Thema-audit Beheer van ICT-risico's bij lokale besturen

Inspiratierapport

13.06.2023

Vlaamse overheid

AUDIT VLAANDEREN

AUDIT
VLAANDEREN

INHOUDSOPGAVE

AUDIT
VLAANDEREN

1 INLEIDING

Dit inspiratierapport biedt lokale besturen meer achtergrondinformatie bij de thema-audit Beheer van ICT-risico's en mogelijkheden om met de conclusies van deze audit aan de slag te gaan.

De samenvatting van de conclusies van deze thema-audit is terug te vinden in het Globaal rapport "Thema-audit Beheer van ICT-risico's bij lokale besturen".

Dit inspiratierapport bevat volgende gedetailleerde informatie als bijlage:
- een beschrijving van de selectie van besturen die deelnamen aan de bevraging in het kader van deze thema-audit;
- analyse van de bestaffing van de ICT-functie in de bevraagde lokale besturen;
- de vragenlijst van de online bevraging, beantwoord in de periode november 2021 - januari 2022 door 144 lokale besturen;
- analyse van de antwoorden op de vragenlijst;
- lijst van bevraagde lokale besturen per provincie.

Auditteam:
- Zoë Akkermans, auditor (Deloitte), auditor (Deloitte)
- Jeff Vandebeeck, auditor (Deloitte), auditor (Deloitte)
- Aurélie Vens, senior auditor (Deloitte), senior auditor (Deloitte)
- Julie Van der Planken, manager-auditor (Deloitte), manager-auditor (Deloitte)
- Inge Cools, auditor, auditor
- Lydia Putseys, auditor
- Gunter Schryvers, manager-auditor

2 BOUWSTENEN

Op basis van de resultaten van de online bevraging en de diepte-interviews kan het lokaal bestuur de eigen antwoorden op de online bevraging toetsen. Het lokaal bestuur kan zelf nagaan in hoeverre de antwoorden op de bevraging aangeven dat het lokaal bestuur in de betreffende risicodomeinen eerder zwak blijkt te scoren. Een onvoldoende beheerst risico kan de goede werking van de organisatie en ook de dienstverlening in het gedrang brengen. Het is dan ook belangrijk om een set van beheersmaatregelen te ontwikkelen. De bouwstenen uit dit rapport kunnen hiervoor een inspiratiebron bieden.

Risicobeheer is maatwerk. Het moet geënt zijn op de geïdentificeerde risico's voor het lokaal bestuur in kwestie. Deze specifieke risico's zullen veelal afhankelijk zijn van de manier waarop de ICT-functie binnen het bestuur werd uitgebouwd en de keuzes die men heeft gemaakt om ICT-expertise al dan niet zelf uit te bouwen of via samenwerkingsverbanden of via externe invulling van de ICT-functie te verwerven. De beheersmaatregelen kunnen dan ook verschillend zijn naargelang de situatie. Een bestuur dat bijvoorbeeld zelf instaat voor een eigen datacenter heeft andere beheersmaatregelen nodig dan een bestuur dat alle data heeft ondergebracht in de cloud. Voor beide types van besturen geldt dat informatieveiligheid belangrijk is maar de aanpak zal verschillen per bestuur.

In dit hoofdstuk worden generieke bouwstenen gegeven die gelden voor elk lokaal bestuur. Deze bouwstenen focussen op de **"wat"**-vraag: wat moet er geïmplementeerd worden om te komen tot een gedegen risicobeheer. In het volgende hoofdstuk wordt toegelicht **hoe** elk type van bestuur (afhankelijk van de uitgangssituatie en het samenwerkingsmodel) werk kan maken van deze bouwstenen.

De bouwstenen hebben betrekking op:
1. Het ontwikkelen van een ICT-visie/-strategie voor het lokaal bestuur;
2. Het opstellen van een risicoanalyse voor het lokaal bestuur;
3. Het implementeren van adequate beheersmaatregelen;
4. Het op punt zetten van de ICT-governance binnen het lokaal bestuur;
5. De coördinatie organiseren tussen de interne ICT-functie enerzijds en de externe ICT-ondersteuning en externe leveranciers anderzijds.

Wat is ICT-governance?
Een ruime definitie van ICT-governance is: het systeem waarbinnen de ICT van een organisatie wordt (aan)gestuurd en beheerst. Het gaat daarbij dan onder meer om de verdeling van taken, bevoegdheden en verantwoordelijkheden met betrekking tot ICT-aspecten over de diverse belanghebbenden binnen de organisatie. Voor een lokaal bestuur zijn de belangrijkste stakeholders op dit vlak : de algemeen directeur, het managementteam, ICT-verantwoordelijke (en zijn/haar leidinggevende), de functionaris voor gegevensbescherming, medewerker organisatiebeheersing. De samenwerking die men opzet met externen (voor ICT-ondersteuning of met leveranciers) is eveneens een aspect van ICT-governance.

AUDIT
VLAANDEREN

Bouwsteen 1: ICT-visie/-strategie van het lokaal bestuur

Het lokaal bestuur stelt een duidelijke interne ICT-visie/strategie op die een leidraad is voor de ICT-inrichting van de organisatie en aansluit op de strategie/-visie en de doelstellingen van het meerjarenplan van het lokaal bestuur.

Deze ICT-visie/strategie voldoet minstens aan volgende voorwaarden:
- ze is voldoende concreet zodat ze een houvast biedt voor concrete acties;
- ze houdt rekening met het dienstverleningsconcept en de informatienoden van de gebruikers;
- ze houdt rekening met digitalisering van processen en technologische evoluties;
- ze kwam tot stand via een ruimere consultatie van het management, het beleid en eventuele sleutelgebruikers van bepaalde toepassingen;
- ze is gedocumenteerd;
- ze is gevalideerd door het management van de organisatie;
- ze wordt regelmatig geactualiseerd;
- ze wordt ook gecommuniceerd naar alle betrokken stakeholders.

Risico dat hiermee kan worden beheerst:
- Het lokaal bestuur slaagt er niet in haar doelstellingen te realiseren omdat ze geen duidelijk ICT-visie/strategie heeft en hierdoor niet de juiste keuzes maakt, inefficiënte investeringen in ICT doet en keuzes maakt voor niet-robuuste en/of incompatibele ICT-toepassingen.

De manier waarmee het lokaal bestuur aan de slag kan gaan met deze bouwsteen zal afhangen van het type en de reeds beschikbare ICT-visie/-strategie. Een concrete aanpak is per type opgenomen in het volgende hoofdstuk.

Bouwsteen 2: Risicoanalyse

Het lokaal bestuur stelt een risicoanalyse op op maat van het lokaal bestuur waarbij zowel rekening gehouden wordt met interne en externe risico's die een impact kunnen hebben op de realisatie van de organisatie- en, in het bijzonder, de ICT-doelstellingen.

Deze risicoanalyse houdt naast de informatieveiligheid ook rekening met:
- continuïteit van de dienstverlening;
- aansturing en monitoring van externen als continu proces:
  - leveranciers van soft- en hardware met onderhoudscontracten en SLA's;
  - externe ICT-ondersteuning.

Risico's die hiermee kunnen worden beheerst:
- Het lokaal bestuur heeft geen of onvoldoende zicht op alle ICT-risico's die in de organisatie aanwezig zijn en kan hierdoor onvoldoende beheersmaatregelen implementeren om deze risico's te beheersen.
- Het lokaal bestuur heeft geen of onvoldoende zicht op de ICT-risico's bij aanpassing of vernieuwing aan het hard- en software gebeuren of wanneer het beheer ervan wordt overgedragen aan externen (risicotransfer), waardoor geen of onvoldoende beheersmaatregelen geïmplementeerd worden.
- Het lokaal bestuur heeft geen of onvoldoende zicht op de ICT-risico's gekoppeld aan de wijze waarop de ICT-functie (intern en of extern) ingevuld worden, waardoor ze onvoldoende beheersmaatregelen kan implementeren.

Vaak vertrekt een risicoanalyse vanuit de kennis over de huidige ICT-werking bij het lokaal bestuur en gekende incidenten of zwakheden. Dat is logisch omdat dit de meest betrouwbare en effectieve informatie is die voorhanden is. Het is evenwel belangrijk dat ICT-risicoanalyses vanuit een veel bredere kijk op de organisatie en de dienstverlening worden benaderd en ook rekening houden met externe, potentiële gebeurtenissen die zich tot nu toe niet hebben voorgedaan.

