Vlaamse overheid

Thema-audit Informatiebeveiliging 2020

Globaal rapport | 26 januari 2021

AUDIT VLAANDEREN

Auditteam

Lydia Putseys, Auditor
Maxim Ternier, Auditor (EY)
Jan Verbrugghe, Auditor (EY)
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 informatiebeveiliging 2020

- **Informatiebeveiligingsrisico's zijn groot** en reëel en de noodzaak om ze aan te pakken blijft steeds toenemen. Naarmate de dienstverlening van lokale besturen meer digitaal verloopt en de werking dus ook meer en meer steunt op ICT-systemen, vergroot ook de potentiële impact van kwetsbaarheden.

- Daarom voerde Audit Vlaanderen **in 2017 – 2018** de **thema-audit Informatiebeveiliging** uit **bij 28 lokale besturen**. Dit initiatief toonde aan dat de geauditeerde lokale besturen wel diverse stappen zetten om hun informatiebeveiliging te verbeteren, maar dat de belangrijke risico's toch nog onvoldoende beheerst waren. Zo konden ethische hackers bij 75% van de lokale besturen de ICT-omgeving overnemen. Daarnaast demonstreerde deze audit dat verscheidene haalbare beschermingsmaatregelen onderbenut blijven.

- In **2019** vond de **opvolging van de aanbevelingen** plaats: de eerder geauditeerde lokale besturen hadden inmiddels vooruitgang geboekt op het domein van informatiebeveiliging. Toch was het duidelijk dat meer of bijkomende inspanningen nodig waren gezien een aanzienlijk deel van de aanbevelingen nog niet gerealiseerd waren.

- Ook blijft de problematiek van phishing en/of ransomware aanvallen toenemen, dit blijkt onder meer uit de regelmatige berichtgeving over (succesvolle) aanvallen bij bedrijven of publieke instellingen.

- Omwille van de ernst van de nog openstaande aanbevelingen m.b.t. informatiebeveiliging en het verder toenemende belang van cybersecurity, besliste het auditcomité voor de lokale besturen om deze problematiek verder op te volgen middels een **tweede thema-audit informatiebeveiliging**.

Auditdoelstelling, risico's en reikwijdte

- De thema-audit Informatiebeveiliging 2020 evalueert in welke mate bij de lokale besturen beheersmaatregelen aanwezig zijn om het gewenste niveau van **beschikbaarheid, integriteit en vertrouwelijkheid van informatie** te garanderen.

- Om op de bovenstaande doelstelling een antwoord te formuleren, ontwikkelde Audit Vlaanderen een controleprogramma dat verder bouwt op de belangrijkste onbeheerste risico's zoals vermeld in het globaal rapport van de thema-audit informatiebeveiliging van 18 september 2018. Dat controleprogramma werd aangevuld om ook rekening te houden met de bijkomende verplichtingen omtrent de beveiliging van persoonsgegevens ten gevolge van de inwerkingtreding van de Algemene Verordening Gegevensbescherming (**AVG**).

- De belangrijkste beheersdoelstellingen in dit verband zijn:
  - Beschikbaarheid: informatie moet toegankelijk zijn – zowel nu als in de toekomst – wanneer het bedrijfsproces dat vereist.
  - Integriteit: de accuraatheid, de volledigheid en de geldigheid van informatie mag niet (on)opzettelijk worden gewijzigd.
  - Vertrouwelijkheid: gevoelige informatie dient beschermd te worden tegen niet-geautoriseerde toegang en/of verspreiding.

- Daarnaast wordt in het kader van deze thema-audit – net zoals bij andere audits bij lokale besturen – ook de aanpak van organisatiebeheersing beoordeeld.

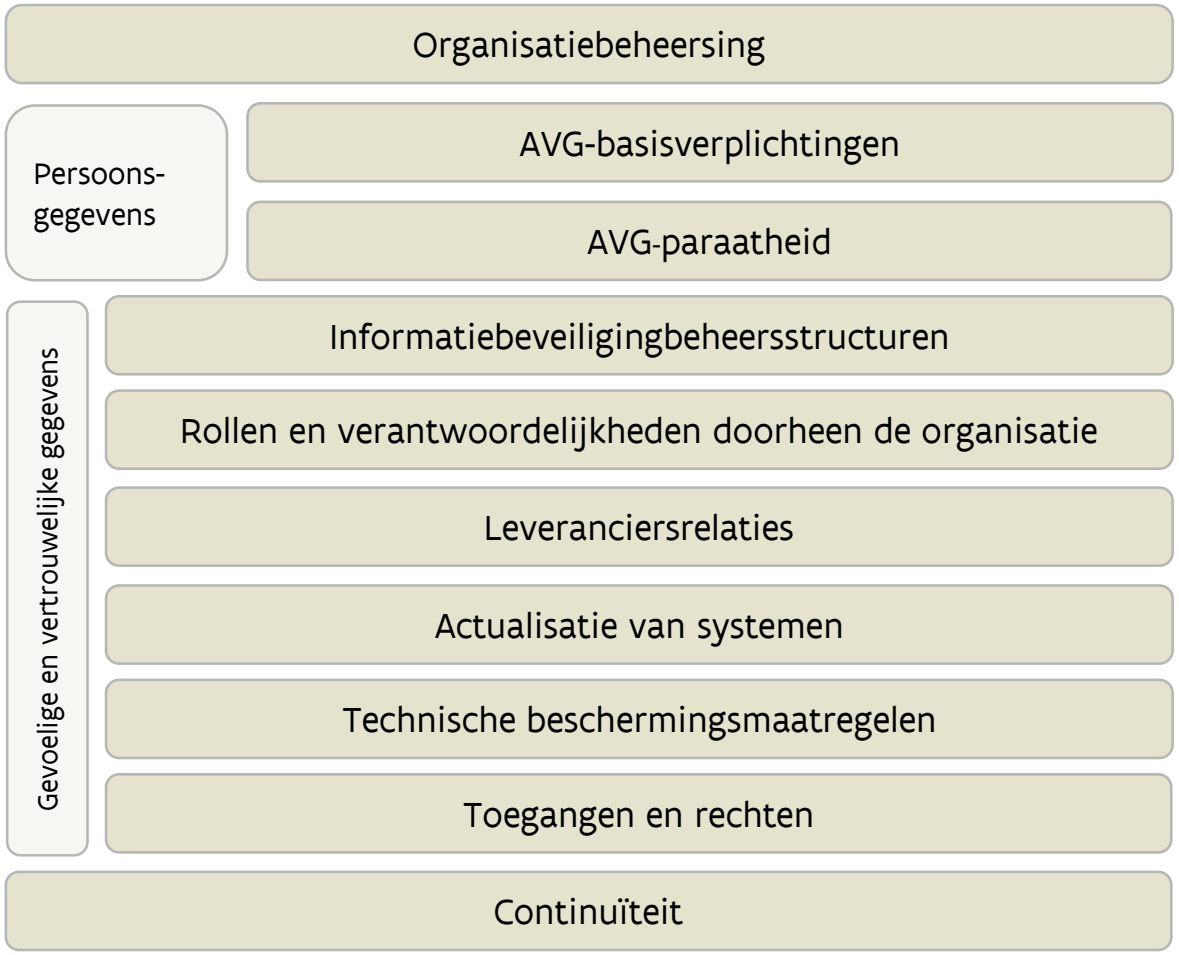
Auditdoelstelling, risico's en reikwijdte

- Deze audit kadert in de ondersteunende rol die Audit Vlaanderen opneemt in het streven naar een effectieve, efficiënte, kwaliteitsvolle en integere werking van de lokale besturen. Audit Vlaanderen levert met deze thema-audit enerzijds voor de betrokken besturen een rapport af dat een overzicht biedt van sterktes en verbeterpunten. Anderzijds komt Audit Vlaanderen tot globale conclusies en aanbevelingen die zinvol kunnen zijn voor alle lokale besturen als geheel en voor andere actoren (bijvoorbeeld de Vlaamse overheid). Deze globale conclusies zijn verwerkt in dit globaal rapport.

- Gedurende deze thema-audit, bezocht Audit Vlaanderen **6 lokale besturen**, nl. Aalst, Boutersem, Denderleeuw, Geel, Wervik en Zutendaal. De selectie van de lokale besturen is gebaseerd op:
  - Lokale besturen waar Audit Vlaanderen recent geen andere audits heeft uitgevoerd;
  - Spreiding van de lokale besturen o.b.v. inwonersaantal;
  - Spreiding van geografische ligging.

