaar op www.auditvlaanderen.be

Vlaamse overheid

AUDIT VLAANDEREN