In de praktijk kan de risicoanalyse die gemaakt werd door de DPO vanuit een bezorgdheid voor informatieveiligheid breder getrokken worden en neemt het ook bedreigingen rond cyberveiligheid, netwerksegregatie en het gedrag van gebruikers op. Een gedegen ICT-risicoanalyse kijkt nog breder naar bijvoorbeeld het operationeel houden van kritieke dienstverlening en applicaties onder stresssituaties zoals overstromingen, black-out van energiesystemen enz. Ook de heropstart na een incident (ook als daar geen datalek of vrijgave van informatie mee gepaard ging) is van belang.

Als inspiratie voor de opmaak van een uitgebreide risicoanalyse bevat bijlage 6 een niet-limitatieve lijst van mogelijke risico's die kunnen geïdentificeerd worden bij een lokaal bestuur.

AUDIT
VLAANDEREN

Bouwsteen 3: Interne beheersmaatregelen

Het lokaal bestuur ontwikkelt interne risicobeheersmaatregelen. Deze maatregelen hebben betrekking op het vrijwaren van de veilige toegang tot informatie en de ondersteuning van de continuïteit van de dienstverlening. Volgende vragen zijn hierbij aan de orde:

- Hoe zijn we zeker dat we risico's, die zich manifesteren tijdig detecteren?
- Welke risico's accepteren we en welke niet?
- Wat zijn bijvoorbeeld vereisten voor de continuïteit van de dienstverlening in de verschillende geledingen van de organisatie?
- Welke preventieve maatregelen zijn in dit kader adequaat?
- Wie doet wat als er zich toch een incident voordoet? Wat zijn prioritaire gebieden om bijvoorbeeld weer op te starten?

Risico's die hiermee kunnen worden beheerst:

- Het lokaal bestuur heeft onvoldoende zicht op de ICT-risico's gekoppeld aan het intern beheer waardoor ze voor de bestaande beheersmaatregelen niet kan beoordelen of deze adequaat zijn.
- Het lokaal bestuur heeft onvoldoende zicht op de ICT-risico's gekoppeld aan het intern beheer waardoor ze de continuïteit van de ICT-dienstverlening aan de gebruikers niet kan verzekeren.
- Risico's en acties om deze risico's te beheersen worden niet of onvoldoende aangepakt omdat er geen duidelijke risico-eigenaar en actie-eigenaar is aangeduid.

Een lokaal bestuur waar de ICT-functie geheel of gedeeltelijk instaat voor de interne ICT-ondersteuning zal de nodige beheersmaatregelen moeten implementeren om de hieraan verbonden risico's te beperken. Het betreft niet alleen de technische aspecten van de ICT-ondersteuning, maar ook de continuïteit van de dienstverlening is hierbij een belangrijk aandachtspunt.

AUDIT
VLAANDEREN

Bouwsteen 4: De ICT-Governancestructuur

Het lokaal bestuur zet een governancestructuur op waarin projectbeheer, planning, processen, rollen en verantwoordelijkheden met betrekking tot ICT uitgewerkt worden zodat de interne werking binnen het lokaal bestuur vlot en gestructureerd kan verlopen.

Dit houdt onder meer in dat:

- een nauwe afstemming en goede relatie tussen de ICT-functie (intern of extern) en het managementteam structureel voorzien wordt zodat een wederzijdse informatie-uitwisseling en duidelijk beslissingslijn de werking ondersteunt de risico's omtrent ICT-governance dienen geïdentificeerd te worden en adequate beheersmaatregelen dienen uitgewerkt, opgevolgd en gecommuniceerd te worden;
- processen en planning dienen gedocumenteerd, geactualiseerd en regelmatig gecommuniceerd te worden;
- een structuur voor communicatie en het maken van afspraken dient opgezet en gedocumenteerd te worden. Voor digitaliseringsprojecten worden stuurgroepen voorzien die zowel de technische uitrol als het veranderingsbeheer bij gebruikers opvolgen.

Risico's die hiermee kunnen worden beheerst:

- Beslissingen voor ICT worden op een inefficiënte manier genomen binnen de organisatie;
- Er worden verkeerde keuzes voor de verdere ontwikkeling van het ICT-gebeuren;
- De informatie-uitwisseling tussen betrokkenen is onvoldoende waardoor het ICT-beheer niet adequaat of inefficiënt verloopt.

Bouwsteen 5: Coördinatie tussen de interne ICT-functie en de externe ICT-ondersteuning en externe leveranciers

De bevraagde besturen geven aan dat ze veel gebruik maken van externen. Ze insourcen ICT-competenties die binnen het bestuur ontbreken, ze kopen licenties aan voor softwaretoepassingen, outsourcen het databeheer aan een extern datacenter, … Dit gebeurt vaak zonder dat er vooraf duidelijkheid is over de inherente risico's en de risicotransfers die men door outsourcing voor ogen heeft en/of effectief in de praktijk realiseert. Een gemiddeld lokaal bestuur geeft aan minstens 10 tot vaak meer dan 20 leveranciers te hebben voor ICT-beheer. Het is dus ook belangrijk dat er duidelijke rollen en verantwoordelijkheden worden toegekend aan alle betrokken partijen en dat de verschillende leveranciers ook daadwerkelijk samenwerken (aan de ICT-visie en -strategie van het lokaal bestuur).

Het lokaal bestuur ontwikkelt een adequate coördinatie tussen de interne ICT-functie en de externe ICT-ondersteuning en externe leveranciers. Het eigenaarschap voor elk geïdentificeerd risico en bijhorende acties wordt expliciet toegekend en er wordt ook expliciet eigenaarschap toegekend van risico's zodat duidelijk is:

- wie is risico-eigenaar van een bepaald risico;
- wie is verantwoordelijk voor de uitwerking van een bepaalde beheersmaatregel of actie om het risico onder controle te brengen (actie-eigenaar).

Het lokaal bestuur ziet er hierbij op toe dat de toewijzing van rollen en verantwoordelijkheden sluitend is zodat dat er geen risico's of acties onbeheerd blijven.

Een adequate coördinatie kan gerealiseerd worden door:

- Afhankelijk van de ondersteuning die de externe partner levert (enkel onderhoudscontract of ruimer ICT-beheer, externe partij/medewerkers die ICT-functie opnemen) samen met de externe partner de risico's/risicodomeinen in kaart brengen waaraan het lokaal bestuur is blootgesteld en waarin de externe partner geheel of gedeeltelijk verantwoordelijk is voor het nemen van risicobeheersmaatregelen.
- De risicobeheersmaatregelen dienen gedefinieerd en opgevolgd te worden met de externe partij en regels en afspraken dienen gemaakt te worden voor het navolgen van deze beheersmaatregelen door de derde partij in de vorm van contractbeheer of SLA's.
- Aansluitend hierop, is het ook van belang dat lokale besturen hun ICT-landschap in kaart brengen en documenteren zodat externe partijen een duidelijk beeld hebben van de reeds bestaande IT-architectuur en de toekomstige noden. Deze documentatie dient steeds geactualiseerd en gedeeld te worden met de externe partner indien er wijzigingen hebben plaatsgevonden.
- Duidelijk af te bakenen welke partij eigenaar is van welke data en er een inventaris is van alle contracten, licenties voor toepassingen die het bestuur gebruikt met hun vervaldatum;
- Afspraken maken voor databeheer, digitaliseringsprojecten, veiligheid, continuïteit, veranderingsaanpak, kwaliteit en relatiebeheer van de externe partner(s) of externe leveranciers.

Risico's die hiermee kunnen worden beheerst:
- Het lokaal bestuur heeft geen of weinig zicht hoe de externen de ICT-functie invullen en kan onvoldoende adequaat reageren bij problemen.
- Bepaalde verantwoordelijkheden werden niet duidelijk toegewezen waardoor de opvolging van de werkzaamheden bemoeilijkt wordt en er niemand verantwoordelijk is voor de opvolging van een bepaald risico of een bepaalde actie.

In de praktijk ontstaan er vaak specifieke situaties die aandacht vergen op het vlak van governance en risico-verdeling. Bijvoorbeeld:

- Lokaal bestuur A geeft de opdracht aan firma B om in te staan voor het beheer van de applicatieservers. Firma B doet beroep op een extern datacenter bij firma C. Firma C heeft op haar beurt een contract met firma D voor de security van het datacenter.
- Lokaal bestuur A doet beroep op zelfstandige B voor het netwerkbeheer. Daarnaast worden de servers en applicaties beheert door firma C. Zelfstandige B denkt dat firma C instaat voor patchmanagement, terwijl firma C denkt dat B dit doet.
- Lokaal bestuur A heeft geen eigen helpdesk maar doet beroep op de diensten van externe helpdeskprovider B. Deze helpdeskprovider kan vanop afstand de schermen van medewerkers van het bestuur overnemen en heeft ook administratorrechten om bepaalde ingrepen in de systemen te kunnen doen. Helpdeskprovider B doet op zijn beurt beroep op firma C voor netwerkbeheer en -security van de helpdesk.
- Lokaal bestuur A heeft een applicatie bij firma Y aangekocht. Die applicatie moet gekoppeld worden met een andere applicatie van firma Z.