- Audit Vlaanderen wilt graag haar appreciatie en dank uiten aan de geauditeerde besturen voor de constructieve samenwerking. Dit globaal rapport kwam tot stand dankzij hun waardevolle inbreng.

Controleprogramma en maturiteitsniveau's



Legende

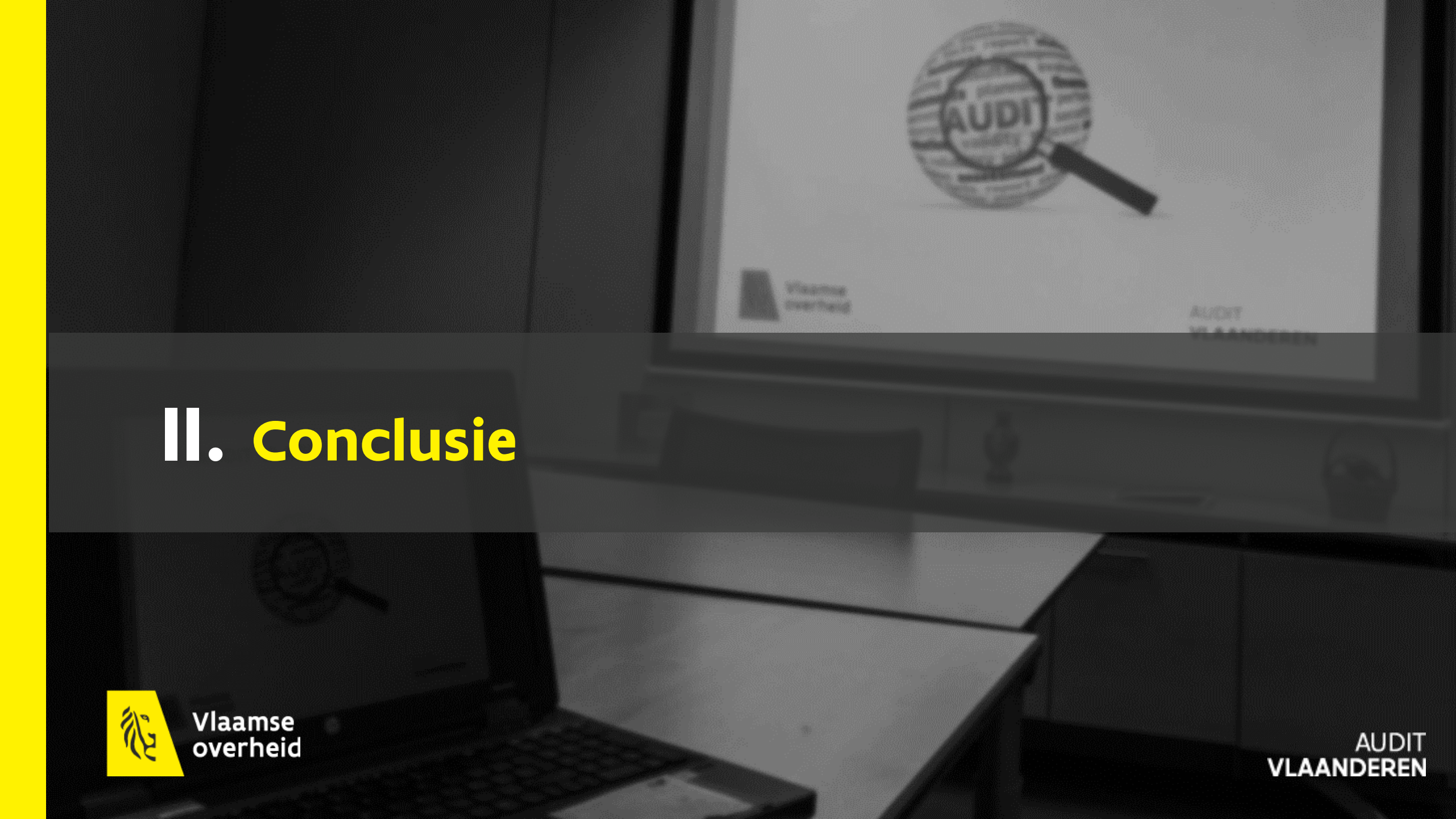
0 – Onbestaand
Er bestaan geen of zeer weinig beheersmaatregelen. Het controlebewustzijn is eerder laag en er worden weinig acties ondernomen om te komen tot een adequaat systeem van organisatiebeheersing.

1 – Ad-hocbasis
Er zijn beheersmaatregelen uitgewerkt op ad-hocbasis. Het bewustzijn van de nood aan adequate beheersmaatregelen (organisatiebeheersing) groeit, maar er is nog geen gestructureerde of gestandaardiseerde aanpak. Het systeem van organisatiebeheersing draait meer rond personen dan rond systemen.

2 – Gestructureerde aanzet
Er is een gestructureerde aanzet tot de ontwikkeling van beheersmaatregelen. De beheersinstrumenten zijn dus in ontwikkeling, maar worden nog niet toegepast ('Plan').

3 – Gedefinieerd
Beheersmaatregelen zijn aanwezig. Zij zijn gestandaardiseerd, gedocumenteerd, gecommuniceerd en worden toegepast ('Do').

4 – Beheerst systeem
De beheersmaatregelen worden periodiek intern geëvalueerd en bijgestuurd ('Check' & 'Act'). Er is een actief adequaat en doeltreffend systeem van organisatiebeheersing.



II. Conclusie

Vlaamse overheid

AUDIT VLAANDEREN

Conclusie thema-audit informatiebeveiliging 2020

- De auditresultaten tonen aan dat de lokale besturen bijkomende inspanningen dienen te leveren om de risico's voor informatiebeveiliging voldoende te beheersen.

- Het extrapoleren van de resultaten van een beperkte steekproef bij 6 lokale besturen naar alle Vlaamse lokale besturen is vanuit statistisch oogpunt niet correct. De resultaten van deze thema-audit informatiebeveiliging 2020 liggen echter wel in lijn met de resultaten van de thema-audit Informatiebeveiliging 2017-2018 bij 28 lokale besturen.

- Hoewel het belang van ICT en daarmee van informatiebeveiliging almaar toeneemt, lijken de lokale besturen geen vooruitgang te boeken met de beheersing van de risico's rond "Leveranciersrelaties", "Actualisatie van systemen", "Technische beschermingsmaatregelen" en "Toegangen en rechten".