3 AAN DE SLAG MET DE BOUWSTENEN

De manier waarop de bouwstenen uitgewerkt kunnen worden in de praktijk is afhankelijk van:

- de startpositie van het lokaal bestuur;
- de keuzes die gemaakt werden over de positie van de ICT-functie in de organisatie;
- het feit of de organisatie een eigen datacenter beheert en
- de samenwerking met externe leveranciers.

Op basis van de auditbevindingen[1] kunnen vijf types van lokale besturen onderscheiden worden. Elk type is zoveel mogelijk duidelijk afgelijnd en gebaseerd op de lokale besturen die deel uitmaken van deze thema-audit. Voor de duidelijkheid is het aantal types beperkt tot vijf. Een aantal lokale besturen zal zich wellicht herkennen in meerdere types. Voor deze besturen is het raadzaam om de ICT-risico's en de bijhorende bouwstenen voor alle types waarin ze zich herkennen te bekijken. Lokale besturen kunnen hieruit inzichten halen voor het afdekken en beheren van hun ICT-risico's. De beschrijvingen van de vijf types lokale besturen worden hieronder opgelijst:

TYPE 1	De ICT-functie in ons lokaal bestuur is een uitvoerende functie die zorgt dat alle computers werken en die ook het netwerk en de servers beheert. Onze ICT-functie is niet actief betrokken bij digitaliseringsprojecten. De medewerkers die de ICT-functie uitvoeren, hebben vooral veel technische ICT-expertise.
TYPE 2	Ons lokaal bestuur heeft geen ICT-functie. Voor het installeren en het beheren van de computers, het netwerk en de servers doen we beroep op externen. Ook voor digitalisering van de processen zijn we afhankelijk van externen. Er is weinig coördinatie van de werkzaamheden die de externen uitvoeren.
TYPE 3	Onze ICT-functie werkt projectmatig en trekt ook onze digitaliseringsprojecten. De ICT-functie speelt een centrale rol bij de verdere uitbouw van de digitalisering. Daarnaast zorgt de ICT-functie er ook voor dat alle computers werken en de ICT-functie beheert het netwerk en de servers. Binnen de ICT-functie combineren we dus technische ICT-kennis met expertise op het vlak van digitalisering door de inzet van onze eigen medewerkers eventueel in samenwerking met externen.
TYPE 4	Onze ICT-functie doet van alles, meestal achter de schermen. Vooral de dagdagelijkse noden en vragen geven sturing aan wat de ICT-functie doet of niet doet. Er is geen duidelijke voorafgaande planning en er wordt ook weinig projectmatig gewerkt aan digitaliseringsprojecten. In de ICT-functie is er wel technische ICT-kennis aanwezig, maar voor digitaliseringsprojecten doen we beroep op externen of zal een andere interne dienst de trekkersrol opnemen.
TYPE 5	Ons lokaal bestuur heeft er bewust voor gekozen om alle uitvoerende taken (helpdesk, onderhoud computers en netwerk- en serverbeheer) uit te besteden aan externen. Occasioneel zal onze ICT-functie nog wel een (beperkte) helpdeskfunctie opnemen. Voor digitaliseringsprojecten doen we vooral een beroep op externe projectleiders. De ICT-functie zorgt als een regisseur dat alle taken en projecten door de externen volgens de afspraken worden uitgevoerd en neemt dus vooral een coördinerende rol op.

[1] De belangrijkste auditbevindingen zijn terug te vinden in het Globaal rapport "Thema-audit Beheer van ICT-risico's bij lokale besturen". Aanvullend hierbij bevatten bijlagen 2, 3 en 4 van dit inspiratierapport de analyse van de zelfevaluatie die de 144 lokale besturen invulden in de periode november 2021-januari 2022.

Voor elk van de 5 types lokale besturen zijn er specifieke aandachtspunten voor het ICT-risicobeheer door de keuzes die deze lokale besturen maakten voor het invullen van de ICT-functie en de taken die de interne ICT-functie opneemt.

Er kan een onderscheid worden gemaakt tussen 5 benaderingen of types. Uiteraard kan een lokaal bestuur ook kenmerken vertonen van meerdere types. We laten het aan het lokaal bestuur zelf over om na te gaan in welk type zij zich het meest herkennen.

TYPE 1

De ICT-functie in ons lokaal bestuur is een uitvoerende functie die zorgt dat alle computers werken en die ook het netwerk en de servers beheert. Onze ICT-functie is niet actief betrokken bij digitaliseringsprojecten. De medewerkers die de ICT-functie uitvoeren, hebben vooral veel technische ICT-expertise.

Aan de slag met:

Bouwsteen 1: ICT-visie/-strategie van het lokaal bestuur

1. Breng de gebruikersnoden in kaart.
2. Overleg met het managementteam over de ambities met betrekking tot digitalisering van de dienstverlening en de interne processen.
3. Spreek af met de stakeholders wat van de ICT-functie verwacht wordt.
4. Kom samen tot een prioritering van de acties die genomen moeten worden op het vlak van ICT.

Bouwsteen 2: Risicoanalyse

1. Documenteer samen met het management en sleutelgebruikers alle risico's en zorg dat er een procedure uitgewerkt wordt om dit overzicht actueel te houden.
2. Besteed bijzondere aandacht aan:
    - toegang tot en fysieke beveiliging van infrastructuur;
    - back-ups moeten in orde zijn;
    - patchmanagement;
    - netwerksegregatie en -segmentatie;
    - documentatie van de architectuur en een overzicht van het applicatielandschap.
3. Besteed bijzondere aandacht aan de manier waarop u zicht krijgt op de risico's die zich voordoen langs de gebruikerskant (door toegang tot informatie via laptops en mobiele toestellen).

Bouwsteen 3: Interne beheersmaatregelen

Ga hierbij stapsgewijs te werk:

1. Stel een risicoanalyse op waarbij de ICT-risico's gerelateerd aan het intern beheer geïdentificeerd worden. Ga na of de bestaande beheersmaatregelen voldoende de ICT-risico's voor het intern beheer afdekken (kloofanalyse). De antwoorden die uw lokaal bestuur gaf op de risicomaturiteit zijn een goede start voor een dergelijke risicoanalyse. Stel deze risicoanalyse op in overleg met vertegenwoordigers van de ICT-functie en de ruimere organisatie (bv. managementteam, leidinggevende, sleutelfiguren voor bepaalde toepassingen).
   OF
   Check of de bestaande risicoanalyse een breed gamma aan interne en externe risico's dekt en dat deze lijst met risico's voldoende actueel is. Breng een strategische dialoog met het management op gang waardoor vanuit het perspectief van kernprocessen en het dienstverleningsconcept van de organisatie wordt nagedacht over de risico's.
2. Vervolgens dienen de mogelijke oorzaken geïdentificeerd te worden samen met de mogelijke impact en waarschijnlijkheid van de ICT-risico's. Dit naast het bepalen, het implementeren en het testen van de mitigerende acties zodoende ICT-continuïteit te verzekeren. Leg de risico-eigenaar(s) en de actie-eigenaar(s) vast.

3. Deze risicoanalyse dient periodiek geactualiseerd, aangepast, getest en gecommuniceerd te worden bij wijzigingen binnen de organisatie.

Bouwsteen 4: Governancestructuur

1. Breng in kaart welke hard- en software het lokaal bestuur gebruikt.
2. Ga vervolgens voor elke hardware en elk softwarepakket na welke externe partner leverancier is en lijst de bijhorende contracten, licenties, onderhoudscontracten en of SLA's op, evenals hun vervaldatum.
3. Ga per hardware en per softwarepakket na welke externe partner(s) betrokken is (zijn) bij het beheer, de security en het onderhoud al dan niet in onderaanneming van de leverancier.
4. Maak afspraken met de betrokken externe partner over het intern beheer, digitaliseringsprojecten, veiligheid, continuïteit, veranderingsaanpak, kwaliteit en relatiebeheer van de externe partner(s) of externe leveranciers;
5. Documenteer en actualiseer de processen en planning en communiceer hierover met alle relevante betrokkenen.
6. Bepaal duidelijke communicatielijnen en structureer het maken van afspraken. Documenteer dit.

Bouwsteen 5: Coördinatie tussen de interne ICT-functie en externe leveranciers

1. Bepaal wie binnen het lokaal bestuur de coördinatie zal opnemen tussen de interne medewerkers en de externe partners.
2. Bespreek zowel met de interne medewerkers als met de externe partners de ICT-visie/-strategie van het lokaal bestuur en de resultaten van de risicoanalyse.
3. Bepaal welke verwachtingen er zijn ten aanzien van degene die de verantwoordelijkheid voor een risico of een beheersmaatregel opneemt.
4. Bepaal per risico en bijhorende beheersmaatregel(en) of de verantwoordelijkheid voor de opvolging en uitvoering intern of extern ligt.
5. Bepaal per risico en bijhorende beheersmaatregel(en) wie effectief de verantwoordelijkheid voor de opvolging en uitvoering opneemt.
6. Documenteer deze afspraken.

AUDIT
VLAANDEREN

TYPE 2

Ons lokaal bestuur heeft geen ICT-functie. Voor het installeren en het beheren van de computers, het netwerk en de servers doen we beroep op externen. Ook voor digitalisering van de processen zijn we afhankelijk van externen. Er is weinig coördinatie van de werkzaamheden die de externen uitvoeren.

Aan de slag met:

Bouwsteen 1: ICT-visie/-strategie van het lokaal bestuur:

1. Ga in dialoog met de externen die ICT-ondersteuning bieden: bevraag de huidige toestand en belangrijke evoluties die van belang zijn voor het bestuur, maak een kloofanalyse, breng in kaart welke noden er concreet zijn en wie het bestuur kan helpen bij toekomstige ontwikkelingen (bvb intergemeentelijk samenwerkingsverband, kenniscentrum, een ander bestuur privé onderneming, ...).
2. Ga in dialoog met andere lokale besturen en bekijk hoe zij de ICT-functie invullen en hun ICT-visie/strategie vormgeven.
3. Vertaal dit naar de eigen situatie in uw lokaal bestuur en lijst alternatieve toekomstscenario's op.
4. Betrek het managementteam bij het maken van keuzes en het uitwerken van een eigen ICT-visie/strategie.

Bouwsteen 2: Risicoanalyse

1. Iemand anders dan de externe ICT-ondersteuning (bv. DPO of medewerker organisatiebeheersing) coördineert de opmaak van de risicoanalyse
2. Hij/zij werkt hiervoor intensief samen met managementteam, de externe ICT-ondersteuning en de gebruikers om een integrale risicoanalyse op te stellen

Bouwsteen 3: Interne beheersmaatregelen

Ga hierbij stapsgewijs te werk:

1. Stel een risicoanalyse op waarbij de ICT-risico's gerelateerd aan het intern beheer geïdentificeerd worden en de bestaande beheersmaatregelen. Ga na of de bestaande beheersmaatregelen voldoende de ICT-risico's voor het intern beheer afdekken (kloofanalyse. De antwoorden die uw lokaal bestuur gaf op de risicomaturiteit zijn een goede start voor een dergelijke risicoanalyse. Stel deze risicoanalyse op in overleg met vertegenwoordigers van de ICT-functie en de ruimere organisatie (bv. managementteam, sleutelgebruikers van bepaalde toepassingen).
   OF
   Check of de bestaande risicoanalyse een breed gamma aan interne en externe risico's dekt en dat deze lijst met risico's voldoende actueel is. Breng een strategische dialoog met het management op gang waardoor vanuit het perspectief van kernprocessen en het dienstverleningsconcept van de organisatie wordt nagedacht over de risico's.
2. Vervolgens dienen de mogelijke oorzaken geïdentificeerd te worden samen met de mogelijke impact en waarschijnlijkheid van de ICT-risico's. Dit naast het bepalen, het implementeren en het testen van de mitigerende acties zodoende ICT-continuïteit te verzekeren. Leg de risico-eigenaar(s) en de actie-eigenaar(s) vast.
3. Deze risicoanalyse dient periodiek geactualiseerd, aangepast, getest en gecommuniceerd te worden bij wijzigingen binnen de organisatie.

Bouwsteen 4: Governancestructuur
De interne coördinator en de externe ICT-ondersteuning werken samen om de governancestructuur op te zetten.

1. Breng in kaart welke hard- en software het lokaal bestuur gebruikt.
2. Ga vervolgens voor elke hardware en elk softwarepakket na welke externe partner leverancier is en lijst de bijhorende contracten, licenties, onderhoudscontracten en of SLA's op, evenals hun vervaldatum.
3. Ga per hardware en per softwarepakket na welke externe partner(s) betrokken is (zijn) bij het beheer, de security en het onderhoud al dan niet in onderaanneming van de leverancier.
4. Maak afspraken met de betrokken externe partner over het intern beheer, digitaliseringsprojecten, veiligheid, continuïteit, veranderingsaanpak, kwaliteit en relatiebeheer van de externe partner(s) of externe leveranciers;
5. Documenteer en actualiseer de processen en planning en communiceer hierover met alle relevante betrokkenen.
6. Bepaal duidelijke communicatielijnen en structureer het maken van afspraken. Documenteer dit.

Bouwsteen 5: Coördinatie tussen de interne coördinator, de externe ICT-ondersteuning en externe leveranciers

1. Bepaal wie binnen het lokaal bestuur de coördinatie intern zal opnemen ten aanzien van externe partner(s), zowel de externe ICT-ondersteuning als de externe leveranciers.
2. Bespreek met de externe partner(s) de ICT-visie/-strategie van het lokaal bestuur en de resultaten van de risicoanalyse.
3. Bepaal welke verwachtingen er zijn ten aanzien van degene die de verantwoordelijkheid voor een risico of een beheersmaatregel opneemt.
4. Bepaal per risico en bijhorende beheersmaatregel(en) of de verantwoordelijkheid voor de opvolging en uitvoering intern of extern ligt. Ga na op welke manier de rollen en verantwoordelijkheden kunnen worden opgenomen in bestekken en in contracten die worden afgesloten. Vaak zal het niet mogelijk zijn bestaande overeenkomsten aan te passen. Ga dan na op welke manier in de toekomst hieraan kan gewerkt worden.
5. Documenteer de afspraken die worden gemaakt over risico-eigenaarschap. Maak een overzicht van wie verantwoordelijk is voor welke beheersmaatregelen.

TYPE 3

Onze ICT-functie werkt projectmatig en trekt ook onze digitaliseringsprojecten. De ICT-functie speelt een centrale rol bij de verdere uitbouw van de digitalisering. Daarnaast zorgt de ICT-functie er ook voor dat alle computers werken en de ICT-functie beheert het netwerk en de servers. Binnen de ICT-functie combineren we dus technische ICT-kennis met expertise op het vlak van digitalisering door de inzet van onze eigen medewerkers eventueel in samenwerking met externen.

Aan de slag met:

Bouwsteen 1: ICT-visie/-strategie van het lokaal bestuur:

1. Breng de noden van uw gebruikers periodiek in kaart.
2. Toets af of deze noden nog passen in de huidige ICT-visie/strategie en bespreek dit op managementniveau.
3. Documenteer en actualiseer de ict-visie/strategie periodiek.

Bouwsteen 2: Risicoanalyse

1. Documenteer de risicoanalyse.
2. Actualiseer periodiek de risicoanalyse.

Bouwsteen 3: Interne beheersmaatregelen

Ga hierbij stapsgewijs te werk:

1. Stel een risicoanalyse op waarbij de ICT-risico's gerelateerd aan het intern beheer geïdentificeerd worden en de bestaande beheersmaatregelen. Ga na of de bestaande beheersmaatregelen voldoende de ICT-risico's voor het intern beheer afdekken (kloofanalyse. De antwoorden die uw lokaal bestuur gaf op de risicomaturiteit zijn een goede start voor een dergelijke risicoanalyse. Stel deze risicoanalyse op in overleg met vertegenwoordigers van de ICT-functie en de ruimere organisatie (bv. managementteam, leidinggevende sleutelfiguren voor bepaalde toepassingen).
   OF
   Check of de bestaande risicoanalyse een breed gamma aan interne en externe risico's dekt en dat deze lijst met risico's voldoende actueel is. Breng een strategische dialoog met het management op gang waardoor vanuit het perspectief van kernprocessen en het dienstverleningsconcept van de organisatie wordt nagedacht over de risico's.
2. Vervolgens dienen de mogelijke oorzaken geïdentificeerd te worden samen met de mogelijke impact en waarschijnlijkheid van de ICT-risico's. Dit naast het bepalen, het implementeren en het testen van de mitigerende acties zodoende ICT-continuïteit te verzekeren. Leg de risico-eigenaar(s) en de actie-eigenaar(s) vast.
3. Deze risicoanalyse dient periodiek geactualiseerd, aangepast, getest en gecommuniceerd te worden bij wijzigingen binnen de organisatie.