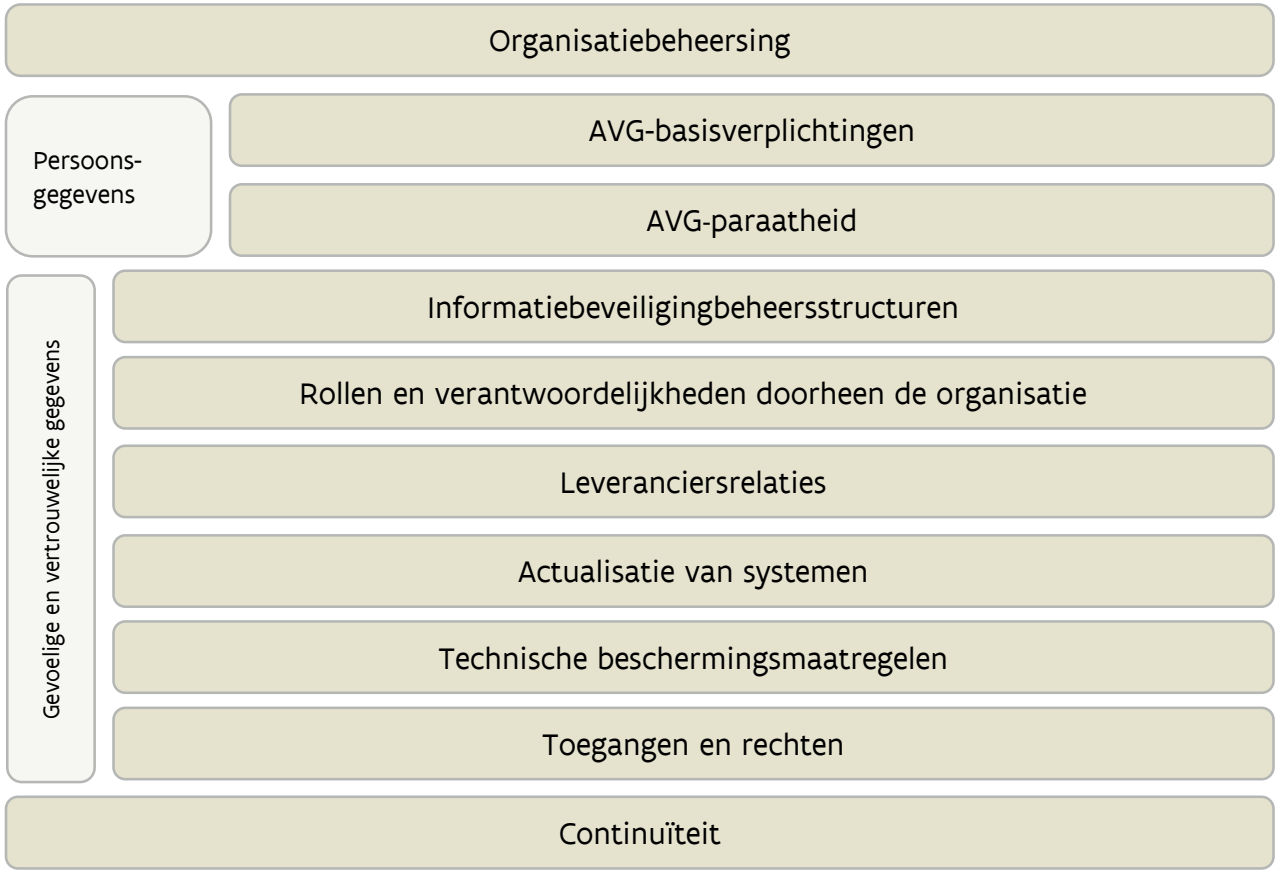
- De meeste lokale besturen zijn zich ervan bewust dat continuïteit van de dienstverlening essentieel is, maar ze maken van het uitwerken van een formeel continuïteitsplan nog onvoldoende werk.

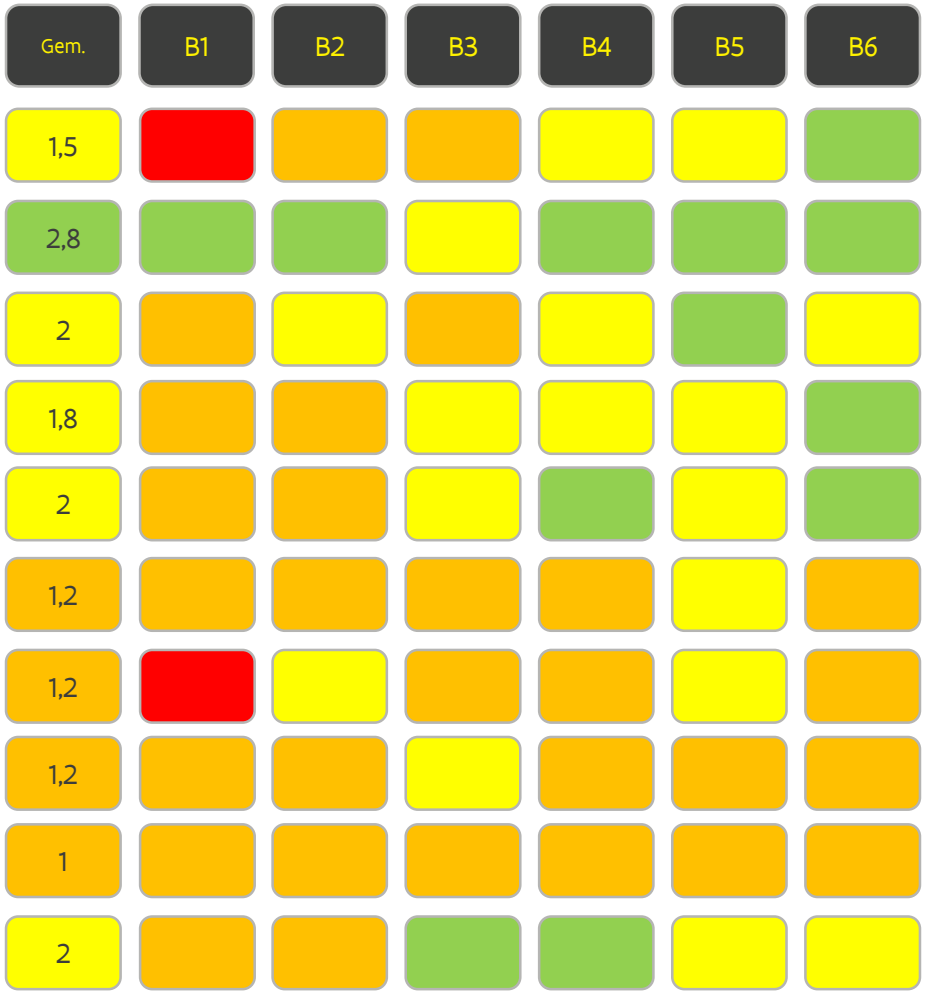
- De lokale besturen beschikken over de nodige beheersmaatregelen om aan de AVG basisverplichtingen te voldoen. Ook voor de vertaling van de principes en verplichtingen voor de bescherming van persoonsgegevens naar de praktijk zijn al inspanningen geleverd. Verdere initiatieven zijn evenwel nog nodig om hieromtrent tot een voldoende paraatheid te komen.

- Lokale besturen met een betere organisatiebeheersing, beheersen de onderzochte risico's voor informatiebeveiliging in het algemeen beter.

Resultaten thema-audit informatiebeveiliging 2020

Audit Vlaanderen auditeerde bij deze thema-audit 6 verschillende lokale besturen, nl. Aalst, Boutersem, Denderleeuw, Geel, Wervik en Zutendaal.





Vergelijking resultaten thema-audits informatiebeveiliging

		Gem. 2020	Gem. 2017-2018
Organisatiebeheersing		1,5	1,8
Persoons-gegevens	AVG-basisverplichtingen	2,8	-
	AVG-paraatheid	2	-
Gevoelige en vertrouwelijke gegevens	Informatiebeveiligingbeheersstructuren	1,8	1,9
	Rollen en verantwoordelijkheden doorheen de organisatie	2	1,9
	Leveranciersrelaties	1,2	1,0
	Actualisatie van systemen	1,2	1,6
	Technische beschermingsmaatregelen	1,2	1,2
	Toegangen en rechten	1	1,4
Continuïteit		2	2,2

De gemiddelde resultaten van de thema-audit informatiebeveiliging uit 2020 (links) tonen in vergelijking met de resultaten van de thema-audit uit 2017 - 2018 (rechts) geen significante vooruitgang. Vele informatiebeveiligingsrisico's zijn nog steeds onvoldoende onder controle.

Het ICT-landschap van de lokale besturen evolueerde sinds 2017 wel. Zo digitaliseerden veel besturen de afgelopen jaren verschillende administratieve processen en zetten ze massaal stappen op het vlak van telewerken.

Het controleprogramma van de thema-audit informatiebeveiliging hernam niet alle onderdelen van de thema-audit informatiebeveiliging 2017-2018. Ook werden sommige elementen beperkt herschikt.
In het controleprogramma van de thema-audit informatiebeveiliging 2020 zijn de verplichtingen omtrent de beveiliging van persoonsgegevens ten gevolge van de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) toegevoegd: AVG-basisverplichtingen en AVG-paraatheid. De AVG is volledig van toepassing sinds 25 mei 2018 en maakte tijdens de thema-audit informatiebeveiliging 2017-2018 geen deel uit van het controleprogramma.

Getekend door:Lydia Putseys (Signature)
Getekend op:2021-01-26 13:55:07 +01:00
Reden:Ik keur dit document goed

Lydia Putseys
Auditor

Getekend door:Karel Bruneel (Signature)
Getekend op:2021-01-26 14:21:15 +01:00
Reden:Ik keur dit document goed

Karel Bruneel
Senior-auditor

Getekend door:Gunter Schryvers (Signat
Getekend op:2021-01-26 14:23:44 +01:00
Reden:Ik keur dit document goed

Gunter Schryvers
Manager-auditor

Getekend door:Mark Vandersmissen (Sig
Getekend op:2021-01-26 15:32:03 +01:00
Reden:Ik keur dit document goed

Mark Vandersmissen
Administrateur-generaal

III. Algemene bevindingen en verbeterpunten

Vlaamse overheid

AUDIT VLAANDEREN

AVG - Basisverplichtingen

2020	2,8	0	0	17%	83%	0%
2017 - 2018	*Maakte geen deel uit van het controleprogramma*					

AVG - Basisverplichtingen

Elk bestuur dat persoonsgegevens verwerkt, is volgens de Algemene Verordening Gegevensbescherming (AVG) verplicht die informatie te beschermen en te beveiligen. Daarvoor treft het bestuur de nodige maatregelen zoals het aanstellen van een functionaris voor gegevensbescherming (FG) of data protection officer (DPO), het bijhouden van een verwerkingsregister en een incidentenregister, het afsluiten van verwerkingsovereenkomsten en het opstellen van een informatieveiligheidsplan.

- Alle geauditeerde lokale besturen beschikken over de nodige beheersmaatregelen om aan de AVG basisverplichtingen te voldoen.
- Aanduiding functionaris voor gegevensbescherming (FG)
  - Alle geauditeerde lokale besturen hebben al enkele jaren een functionaris voor gegevensbescherming aangesteld. De meerderheid van de geauditeerde lokale besturen geeft voorkeur aan een externe partij om deze functie in te vullen. Daarnaast hebben deze organisaties vaak een intern aanspreekpunt dat de externe FG ondersteunt en een brugfunctie vervult.
  - De tijdsbesteding van de functionarissen varieert sterkt van bestuur tot bestuur.
  - Bij enkele lokale besturen werd een wissel van functionaris vastgesteld. Dit verloop kan vertragend werken op de inspanningen m.b.t. informatieveiligheid.
- Verwerkingsregister(s)
  - Alle geauditeerde lokale besturen beschikken over een verwerkingsregister. Tijdige actualisatie is echter noodzakelijk en blijft een aandachtspunt.
- Verwerkersovereenkomsten
  - Lokale besturen zijn zich bewust van de noodzaak om verwerkingsovereenkomsten af te sluiten. Toch blijkt het vaak moeilijk om leveranciers zich hiertoe te laten verbinden. Zo zijn bij verschillende organisaties nog onderhandelingen lopende om enkele overeenkomsten af te sluiten.
  - Een overzicht van alle leveranciers of een lijst van de verwerkingsactiviteiten gelinkt aan de daarvoor ingezette toepassingen is nuttig om dit op te volgen.
- Incidentenregister
  - Incidentenregisters zijn bij alle geauditeerde lokale besturen aanwezig, maar het systematisch registreren van incidenten vraagt een inspanning die niet door alle besturen geleverd wordt.
- Veiligheidsplan
  - De meeste geauditeerde besturen stelden hun veiligheidsplan op in 2017-2018. Slechts bij een aantal besturen is een eerste actualisatieronde lopende.

AVG - Paraatheid

2020	2,2	0%	33%	17%	50%	0%
2017 - 2018	*Maakte geen deel uit van het controleprogramma*					

AVG - Paraatheid

In het licht van de Algemene Verordening Gegevensbescherming (AVG) speelt de bescherming van persoonsgegevens een cruciale rol. AVG-paraatheid beoogt na te gaan in welke mate de organisatie daar in de praktijk consistent aandacht voor heeft. In het kader van deze audit komen de volgende aspecten aan bod: rechten van betrokkenen, incidentenbeheer en de vertaalslag in de praktijk.

- Rechten van betrokkenen
  - De AVG geeft de personen wiens persoonsgegevens worden verwerkt (= de betrokkenen) verschillende expliciete rechten (bv. recht op inzage, bezwaar, rectificatie en wissen van de verwerkte persoonsgegevens). Om de uitoefening van deze rechten vlot mogelijk te maken, dient de organisatie een gepaste aanpak hieromtrent te hebben.
  - De procedures en/of processen om snel en gepast te kunnen reageren wanneer deze rechten worden uitgeoefend, zijn slechts zelden beschikbaar.
  - De meeste lokale besturen geven aan om ad-hoc op de wetgeving terug te vallen.

- Incidentenbeheer
  - Alle geauditeerde lokale besturen stelden procedures op voor het beheren van incidenten. Soms beperkt zich dit enkel tot een schema, wat de toepasbaarheid beperkt.
  - De bekendheid van en communicatie omtrent deze procedure is vaak onvoldoende: de procedure is in de meeste gevallen intern weinig gekend.
  - Meldingen van informatieveiligheids- of AVG- incidenten komen in veel gevallen via de leden van informatieveiligheidscel.

- Vertaalslag in de praktijk
  - In de periode 2017 - 2018 organiseerden alle geauditeerde lokale besturen sensibiliseringscampagnes, vaak in samenwerking met de externe FG. Dergelijke initiatieven werden nadien niet altijd herhaald.
  - Concrete instructies voor medewerkers om informatiebeveiliging toe te passen in hun dagelijkse werkzaamheden zijn niet altijd beschikbaar.
  - Interne ondersteuning voor medewerkers om vragen via een gekende weg (bv. intern aanspreekpunt) te stellen, blijkt bij verschillende lokale besturen een meerwaarde.
  - De (externe) FG is vaak niet in de gehele organisatie gekend. De interne aanspreekpunten daarentegen zijn dat wel.

Informatiebeveiligings-beheersstructuren

2020	1,8	0%	33%	50%	17%	0%
2017 - 2018	1,9	0%	26%	56%	19%	0%

Informatiebeveiligingsbeheersstructuren

Om informatiebeveiliging te kunnen garanderen is de aanwezigheid van gepaste structuren een belangrijke randvoorwaarde. Elke organisatie dient de nodige overleg- en communicatiestructuren in te richten om de informatiebeveiliging op te volgen, te beheren en doorheen de organisatie te doen leven.

- Informatieveiligheidscel
  - Alle besturen richtten een informatieveiligheidscel op. Toch zijn er opmerkelijke verschillen tussen de lokale besturen. Zo is de informatieveiligheidscel niet bij elk lokaal bestuur even actief en/of even sterk verbonden met de rest van de organisatie;
  - De samenstelling van de informatieveiligheidscel bestaat minstens uit de sleutelactoren binnen de organisatie. Bij enkele lokale besturen worden ook andere medewerkers op afroep uitgenodigd, naargelang het onderwerp of de nood aan sensibilisering. Zo streven de organisaties naar betrokkenheid binnen de bredere organisatie;
  - De frequentie van samenkomst varieert van 2 tot 4 keer per jaar. De frequentie van overleg tussen het intern aanspreekpunt en de externe FG ligt hoger;
  - De informatieveiligheidscel vervult een centrale rol voor informatiebeveiliging maar legt de focus voornamelijk op initiatieven rond de AVG.

- Andere overleg- en communicatiestructuren
  - Informatiebeveiliging wordt slecht sporadisch op de agenda van andere overlegorganen geagendeerd. De verbondenheid van de informatieveiligheidscel met de rest van de organisatie heeft dus nog groeipotentieel.

Rollen en verantwoordelijkheden

2020	2	0%	33%	33%	33%	0%
2017 - 2018	1,9	0%	26%	56%	19%	0%

Rollen en verantwoordelijkheden

Iedereen is betrokken bij de realisatie van informatiebeveiliging. Het is dan ook belangrijk dat elkeen zich bewust is van zijn/haar verantwoordelijkheden en rol daaromtrent. In overeenstemming met haar informatiebeveiligingsbeleid, dient elk bestuur te bepalen en te communiceren wat de verschillende rollen en verantwoordelijkheden inzake informatiebeveiliging zijn. Zeker voor sleutelactoren dienen rollen en verantwoordelijkheden voldoende vastgelegd en afgestemd te zijn.

- De verantwoordelijkheden inzake informatieveiligheid zijn meestal vastgelegd in een of meerdere van de volgende documenten:
  - Arbeidsreglement;
  - Veiligheidsplan;
  - Functiebeschrijvingen;
  - Oprichtingsbesluit van de informatieveiligheidscel;
- Rollen en verantwoordelijkheden inzake informatieveiligheid worden te vaak uitsluitend toegekend aan medewerkers van de dienst ICT en/of de functionaris voor gegevensbescherming;
- Verantwoordelijkheden of verwachtingen voor medewerkers zijn vaak weinig of niet gedefinieerd, ook niet voor sleutelactoren uit de informatieveiligheidscel of externen;
- Vaak ontbreekt een vertaling van de verwachtingen of verantwoordelijkheden naar concrete taken. Dit ondermijnt het draagvlak en het bewustzijn rond informatiebeveiliging en maakt dat het risico bestaat dat sommige taken en verantwoordelijkheden niet, onvoldoende of dubbel worden opgenomen.