Bouwsteen 4: Governancestructuur

De interne coördinator en de externe ICT-ondersteuning werken samen om de governancestructuur op te zetten.

1. Breng in kaart welke hard- en software het lokaal bestuur gebruikt.
2. Ga vervolgens voor elke hardware en elk softwarepakket na welke externe partner leverancier is en lijst de bijhorende contracten, licenties, onderhoudscontracten en of SLA's op, evenals hun vervaldatum.

3. Ga per hardware en per softwarepakket na welke externe partner(s) betrokken is (zijn) bij het beheer, de security en het onderhoud al dan niet in onderaanneming van de leverancier.
4. Maak afspraken met de betrokken externe partner over het intern beheer, digitaliseringsprojecten, veiligheid, continuïteit, veranderingsaanpak, kwaliteit en relatiebeheer van de externe partner(s) of externe leveranciers;
5. Documenteer en actualiseer de processen en planning en communiceer hierover met alle relevante betrokkenen.
6. Bepaal duidelijke communicatielijnen en structureer het maken van afspraken. Documenteer dit.

Bouwsteen 5: Coördinatie tussen de interne ICT-functie, (de externe ICT-ondersteuning) en externe leveranciers

1. Bepaal wie binnen het lokaal bestuur de coördinatie zal opnemen tussen de interne medewerkers en de externe partners.
2. Bespreek zowel met de interne medewerkers als met de externe partners de ICT-visie/-strategie van het lokaal bestuur en de resultaten van de risicoanalyse.
3. Bepaal welke verwachtingen er zijn ten aanzien van degene die de verantwoordelijkheid voor een risico of een beheersmaatregel opneemt.
4. Bepaal per risico en bijhorende beheersmaatregel(en) of de verantwoordelijkheid voor de opvolging en uitvoering intern of extern ligt.
5. Bepaal per risico en bijhorende beheersmaatregel(en) wie effectief de verantwoordelijkheid voor de opvolging en uitvoering opneemt.
6. Documenteer deze afspraken.

AUDIT
VLAANDEREN

TYPE 4

Onze ICT-functie doet van alles, meestal achter de schermen. Vooral de dagdagelijkse noden en vragen geven sturing aan wat de ICT-functie doet of niet doet. Er is geen duidelijke voorafgaande planning en er wordt ook weinig projectmatig gewerkt aan digitaliseringsprojecten. In de ICT-functie is er wel technische ICT-kennis aanwezig, maar voor digitaliseringsprojecten doen we beroep op externen of zal een andere interne dienst de trekkersrol opnemen.

Aan de slag met:

Bouwsteen 1: ICT-visie/-strategie van het lokaal bestuur:

1. Maak bewust tijd de volgende maanden om na te denken over de werking van de ICT-functie en ga op zoek naar een klankbord bij besturen. Kies bewust voor besturen waar de ICT-functie op een andere manier wordt ingevuld dan in de eigen organisatie.
2. Ga op basis van de inzichten de dialoog aan met het managementteam over de evolutie van de ICT-functie in de organisatie
3. Maak samen keuzes en prioritiseer de acties die de ICT-functie op korte en middellange termijn zal opnemen

Bouwsteen 2: Risicoanalyse

1. Bekijk wie (intern of extern) een risicoanalyse kan opmaken;
2. Betrek bij de opmaak van de minstens de DPO, medewerker(s) organisatiebeheersing en het managementteam
3. Heb aandacht voor een degelijke risicoanalyse die ook rekening houdt met toekomstige ontwikkelingen en met de noden van de organisatie op het vlak van digitalisering
4. Volg de opmaak van de risicoanalyse actief op

Bouwsteen 3: Interne beheersmaatregelen

Ga hierbij stapsgewijs te werk:

1. Stel een risicoanalyse op waarbij de ICT-risico's gerelateerd aan het intern beheer geïdentificeerd worden en de bestaande beheersmaatregelen. Ga na of de bestaande beheersmaatregelen voldoende de ICT-risico's voor het intern beheer afdekken (kloofanalyse. De antwoorden die uw lokaal bestuur gaf op de risicomaturiteit zijn een goede start voor een dergelijke risicoanalyse. Stel deze risicoanalyse op in overleg met vertegenwoordigers van de ICT-functie en de ruimere organisatie (bv. managementteam, leidinggevende sleutelfiguren voor bepaalde toepassingen).
   OF
   Check of de bestaande risicoanalyse een breed gamma aan interne en externe risico's dekt en dat deze lijst met risico's voldoende actueel is.
   Breng een strategische dialoog met het management op gang waardoor vanuit het perspectief van kernprocessen en het dienstverleningsconcept van de organisatie wordt nagedacht over de risico's.
2. Vervolgens dienen de mogelijke oorzaken geïdentificeerd te worden samen met de mogelijke impact en waarschijnlijkheid van de ICT-risico's. Dit naast het bepalen, het implementeren en het testen van de mitigerende acties zodoende ICT-continuïteit te verzekeren. Leg de risico-eigenaar(s) en de actie-eigenaar(s) vast.
3. Deze risicoanalyse dient periodiek geactualiseerd, aangepast, getest en gecommuniceerd te worden bij wijzigingen binnen de organisatie.

Bouwsteen 4: Governancestructuur

1. Breng in kaart welke hard- en software het lokaal bestuur gebruikt.
2. Ga vervolgens voor elke hardware en elk softwarepakket na welke externe partner leverancier is en lijst de bijhorende contracten, licenties, onderhoudscontracten en of SLA's op, evenals hun vervaldatum
3. Ga per hardware en per softwarepakket na welke externe partners betrokken is het beheer, security en onderhoud al dan niet in onderaanneming van de leverancier.
4. Maak afspraken met de betrokken externe partner over intern beheer, digitaliseringsprojecten, veiligheid, continuïteit, veranderingsaanpak, kwaliteit en relatiebeheer van de externe partner(s) of externe leveranciers;
5. Documenteer en actualiseer de processen en planning en communiceer hierover met alle relevante betrokkenen.
6. Bepaal duidelijke communicatielijnen en structureer het maken van afspraken. Documenteer dit.

Bouwsteen 5: Coördinatie tussen de interne ICT-functie, de externe ICT-ondersteuning en externe leveranciers

1. Bepaal wie binnen het lokaal bestuur de coördinatie zal opnemen tussen de interne medewerkers en de externe partners.
2. Bespreek zowel met de interne medewerkers als met de externe partners de ICT-visie/-strategie van het lokaal bestuur en de resultaten van de risicoanalyse.
3. Bepaal welke verwachtingen er zijn ten aanzien van degene die de verantwoordelijkheid voor een risico of een beheersmaatregel opneemt.
4. Bepaal per risico en bijhorende beheersmaatregel(en) of de verantwoordelijkheid voor de opvolging en uitvoering intern of extern ligt.
5. Bepaal per risico en bijhorende beheersmaatregel(en) wie effectief de verantwoordelijkheid voor de opvolging en uitvoering opneemt.
6. Documenteer deze afspraken.

AUDIT
VLAANDEREN

TYPE 5

Ons lokaal bestuur heeft er bewust voor gekozen om alle uitvoerende taken (helpdesk, onderhoud computers en netwerk- en serverbeheer) uit te besteden aan externen. Occasioneel zal onze ICT-functie nog wel een (beperkte) helpdeskfunctie opnemen. Voor digitaliseringsprojecten doen we vooral een beroep op externe projectleiders. De ICT-functie zorgt als een regisseur dat alle taken en projecten door de externen volgens de afspraken worden uitgevoerd en neemt dus vooral een coördinerende rol op.

Aan de slag met:

Bouwsteen 1: ICT-visie/-strategie van het lokaal bestuur

1. Ga in dialoog met de externen die u ondersteunen: bevraag de huidige toestand en belangrijke evoluties die van belang zijn voor het lokaal bestuur, maak een kloofanalyse, breng in kaart welke noden er concreet zijn en wie kan het bestuur kan helpen bij toekomstige ontwikkelingen (bvb intergemeentelijk samenwerkingsverband, kenniscentrum, een ander bestuur privé onderneming, ...)
2. Breng de noden van uw gebruikers periodiek in kaart
3. Toets af of deze noden nog passen in de huidige ICT-visie/strategie
4. Documenteer en actualiseer de ICT-visie/strategie periodiek

Bouwsteen 2: Risicoanalyse

1. Check risicotransfer naar externen of deze risico's allemaal beheerst zijn en of er geen risico's zijn waarvoor niemand de verantwoordelijkheid opneemt. (bvb wie doet patchmanagement van welke software, wie onderhoudt welke firewall, server, ...; wie neemt welke rol op bij het bedrijfscontinuïteitsmanagement)

Bouwsteen 3: Interne beheersmaatregelen

Ga hierbij stapsgewijs te werk:

1. Stel een risicoanalyse op waarbij de ICT-risico's gerelateerd aan het intern beheer geïdentificeerd worden en de bestaande beheersmaatregelen. Ga na of de bestaande beheersmaatregelen voldoende de ICT-risico's voor het intern beheer afdekken (kloofanalyse. De antwoorden die uw lokaal bestuur gaf op de risicomaturiteit zijn een goede start voor een dergelijke risicoanalyse. Stel deze risicoanalyse op in overleg met vertegenwoordigers van de ICT-functie en de ruimere organisatie (bv. managementteam, leidinggevende sleutelfiguren voor bepaalde toepassingen).
   OF
   Check of de bestaande risicoanalyse een breed gamma aan interne en externe risico's dekt en dat deze lijst met risico's voldoende actueel is.
   Breng een strategische dialoog met het management op gang waardoor vanuit het perspectief van kernprocessen en het dienstverleningsconcept van de organisatie wordt nagedacht over de risico's.
2. Vervolgens dienen de mogelijke oorzaken geïdentificeerd te worden samen met de mogelijke impact en waarschijnlijkheid van de ICT-risico's. Dit naast het bepalen, het implementeren en het testen van de mitigerende acties zodoende ICT-continuïteit te verzekeren. Leg de risico-eigenaar(s) en de actie-eigenaar(s) vast.
3. Deze risicoanalyse dient periodiek geactualiseerd, aangepast, getest en gecommuniceerd te worden bij wijzigingen binnen de organisatie.

Bouwsteen 4: Governancestructuur

1. Breng in kaart welke hard- en software het lokaal bestuur gebruikt.
2. Ga vervolgens voor elke hardware en elk softwarepakket na welke externe partner leverancier is en lijst de bijhorende contracten, licenties, onderhoudscontracten en of SLA's op, evenals hun vervaldatum
3. Ga per hardware en per softwarepakket na welke externe partners betrokken is het beheer, security en onderhoud al dan niet in onderaanneming van de leverancier.
4. Maak afspraken met de betrokken externe partner over intern beheer, digitaliseringsprojecten, veiligheid, continuïteit, veranderingsaanpak, kwaliteit en relatiebeheer van de externe partner(s) of externe leveranciers;
5. Documenteer en actualiseer de processen en planning en communiceer hierover met alle relevante betrokkenen.
6. Bepaal duidelijke communicatielijnen en structureer het maken van afspraken. Documenteer dit.

Bouwsteen 5: Coördinatie tussen de interne ICT-functie, de externe ICT-ondersteuning en externe leveranciers

1. Bepaal wie binnen het lokaal bestuur de coördinatie zal opnemen tussen de interne medewerkers en de externe partners.
2. Bespreek zowel met de interne medewerkers als met de externe partners de ICT-visie/-strategie van het lokaal bestuur en de resultaten van de risicoanalyse.
3. Bepaal welke verwachtingen er zijn ten aanzien van degene die de verantwoordelijkheid voor een risico of een beheersmaatregel opneemt.
4. Bepaal per risico en bijhorende beheersmaatregel(en) of de verantwoordelijkheid voor de opvolging en uitvoering intern of extern ligt.
5. Bepaal per risico en bijhorende beheersmaatregel(en) wie effectief de verantwoordelijkheid voor de opvolging en uitvoering opneemt.
6. Documenteer deze afspraken.

3.1 INSPIRATIEBRONNEN

Lokale besturen die met deze bouwstenen aan de slag gaan kunnen gebruik maken van instrumenten en goede voorbeelden die aangeboden worden door verschillende actoren.

- In het kader van het programma cyberveilige gemeenten ontwikkelde VVSG een cybersecurity toolkit. Hierin zijn voorbeelden en sjablonen opgenomen voor onder meer een bedrijfscontinuïteitsplan, procedures, … Ook richtlijnen rond ICT-organisatiebeheersing, diverse infosessies en webinars die VVSG organiseerde in het kader van het project cyberveilige gemeenten en nog veel meer is te vinden op de VVSG-website.
- Daarnaast is in 2022 en 2023 nog het aanbod voor ethisch hacken in samenwerking met Howest beschikbaar voor lokale besturen die hun ICT-systemen willen laten testen.
- De mogelijkheid om cofinanciering aan te vragen voor een ICT-veiligheidsaudit uitgevoerd door een professionele auditfirma om de ICT-systemen te testen of andere ICT-werkzaamheden uit te voeren blijft ook in 2022 en 2023 beschikbaar. Dergelijke ICT-veiligheidsaudits kan een lokaal bestuur in de toekomst blijven bestellen op basis van de raamovereenkomst 2019/HFB/OP/52630, perceel 3 Operationele audit bij de lokale besturen of in een interbestuurlijke context (evenwel zonder cofinanciering) of hiervoor zelf een eigen overheidsopdracht uitschrijven. Het controleprogramma van deze ICT-veiligheidsaudits kan een inspiratie bieden voor auditwerkzaamheden of testen op de ICT-systemen van het lokaal bestuur.
- De globale rapporten van de thema-audits informatiebeveiliging bij de lokale besturen geven een zicht op de uitdagingen en risico's die informatiebeveiliging bij lokale besturen werden vastgesteld door Audit Vlaanderen. Tijdens deze audits werd bij tal van lokale besturen goede praktijken vastgesteld met betrekking tot informatieveiligheid. Deze lokale besturen delen hun expertise met andere lokale besturen via de databank op de website van Audit Vlaanderen.
- Maak gebruik van **agile methodieken om te komen tot een prioritering van risico's en acties**.

Een van deze methoden is een MoSCoW-analyse (ontwikkeld door Dai Clegg van Oracle). MoSCoW staat voor:

- Must have. Een must have is een harde eis waaraan niet te tornen valt. Hier moeten we gewoonweg aan voldoen. Als het beoogde resultaat niet wordt behaald, voldoet het projectresultaat niet aan de eisen en is de oplevering of het project mislukt.
- Should have. Een should have is ook een eis, maar geen keiharde. Hieraan moeten we eigenlijk ook voldoen, maar er is wel enige speling: misschien mag het resultaat enigszins afwijken, is er een alternatieve oplossing mogelijk, of kunnen we de eis bij een volgende oplevering meenemen.
- Could have. Een could have is geen eis, maar een wens. Onze inspanning heeft meerwaarde en het is zeker nuttig de wens in te vullen, maar dit is niet noodzakelijk. Could haves zijn zaken waar je tijd aan kunt besteden als aan de must en should haves is voldaan en moest er nog wat tijd en middelen over zijn.

– Won't have. Een won't have is een eis of wens, waarvan is afgesproken dat deze – in ieder geval in de huidige sprint/oplevering – niet binnen de scope valt. Het is dus niet zo, dat het leuk zou zijn als deze eis of wens wordt ingevuld. Integendeel: er mogen aan een won't have geen tijd en resources besteed worden, want dit heeft namelijk geen toegevoegde waarde of gaat ten koste van belangrijkere eisen.

  Een project dat er niet in slaagt om alle must have vereisten te realiseren, heeft zijn einddoel niet bereikt.