In Wervik is een goede praktijk voor rollen en verantwoordelijkheden vastgesteld.

Leveranciersrelaties

2020	1,2	0%	83%	17%	0%	0%
2017 - 2018	1,1	0%	93%	7%	0%	0%

Leveranciersrelatie

Besturen vertrouwen in belangrijke mate op externe software- en ICT-dienstenleveranciers. Om te vermijden dat misverstanden ontstaan over wie wat opneemt of dat de invulling verschilt van de verwachtingen, is het belangrijk om met deze partijen concrete afspraken te maken. Gelet op de afhankelijkheid van de leveranciers, is het ook belangrijk voldoende op te volgen in welke mate deze leveren wat afgesproken is en hen aan te spreken bij problemen of incidenten.

- De lokale besturen werken voor de verwerking, opslag en communicatie van gegevens samen met meerdere software- en ICT-dienstenleveranciers die een verregaande toegang hebben tot de systemen van het lokaal bestuur. Meer nog, de lokale besturen vertonen een grote afhankelijkheid van software- en ICT-dienstenleveranciers;

- Toch ontbreken frequent concrete afspraken voor de samenwerking rond beheer en opvolging van:
  - Informatiebeveiliging;
  - rechten en toegangen;
  - configuraties en monitoring;
  - licenties en certificaten;
  - storingen en structurele problemen;
  - documentatie en logging;

- Lokale besturen zien nauwelijks toe op de naleving van aanwezige afspraken met de leveranciers. Vaak heeft de verantwoordelijke voor de opvolging van de leveranciers geen volledig overzicht van de overeenkomsten of de daarbij horende (veiligheids)vereisten. Ook zijn de ICT-dienstenleveranciers niet vereist om te rapporteren over hun geleverde of uitgevoerde acties. Dit bemoeilijkt de opvolging van de diensten of uitgevoerde activiteiten;

- Bij diverse lokale besturen zijn bepaalde formele contracten niet aanwezig. Wanneer dit wel het geval is, zijn ze vaak niet actueel.

Actualisatie van systemen

2020	1,2	17%	50%	33%	0%	0%
2017 - 2018	1,6	0%	44%	56%	0%	0%

Actualisatie van systemen

Lokale besturen dienen hun gebruikerstoepassingen en de onderliggende systemen van hun ICT-infrastructuur systematisch te actualiseren. Daartoe moet duidelijk zijn wie met welke periodiciteit de actualiteit van de respectievelijke systemen dient te verifiëren en desgevallend actualisaties dient uit te voeren. Door verouderde software te blijven gebruiken en kritische beveiligingsupdates niet toe te passen, blijven gekende kwetsbaarheden bestaan waarvan misbruik kan worden gemaakt.

- De gebruikerstoestellen van medewerkers worden door de ICT-diensten bijgewerkt. Daarvoor zijn meestal specifieke tools aanwezig. Onder meer doordat de processen of instructies voor het actualiseren niet altijd beschreven zijn, is er een grote afhankelijkheid van de beschikbaarheid van de systeembeheerder om deze toestellen bij te werken;

- De actualisatie van servers en overige ICT-infrastructuur wordt voornamelijk uitbesteed aan externe partijen. De daarvoor gebruikte aanpak:
  - verloopt vanop afstand via specifieke beveiligde kanalen;
  - is vaak onvoldoende gestructureerd: de lokale besturen missen een referentiekader om de actualisatie door derden op te volgen en te kunnen inschatten of die voldoende tegemoet komt aan hun verwachtingen;

- De uitgevoerde aanval- en penetratietesten toonden aan dat het actualiseren van systemen in de praktijk niet altijd nauwgezet gebeurt. Door verouderde versies van een systeem te gebruiken en kritische beveiligingsupdates niet door te voeren, blijven gekende kwetsbaarheden bestaan waarvan personen met malafide bedoelingen misbruik kunnen maken.

Technische beschermingsmaatregelen

2020	1,2	0	83%	17%	0%	0%
2017 - 2018	1,2	11%	63%	26%	0%	0%

Technische beschermingsmaatregelen

Een goed technisch beheer is nodig om te vermijden dat zwaktes in de beveiliging de vertrouwelijkheid en de integriteit van gevoelige informatie kunnen ondermijnen. Om informatie veilig te houden, zowel in opslag als in transport, is versleuteling een belangrijke technische beschermingsmaatregel. Om erover te waken dat de organisatie versleuteling doeltreffend en correct inzet, evalueert ze voor welke gegevens versleuteling wenselijk is en houdt ze de ingezette versleutelingsalgoritmes actueel. Om de gevolgen van een besmetting van de ICT-omgeving te beperken, dient de organisatie ook maatregelen te nemen om te vermijden dat dergelijke besmetting zich ongemerkt en ongebreideld zou kunnen verderzetten doorheen het netwerk.

- Gevoelige informatie of informatiestromen kunnen worden afgeschermd door deze te versleutelen. Versleuteling van gegevens bij lokale besturen is:
  - geregeld gebaseerd op verouderde versleutelingsmechanismen en daardoor van weinig nut;
  - frequent aanwezig op externe communicatie (VPN, e-loket, e-mail,...);
  - meestal afwezig op draagbare toestellen en USB-sleutels;

- Het merendeel van de lokale besturen formuleerde geen beleid inzake versleuteling van gegevens (cryptografie). Als gevolg daarvan is er vaak geen structurele aanpak voor cryptografie binnen het lokaal bestuur.

- Om bij eventuele incidenten de impact te beperken, kan het nuttig zijn om beperkingen in te stellen op het verkeer tussen de verschillende delen van het netwerk. Het is courant dat één of andere vorm van opdeling is opgezet (netwerksegmentatie), maar slechts bij uitzondering zijn er beperkingen en/of monitoring opgezet voor de communicatie tussen deze netwerksegmenten (netwerksegregatie). Hierdoor zijn achterliggende systemen kwetsbaar voor infecties op eindgebruikersapparatuur en kan een ongeautoriseerde gebruiker die zichzelf toegang verschaft tot het interne netwerk meteen alle netwerk- en systeembeheerinterfaces aanvallen.

Toegangen en rechten

2020	1	0%	100%	0%	0%	0%
2017 - 2018	1,4	4%	52%	44%	0%	0%

Toegangen en rechten

Een degelijke toegangsbeveiliging is cruciaal om onrechtmatige toegang tot (gevoelige) informatie te voorkomen. Toegangs- en gebruikersrechten worden telkens best beperkt tot wat nodig is voor het normale functioneren van de gebruiker. Bij het toekennen van toegangen en rechten dient aandacht te worden besteed aan de vereiste functiescheiding of - waar niet mogelijk- aan de vereiste compenserende beheersmaatregelen (bv. actieve monitoring). Bij wijzigingen aan de functie is een evaluatie van de toegangen een vereiste.

- De lokale besturen hebben nog geen gedefinieerde aanpak voor de toekenning, wijziging en intrekking van toegangs- en gebruikersrechten. Verschillende besturen werken hier aan, maar deze aanpak staat nog niet geheel op punt.
- De organisaties voorzien wel via hun ICT-dienst technische beheersmaatregelen om de toegang tot het interne netwerk en de centrale ICT-omgeving te beperken en te beheren.
- Applicatiebeheerders kunnen ook rechten toekennen voor gebruikerstoepassingen. Vaak zijn deze beheerders niet formeel aangeduid en verloopt het toebedelen van toegangen eerder ad-hoc.
- Lokale besturen maken slechts sporadisch gebruik van multi-factor-authenticatie (MFA) en single sign-on (SSO). Deze technologieën zorgen voor goede beveiliging zonder in te boeten op gebruiksgemak.
- Om onrechtmatige toegang en misbruik van toegang tot gevoelige informatie te beperken, beschrijven lokale besturen het gebruik van authenticatie-informatie vaak in een summier wachtwoordbeleid. De uitgevoerde aanval- en penetratietesten tonen aan dat het wachtwoordbeleid in de praktijk niet voldoende wordt afgedwongen.