AUDIT
VLAANDEREN

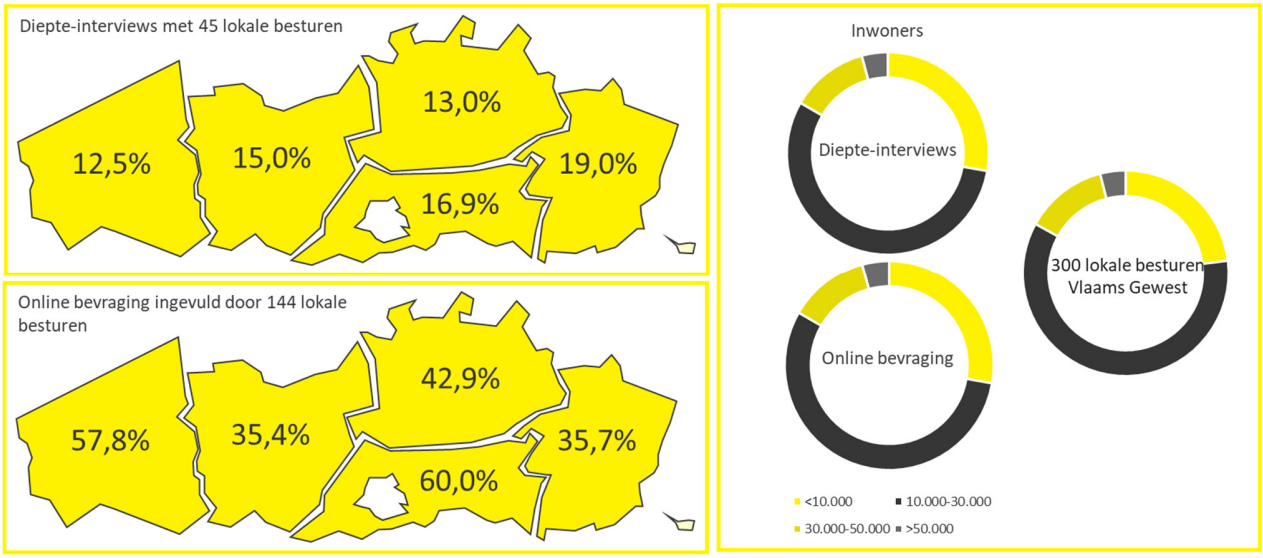
BIJLAGE 1: SELECTIE VAN DE LOKALE BESTUREN

De 144 geselecteerde lokale besturen hadden in oktober 2021 hadden ze (nog) geen ICT-veiligheidsaudit besteld. Bij deze besturen heeft Audit Vlaanderen in het verleden nog geen thema-audit informatiebeveiliging uitgevoerd in 2017-2018 en 2020. De selectie van de 45 lokale besturen voor de diepte-interviews gebeurde op basis van volgende criteria:

- hun antwoorden op de online bevraging;
- geografische spreiding;
- het aantal inwoners.

De verdeling op basis van de geografische verdeling van de lokale besturen opgenomen in de online bevraging werd in grote mate gerespecteerd werd voor de selectie van de lokale besturen voor de diepte-interviews. Voor de selectie van de lokale besturen op basis van het inwonersaantal is de verdeling van de lokale besturen geselecteerd voor de online bevraging gelijklopend met deze die geselecteerd werden voor de diepte-interviews. In vergelijking met alle 300 lokale besturen in het Vlaamse Gewest blijkt dat bij deze thema-audit iets meer kleinere lokale besturen werden opgenomen in de selectie.

De volledige lijst van de bevraagde lokale besturen is terug te vinden in bijlage 5.



Figuur 1. Overzicht van het percentage deelnemende lokale besturen ten opzichte van totaal aantal lokale besturen per provincie (links) en indicatie van de grootte van deze besturen (uitgedrukt in aantal inwoners)

BIJLAGE 2: DE BESTAFFING VAN DE ICT-FUNCTIE IN LOKALE BESTUREN

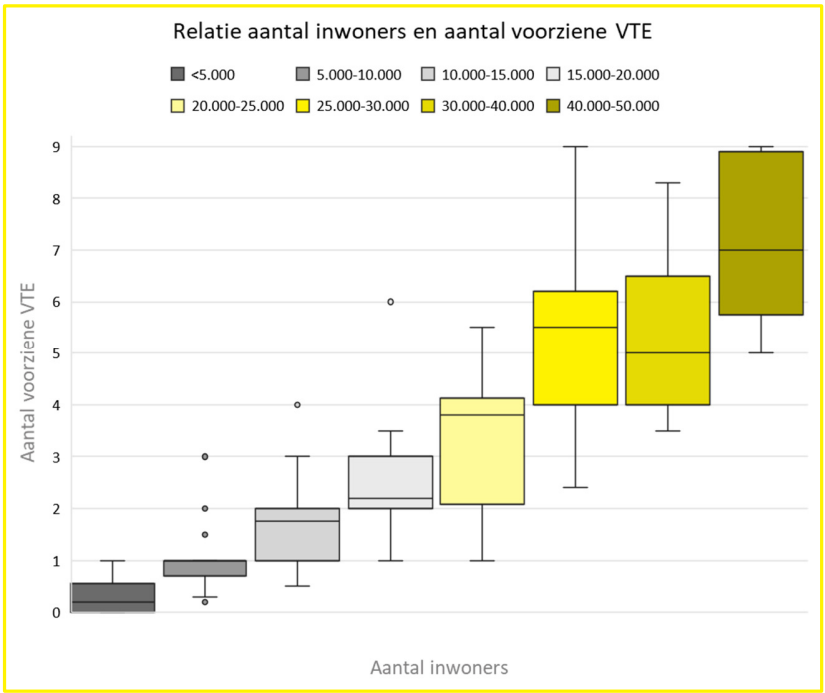
Op basis van de resultaten van de online bevraging werd een analyse gemaakt over de bestaffing van de ICT-functie in de bevraagde lokale besturen. De vragenlijst en de resultaten zijn terug te vinden in de bijlagen 3 en 4.

Personeelskader

Het aantal VTE voorzien voor de ICT-functie blijkt vooral afhankelijk van volgende factoren:

Factor 1: Het aantal inwoners

Het aantal VTE dat voor de ICT-functie wordt voorzien in het organigram van een lokaal bestuur is sterk uiteenlopend. In figuur 3 wordt op de Y-as telkens de voorziene bestaffing van de ICT-dienst weergegeven (uitgedrukt in VTE) voor 8 categorieën van lokale besturen (afhankelijk van het aantal inwoners gaande van <5.000 tot 50.000 inwoners). Voor besturen met meer dan 50.000 inwoners is er niet voldoende data beschikbaar om een representatief beeld te geven van deze categorie. De horizontale lijn geeft telkens de mediaan per categorie weer. Uit deze figuur kan er afgeleid worden dat voor besturen tussen de 0-20.000 inwoners de mediaan van het aantal VTE steeds onder de 3 VTE ligt. Vanaf 20.000 inwoners stijgt het gemiddeld aantal VTE naar meer dan 3 VTE.



Figuur 2. Relatie van het aantal voorziene VTE in het organigram en aantal inwoners voor de 144 bevraagde lokale besturen

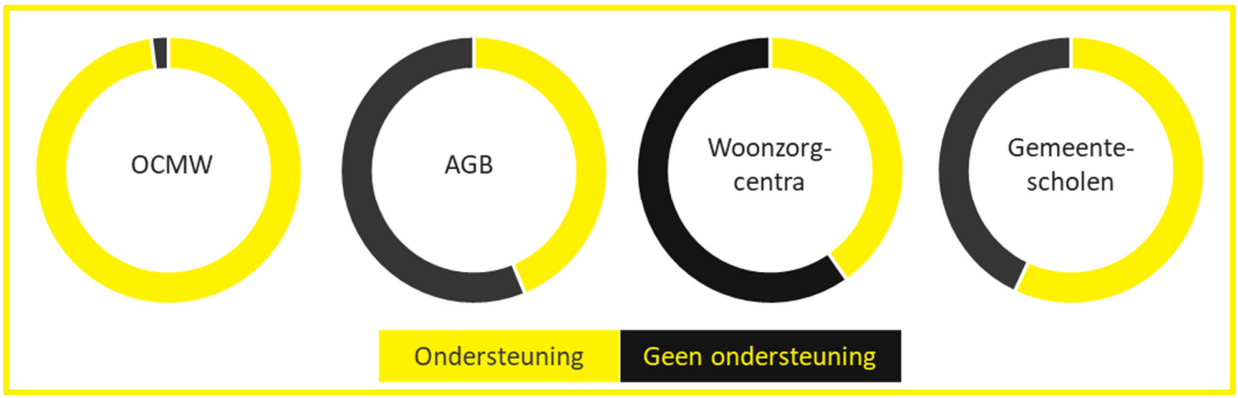
Factor 2: Het aantal entiteiten en het aantal eindgebruikers die ondersteund worden

Naast het aantal inwoners is het aantal te ondersteunen eigen diensten en bij uitbreiding aangeboden dienstverlening (buiten de klassieke diensten) en al dan niet verzelfstandigede of verwante entiteiten een belangrijke indicator voor de werklast. Hoe meer ondersteuning voor diensten en entiteiten , hoe meer verschillende locaties en hoe meer eindgebruikers moeten worden ondersteund met hardware en software.

Typisch ondersteunt een ICT-dienst de eigen diensten van de gemeente, het OCMW en eventuele AGB's. Een deel van de lokale besturen bieden ook aan andere (al dan niet verzelfstandigde of verwante) entiteiten ICT-dienstverlening. Figuur 4 geeft de procentuele verdeling weer van de ondersteuning die de 45 bevraagde besturen geven.