Continuïteit

2020	2	0%	33%	33%	33%	0%
2017 - 2018	2,2	0%	30%	19%	52%	0%

Continuïteit

De organisatie treft continuïteitsmaatregelen om de onbeschikbaarheid van (tijds)kritische diensten en van informatie door een uitval van ICT-systemen, huisvesting en/of logistieke ondersteuning te beperken en de werking te herstellen na een incident. Ook een ruimer continuïteitsplan met aandacht voor crisismanagement, logistiek en communicatie kan hierbij van belang zijn. Om te verzekeren dat de uitgewerkte maatregelen werken, test de organisatie ze periodiek en stuurt ze bij waar nodig.

- De ICT-diensten verzekeren de basiscontinuïteit op verschillende manieren:
  - ze zorgen ervoor dat back-ups beschikbaar zijn. Vaak zijn dit ook back-ups die offline opgeslagen worden;
  - zo goed als allemaal hebben ze ook geïnvesteerd in een noodstroomvoorziening. Zo zijn servers beschermd tegen een plotse stroomonderbreking;

In Wervik is een goede praktijk voor continuïteit vastgesteld

- Maar lokale besturen hebben te veel vertrouwen dat ze bij een calamiteit de activiteiten vlot zullen kunnen herstellen:
  - De back-ups of de toestellen waarop die worden opgeslagen, zijn soms niet beschermd tegen ransomware[1]. Ook het testen van back-ups is een activiteit die zelden uitgevoerd wordt. Lokale besturen gaan niet (frequent) na of het maken van back-ups succesvol verliep en of de gemaakte back-ups integer en dus effectief bruikbaar zijn.
  - Volwaardig continuïteitsbeheer is eerder een uitzondering: de prioritering van de te herstellen processen en systemen en vooral een ruimer bedrijfscontinuïteitsplan ontbreken vaak. Daardoor is er geen garantie dat in geval van onbeschikbaarheid van (tijds)kritische diensten en van informatie, efficiënt kan worden opgetreden en dat daarbij de werking binnen een redelijke termijn kan worden hersteld.

(1) Ransomware is kwaadwillige software (zogenaamde 'malware') die de gegevens op computers versleutelt (en dus onleesbaar maakt voor de gebruiker), waarna een boodschap verschijnt met de vraag losgeld te betalen.

IV. Verder aan de slag

Vlaamse overheid

AUDIT VLAANDEREN

Eerder al aan de slag

2017 -2018

- Thema-audit informatiebeveiliging bij 28 lokale besturen

2018 -2019

- De geauditeerde besturen gaan aan de slag met de geformuleerde aanbevelingen
- Voor de overige lokale besturen werd een uitgebreide sensibiliseringscampagne opgezet om de tijdens de thema-audit gedetecteerde aandachtspunten en goede praktijken kenbaar te maken teneinde ook hen toe te laten aan de slag te gaan

2019

- Opvolging van een steekproef van aanbevelingen uit de thema-audit informatiebeveiliging bij 28 lokale besturen

2020

- Thema-audit informatiebeveiliging 2020 bij 6 lokale besturen

Verder aan de slag

2020

- De Vlaamse Regering lanceerde initiatieven ter ondersteuning van cyberveilige gemeenten:
  - Aanbod voor ethische hacking (VVSG i.s.m. Howest) opgestart eind 2020;
  - Digitale toolbox cyberveiligheid (VVSG) in ontwikkeling tegen 2022;
  - Cofinanciering voor ICT-veiligheidsaudits (professionele auditfirma's met coördinatie van Audit Vlaanderen) 2020 – 2021 .
    - De technische testen werden al bij verschillende lokale besturen afgerond. De eerste resultaten bevestigen de resultaten uit deze thema-audit informatiebeveiliging. Met deze resultaten kunnen lokale besturen gericht kwetsbaarheden aanpakken.
    - De in het basisaanbod inbegrepen dag om samen met experten aan informatiebeveiliging te werken wordt door de betrokken besturen naar eigen wens ingevuld. Dat kan zowel gaan:
      - om acties op beleidsniveau - bijvoorbeeld het simuleren van het crisismanagement tijdens een incident of het brainstormen over beleidskeuzes m.b.t. digitalisering, architectuurkeuzes en/of investeringskeuzes;

2021

      - om acties op operationeel vlak - bijvoorbeeld het bijdragen aan de opzet van een bedrijfscontinuïteitsplan;
      - als om technische acties - bijvoorbeeld het bespreken van de aanpassingen om de vastgestelde open deuren te sluiten of het begeleiden van risicomanagementworkshops om ICT-risico's beter te identificeren en beheersen.
    - Bestellingen voor ICT-veiligheidsaudits met cofinanciering kunnen ook in 2021 nog worden geplaatst en uitgevoerd. Ook voor de cofinanciering van aanvullende ICT-veiligheidsaudits is nog ruim budget beschikbaar. Lokale besturen kun dus nog steeds contact opnemen met de betrokken leveranciers: contactgegevens.

2021

- Dit globaal rapport thema-audit informatiebeveiliging 2020 werd gepubliceerd op de website van Audit Vlaanderen.
- Verdere sensibilisering. Ook de gedetecteerde goede praktijken blijven beschikbaar op https://overheid.vlaanderen.be/goede-praktijken-leidraad-organisatiebeheersing.

2022

- Welke verdere initiatieven nodig zijn vanaf 2022, zal nog worden opgevolgd (zo behoort bijvoorbeeld een volgende reeks thema-audits informatiebeveiliging tot de mogelijkheden).

Aan de slag gaan heeft impact

I. **Aan de slag gaan, verbetert de informatiebeveiliging.**

Reeds in het kader van de voorbereiding van het globaal rapport in 2018 werden een aantal technische bevindingen bij de in 2017 en 2018 geauditeerde besturen opnieuw getest, in sommige gevallen al 4 maanden na de initiële test. De hoge risico's bleken in 53% van de gevallen al volledig geremedieerd en in 21% al deels geremedieerd.

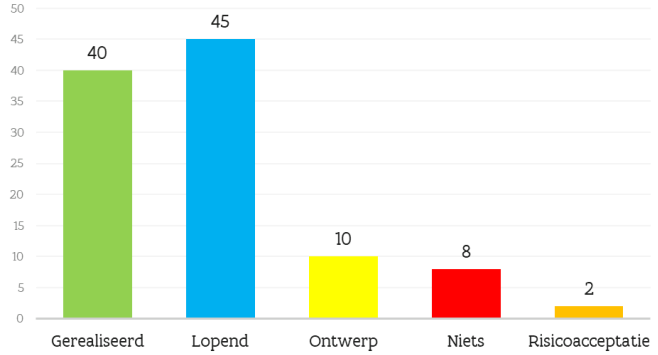
Daarnaast toonde de opvolging van de in 2017 en 2018 geformuleerde aanbevelingen m.b.t. informatiebeveiliging in 2019 aan dat de eerder geauditeerde lokale besturen effectief vooruitgang hadden geboekt op het domein van informatiebeveiliging.

Hoge veiligheidsrisico's	Volledig geremedieerd	Deels geremedieerd	Niet geremedieerd
Configuraties	20	2	6
Beveiligingsupdates	9	4	8
Wachtwoordbeleid	8	9	4
	37	15	18
	53%	**21%**	**26%**

II. **Aan de slag gaan met informatiebeveiliging, vergt een volgehouden inspanning.**

De opvolging van 105 geformuleerde aanbevelingen waarvan de streefdatum was gepasseerd, toonde in 2019 ook aan dat een aanzienlijk deel van de aanbevelingen nog niet gerealiseerd waren. Meer of bijkomende inspanningen waren nog verder nodig.

Statussen van 105 opgevolgde aanbevelingen in 2019



III. **Niet aan de slag gaan, laat grote risico's onvoldoende afgedekt.**

Tijdens de technische testen van deze thema-audit slaagde Audit Vlaanderen erin bij 5 van de 6 geauditeerde besturen volledige controle over het interne netwerk verwerven. De veiligheidsrisico's die lokale besturen lopen zijn reëel en groot.

Het aantal incidenten met een significante impact neemt ook bij lokale besturen toe. Het gaat daarbij zeker niet alleen om de besturen die hun ervaringen publiek delen om collega's te waarschuwen en te helpen voorbereiden.

Zelf aan de slag

Lokale besturen met een beter ontwikkelde organisatiebeheersing, beheersen de onderzochte risico's op het vlak van informatiebeveiliging in het algemeen beter. Werk maken van organisatiebeheersing loont dus ook hiervoor.

Reeds in het globaal rapport dat werd gepubliceerd in 2018 werd gewezen op een reeks haalbare beschermingsmaatregelen die vaak onderbenut blijven. Toch kan (beter) werk maken van deze maatregelen een echt verschil maken:

- Hanteer een **wachtwoordbeleid** voor alle systemen waar uw lokaal bestuur gebruik van maakt. En dwing waar mogelijk sterke wachtwoorden af, ook bij technische accounts.

  In een moderne omgeving wil een goed wachtwoordbeleid ook zeggen dat maximaal gebruik wordt gemaakt van multi-factor-authenticatie.

  Op de websites van de Vlaamse overheid en Safe on Web kan u terecht voor nuttige tips en tricks en bruikbaar sensibiliseringsmateriaal.

- Werk goede afspraken uit voor het beheren van alle **toegangen en rechten** bij indiensttreding, bij wijzigingen en bij uitdiensttreding. De veelheid van gebruikte systemen binnen én buiten de eigen ICT-omgeving maakt dat veelal meerdere (applicatie)verantwoordelijken betrokken zijn bij het in de praktijk brengen daarvan. Goede communicatie en transparante rapportering zijn daarbij dan ook belangrijk. Om geen zaken over het hoofd te zien, is ook een periodieke evaluatie aangewezen. Met de juiste rapportering hoeft dit voor leidinggevenden en/of inhoudelijk verantwoordelijken geen grote inspanning te vergen. Onder meer de praktijk van Haacht op de website met goede praktijken voor lokale besturen kan als inspiratiebron dienen.

- Zorg dat voor elk ICT-systeem duidelijk is wie met welke minimale frequentie instaat voor het **actueel houden** ervan. Vergeet daarbij ook ondersteunende systemen, services en configuraties niet. Naast transparante opvolging van de geleverde inspanningen kan ook een periodieke check aan de hand van een kwetsbaarheidsscan zekerheid bieden over de mate waarin de gewenste bescherming wordt gerealiseerd.

Zelf aan de slag

- Maak afspraken over **versleuteling**, zowel op de gebruikte apparatuur, tijdens transport als in opslag, in functie van de gevoeligheid en vertrouwelijkheid van de betrokken gegevens.
  Onder meer de praktijken van Wevelgem en Erpe-Mere op de website met goede praktijken voor lokale besturen kunnen als inspiratiebron dienen.

- Investeer – minstens bij de volgende vernieuwing van netwerkcomponenten – in een actieve opdeling van het netwerk met voldoende onderlinge monitoring en/of afscherming (**netwerksegregatie**) om bij een ransomware- of andere aanval de schade te kunnen beperken.

- **Volg gekende zwakke plekken** in de informatiebescherming goed op en investeer tijdig om kwetsbaarheden in niet langer ondersteunde apparatuur en/of systemen te vermijden.

- Werk een volwaardig **bedrijfscontinuïteitsplan** uit en investeer in wat nodig is om bij een incident de crisis goed te kunnen aanpakken en vlot tot herstel van de normale werking te komen met een aanvaardbaar verlies van gegevens en dienstverlening.
  Onder het stappenplan van de toolbox bedrijfscontinuïteitsmanagement en de praktijken van Wemmel, Lanaken en Erpe-Mere op de website met goede praktijken voor lokale besturen kunnen als inspiratiebron dienen.

Zelf aan de slag

Lokale besturen zitten aan het stuur om te bepalen hoe de beoogde ICT-ondersteuning én digitalisering in de praktijk wordt opgezet.
Botst uw lokaal bestuur daarbij tegen moeilijkheden of is het niet zeker hoe u specifieke elementen/risico's best aanpakt? Aarzel dan niet om voor de nodig kennis en competentie te zorgen, om waar mogelijk samen te werken én om uitgebreid hulp te zoeken bij belangenorganisaties en professionele – al dan niet gespecialiseerde – dienstverleners.

Nog heel 2021 helpt de Vlaamse overheid om de inzet van professionele auditfirma's door lokale besturen financieel haalbaarder te maken. Strategische en/of praktische begeleiding m.b.t. cybersecurity én beveiliging van vertrouwelijkheid, integriteit en beschikbaarheid van de dienstverlening zijn daarbij mogelijk naast de oplijsting van de mate waarin uw bestuur beschermd is tegen courante technische kwetsbaarheden. Uw bestuur moet daarvoor wel tot bestelling overgaan. Praktische informatie om daartoe over te gaan is te vinden hier.

Onder andere VVSG zorgt in 2021 en in 2022 voor kennisdeling en sensibilisering, aan de hand van online infosessies en een studiedag.
Houd de VVSG-nieuwsbrief in de gaten voor het laatste nieuws hierrond.

Ook worden vanuit verschillende organisaties en op verschillende manieren mogelijkheden geboden om samen te werken en kennis te delen, onder meer omtrent ICT, informatiebeveiliging en bescherming van persoonsgegevens. Onder meer sommige kennisdelingsmomenten georganiseerd door V-ICT-OR en sommige sessies voor functionarissen voor gegevensbescherming kunnen gratis worden bijgewoond.

Tenslotte werkt de VVSG in kader van het Project Cyberveilige Gemeenten aan een cyberveiligheidskaart die lokale besturen helpt om makkelijker de weg te vinden in het ruime commerciële aanbod. Dienstverleners zullen vrij kunnen toetreden tot dit overzicht en kunnen contact opnemen via cyberveiligheid@vvsg.be om op de hoogte te blijven van de ontwikkeling.

V. Bijlagen

Vlaamse overheid

AUDIT VLAANDEREN

Audit Vlaanderen

- Audit Vlaanderen is een onafhankelijke, objectieve en bekwame partner van de organisatie die helpt bij het beheersen van financiële, wettelijke en organisatorische risico's. Op die manier wilt Audit Vlaanderen samen met de organisatie toegevoegde waarde te creëren bij de uitbouw van een efficiënte, effectieve, integere en kwaliteitsvolle organisatie.

- Het agentschap Audit Vlaanderen heeft als opdracht het systeem van organisatiebeheersing van de lokale besturen en de Vlaamse administratie te evalueren. Die evaluatie doet Audit Vlaanderen door audits uit te voeren. Twee auditcomités sturen Audit Vlaanderen aan: een auditcomité van de lokale besturen en een auditcomité van de Vlaamse administratie. De auditcomités staan in voor de strategische keuzes van en het toezicht op het agentschap.

- Bijkomende informatie omtrent Audit Vlaanderen en haar activiteiten kan u terugvinden op www.auditvlaanderen.be.
  Hier kan u bijvoorbeeld de volgende informatie terugvinden:
  - Leidraad Organisatiebeheersing;
  - Globale rapporten;
  - Zelfevaluatie-instrumenten;
  - Nieuwsbrieven;
  - Publicaties, o.a. jaarverslag.

  Tot slot kan u ook kennis maken met Audit Vlaanderen en zien hoe audits in lokale besturen verlopen in het volgende filmpje: https://www.auditvlaanderen.be/samen-beter-werken.

Resultaten thema-audit Informatiebeveiliging (2017 -2018)

Meer informatie over de thema-audit Informatiebeveiliging (2017 -2018) is terug te vinden op:
https://www.auditvlaanderen.be/globaal-rapport-thema-audit-informatiebeveiliging

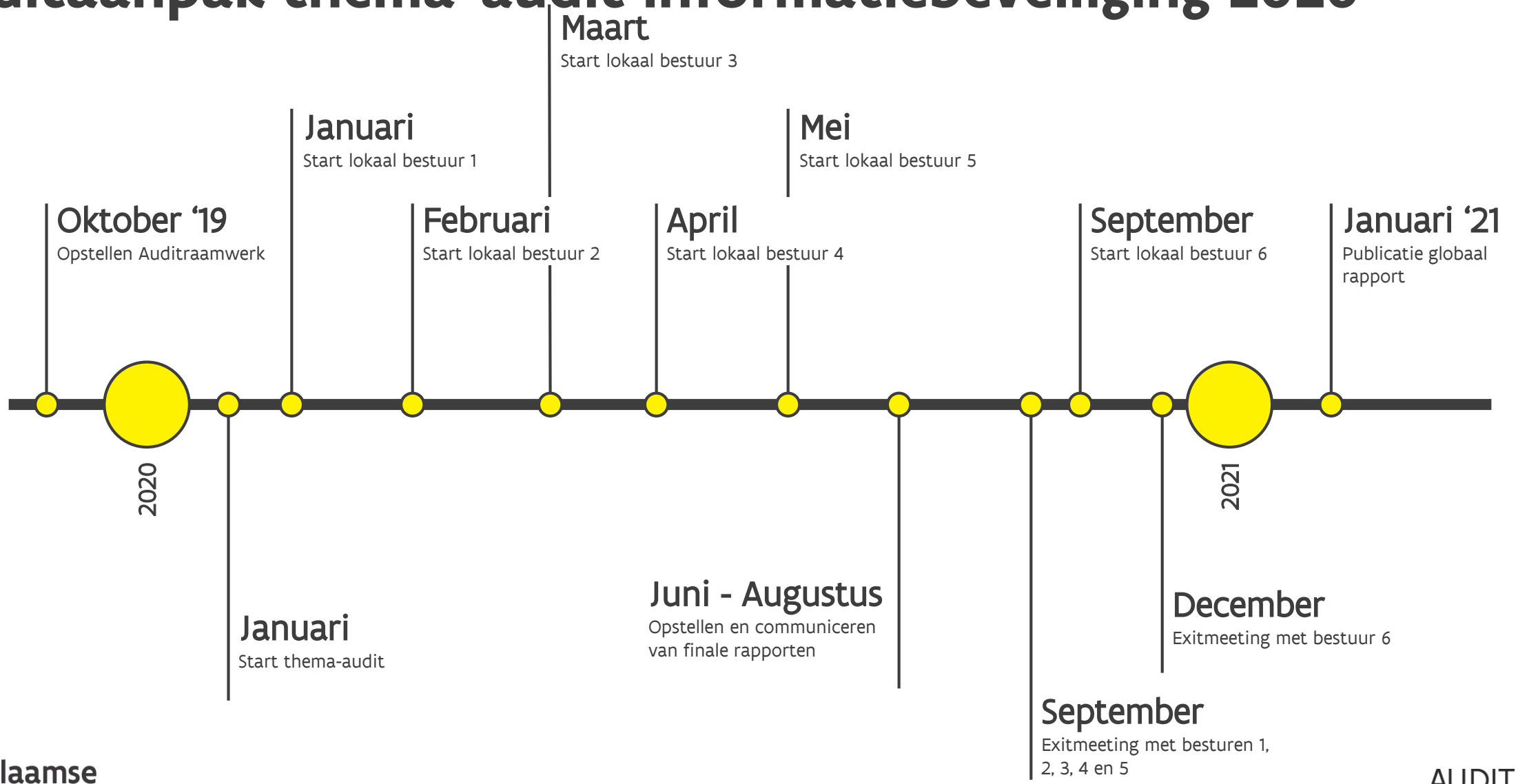
	+ 19.000 inwoners									aantal inwoners < 19.000 en > 12.000									< 12.000 inwoners									gemiddelde
Organisatiebeheersing	3	3	2	2	3	0	3	0	2	3	0	3	3	2	2	2	2	0	2	0	3	0	0	0	0	2	3	1,67
BELEID EN ORGANISATIE	**3**	**2**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**2**	**3**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**1**	**1**	**1,78**
informatiebeveiligingsbeleid	3	3	2	1	1	2	1	1	2	3	3	1	1	2	2	2	2	2	2	1	2	2	2	2	2	1	2	1,85
verantwoordelijkheden	3	3	2	1	2	2	2	1	2	3	3	2	2	2	2	2	1	2	2	2	1	2	1	3	2	1	1	1,93
leveranciersrelaties	2	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,07
naleving	3	2	2	2	2	1	2	1	1	1	4	3	3	1	1	1	1	2	2	2	2	1	1	1	2	1	1	1,70
BEWUSTZIJN	**2**	**2**	**2**	**1**	**2**	**1**	**1**	**1**	**1**	**3**	**3**	**3**	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**1**	**2**	**2**	**1,78**
veilig personeel	2	3	3	2	1	1	2	1	1	2	3	3	2	3	2	1	1	1	2	2	2	2	2	1	1	1	2	1,81
omgang met informatiedragers	3	2	2	1	2	2	1	2	1	3	3	3	1	2	1	1	1	2	1	3	2	2	1	1	1	2	2	1,78
TECHNISCH BEHEER	**2**	**2**	**2**	**2**	**1**	**1**	**2**	**1**	**1**	**2**	**1**	**1**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**1**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1,44**
cryptografie	3	2	2	1	1	1	2	1	1	1	1	1	2	0	1	1	2	0	1	1	1	1	1	1	1	1	0	1,15
fysieke beveiliging	2	2	3	3	2	2	nvt	2	1	3	3	2	3	2	2	2	2	2	2	2	3	2	1	2	1	3	1	2,04
beveiliging van de IT-omgeving	2	2	2	2	1	1	2	1	1	2	1	1	2	1	2	2	2	1	2	2	2	1	2	1	1	1	1	1,52
netwerkbeveiliging	2	2	2	2	2	2	2	1	1	2	1	1	2	1	2	1	2	1	2	2	2	2	1	2	1	2	1	1,63
ontwikkeling	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1,04
LOGISCH TOEGANGSBEHEER	**2**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**3**	**2**	**2**	**1**	**2**	**2**	**1**	**1**	**1**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1,56**
uitdiensttreding	1	2	2	2	2	1	1	1	0	3	2	3	1	2	3	1	1	1	2	2	1	2	1	1	0	2	1	1,52
beheer en classificatie	2	2	2	2	2	1	1	2	1	3	2	2	1	2	1	1	1	2	1	2	2	1	1	1	1	1	2	1,56
toegangsbeveiliging	2	1	2	2	2	2	1	1	2	2	3	2	1	2	1	2	1	1	3	2	2	2	2	1	1	1	1	1,67
CONTINUÏTEIT	**2**	**3**	**3**	**3**	**3**	**3**	**2**	**3**	**2**	**3**	**1**	**3**	**3**	**3**	**3**	**3**	**2**	**1**	**3**	**1**	**1**	**1**	**2**	**1**	**3**	**1**	**1**	**2,22**
INCIDENTENBEHEER	**3**	**1**	**1**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**1**	**1**	**1**	**2**	**1**	**1**	**1,26**
gemiddelde maturiteit informatiebeveiliging	2,25	2,00	2,00	1,75	1,69	1,50	1,47	1,31	1,19	2,19	2,06	1,94	1,75	1,63	1,63	1,44	1,38	1,31	1,75	1,69	1,69	1,50	1,31	1,31	1,31	1,31	1,19	1,61
	1,68									1,70									1,45									

Auditaanpak thema-audit informatiebeveiliging 2020

- Om na te gaan in welke mate lokale besturen deze risico's beheersen, stelde Audit Vlaanderen een controleprogramma op. Dit is een kader specifieke beheersdoelstellingen, risico's en mogelijke beheersmaatregelen rond informatiebeveiliging. Audit Vlaanderen gaat ook na of er een globaal kader voor organisatiebeheersing is vastgelegd en of hierover gerapporteerd wordt.

- Elke opdracht binnen deze thema-audit doorloopt de volgende stappen:
  - Inzicht krijgen in de informatiebeveiligingsrisico's en de daarbij horende beheersmaatregelen via:
    - documentenstudie;
    - interviews.
  - De toepassing van de beheersmaatregelen in de praktijk onderzoeken via:
    - testen;
    - interviews.
- Tijdens het terreinwerk worden in overleg met het bestuur onder andere een aantal technische veiligheidstesten uitgevoerd. Deze testen zijn niet exhaustief en garanderen niet dat alle mogelijke kwetsbaarheden worden gedetecteerd.
- Tijdens de audit beoordeelt Audit Vlaanderen of de risico's, die in het kader van deze audit worden onderzocht, zijn afgedekt door de aanwezige beheersmaatregelen.
- Indien dit niet het geval is, formuleren de auditoren een of meerdere aanbevelingen met het oog op de verbetering van deze risicoafdekking.

Auditaanpak thema-audit informatiebeveiliging 2020



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