Figuur 5 geeft een inzicht voor enkele veel voorkomende diensten of entiteiten waarvoor

Figuur 4. Voor de 45 geselecteerde lokale besturen wordt de verdeling weergegeven van het aantal diensten, al dan niet verzelfstandigde of verwante entiteiten die door de ICT-functie ondersteund worden. De binnenste ring omvatten de klassieke diensten van een lokaal bestuur. de tweede ring is de extra dienstverlening die het lokaal bestuur aan zijn inwoners aanbiedt via al dan niet verzelfstandigde entiteiten, maar meestal wel op een aparte locatie. De buitenste ring zijn verwante entiteiten waar een lokaal bestuur soms ook ICT-ondersteuning voor aanbiedt.



Figuur 5. Overzicht van de ondersteuning die de 144 bevraagde lokale besturen geven aan OCMW, AGB, woonzorgcentra en gemeentescholen

het lokaal bestuur ICT-ondersteuning in de 144 lokale besturen (naast de eigen gemeentelijke diensten) leveren aan OCMW (98%), AGB's (44%), woonzorgcentra (40%) en gemeentescholen (57%).

Factor 3: De breedte van het takenpakket, opgenomen door de ICT-functie verschilt per lokaal bestuur

Er zijn lokale besturen waar de ICT-functie voornamelijk operationele (basis)ondersteuning levert zoals het onderhouden van een helpdesk, het beheren van zowel soft- als hardware en netwerkbeheer. Ruimere taken worden bij deze lokale besturen niet opgepakt door de ICT-functie, maar hiervoor wordt externe ondersteuning al dan niet tijdelijk ingehuurd. Bij andere lokale besturen neemt de ICT-functie naast de operationele (basis)ondersteuning ook ruimere taken op zoals digitaliseringsprojecten, sensibiliseren van eindgebruikers met betrekking tot informatieveiligheid, enz.

Tijdens de audit werd eveneens duidelijk dat de lokale besturen uiteenlopende keuzes gemaakt hebben over welke taken door de ICT-functie in eigen beheer worden opgenomen en voor welke ICT-dienstverlening of -expertise men een beroep op commerciële partners en/of op publieke organisaties zoals intergemeentelijke samenwerkingsverbanden of het provinciebestuur.

Factor 4: De manier waarop er al dan niet samengewerkt wordt met externe partijen

Tijdens de diepte-interviews met de 45 lokale besturen komt naar boven dat een aantal besturen beroep doet op externe medewerkers voor de invulling van kerntaken zoals helpdesk, beheer van servers, enz.. Daarnaast doen lokale besturen voornamelijk beroep op externe partijen voor de ontwikkeling of de levering van specifieke pakketten (software). Deze leveranciers nemen vaak het beheer op van de software en zorgen dat aan SLA's wordt voldaan. Als gevolg hiervan wordt contractbeheer en opvolging of overleg met leveranciers een belangrijke taak voor de ICT-functie. In een aantal lokale besturen zal deze taak eerder bij het management terecht komen bij gebrek aan een interne ICT-functie.

Welke keuze het lokaal bestuur ook gemaakt heeft over wat ze zelf met eigen personeel als ICT-functie aanbiedt, in elk lokaal bestuur wordt samengewerkt met externen. Hierdoor is de opvolging van de contracten met de externe (diensten)leveranciers een essentieel onderdeel van de interne ICT-functie. Dit is een taak die intern bij het lokaal bestuur zal opgepakt moeten worden zelfs als er geen interne ICT-functie voorzien wordt.

De samenwerkingsvormen en partnerschappen die lokale besturen aangaan verschillen onderling. Er zijn vijf types samenwerkingsverbanden te onderscheiden binnen de lokale besturen. Deze samenwerkingsverbanden hebben ook hun gevolg voor de manier waarop de ICT-functie invulling krijgt en op de risicotransfer (tussen het lokaal bestuur en de ICT-leveranciers en -dienstverleners). Deze types kunnen teruggevonden worden in het hoofdstuk 'Aan de slag met de bouwstenen'.

AUDIT
VLAANDEREN

BIJLAGE 3: ONLINE BEVRAGING - VRAGENLIJST

De online bevraging werd opgesteld met het oog op het inschatten van het beheer van de ICT-risico's op een efficiënte manier zonder een al te grote belasting van de lokale besturen. De focus van de digitale bevraging lag bij de opzet van de ICT-governance van het bestuur. Dit is immers een kritieke succesfactor voor een uitrol van risicobeheer. In deze zelfevaluatie werd niet dieper ingegaan op de bevraging van specifieke risicodomeinen. Aan de hand van de diepte-interviews met 45 lokale besturen kreeg dit wel verder vorm.

Onderstaande vragenlijst en antwoordmogelijkheden konden online de lokale besturen invullen in de periode november 2021 – januari 2022. Bij het versturen van de online bevraging werd gevraagd om deze te laten invullen door de ICT-verantwoordelijke van het lokaal bestuur.

ICT-risico's op organisatieniveau bij de lokale besturen – vragenlijst

Aanleiding en aanpak voor deze thema-audit

Audit Vlaanderen selecteerde jouw lokaal bestuur, samen met een hele reeks andere lokale besturen, voor de thema-audit Beheer van ICT-risico's. Meer informatie over de aanleiding en de aanpak van deze thema-audit kan je terugvinden op de website van Audit Vlaanderen (https://auditvlaanderen.be/ict-risicos-op-organisatieniveau-bij-de-lokale-besturen).

Deze thema-audit bestaat uit een brede, online bevraging over de omgang met diverse ICT-risico's bij de gemeente en het OCMW. Deze online bevraging is beknopt en heeft niet tot doel om alle risico's exhaustief te bevragen. Dergelijk uitgebreid risicomanagement behoort immers tot de verantwoordelijkheid van het lokaal bestuur. Deze bevraging peilt naar de maturiteit van het risicomanagement op het vlak van overkoepelende ICT-risico's bij de organisatie van het ICTgebeuren ("IT-beheersmaatregelen op organisatiebreed niveau") en op het vlak van de voornaamste generieke ICT-risico's ("Algemene IT-beheersmaatregelen, soms ook naar verwezen met de term IT general controls").

Het invullen van de bevraging neemt ongeveer een half uur in beslag en mag gebaseerd zijn op parate kennis. Er is **geen interne consultatie of bijkomend opzoekwerk vereist**.

Opbouw van de vragenlijst
Deze vragenlijst bestaat uit 6 delen:
I. Identificatie
II. Situering van de ICT-functie of de ICT-verantwoordelijke binnen de organisatie
III. ICT-visie en -strategie bij jouw lokaal bestuur
IV. Strategie voor digitale transformatie en innovatie in ICT
V. ICT-risicobeheer bij jouw lokaal bestuur
VI. Inschatting van een aantal beheersmaatregelen

AUDIT
VLAANDEREN

De vragenlijst is ook beschikbaar op onze website.

Kan je deze vragenlijst uiterlijk voor **30 november 2021** invullen aub ?
Indien je vragen hebt bij het invullen van de vragenlijst kan je contact opnemen met het auditteam via e-mail: ICTbevraging2021@vlaanderen.be (mailto:ICTbevraging2021@vlaanderen.be)

Het auditteam

* Vereist

I. IDENTIFICATIE

1. Voor welk lokaal bestuur vul je deze vragenlijst in? *

2. Vul je contactgegevens in (naam, telefoonnummer, e-mailadres, functie binnen het lokaal bestuur).
Alle gegevens worden enkel in kader van deze thema-audit verwerkt in overeenstemming met de Algemene Verordening Gegevensbescherming. Meer info in de Privacyverklaring op de website van Audit Vlaanderen. *

3. Welke entiteit(en) maken gebruik van de ICT-omgeving/ICT-functieverlening van je lokaal bestuur?
Meerdere antwoorden zijn mogelijk. *

- *gemeentelijke administratie*
- *OCMW-administratie*
- *AGB(’s)*
- *Welzijnsvereniging(en)*
- *Woonzorgcentr(um/a)*
- *Gemeentescho(o)l(en)*
- *Andere*

II. SITUERING VAN DE ICT-FUNCTIE of ICT-VERANTWOORDELIJKE BINNEN DE ORGANISATIE

4. Hoeveel menskracht (uitgedrukt in VTE) wordt er in het organigram van het lokaalbestuur voorzien voor het ICT-beheer van de organisatie?
Met ICT-beheer bedoelen we alle activiteiten die in de meest brede zin behoren tot ICT: bemannen van de helpdesk, functionele analisten, beheer van hardware en applicaties, data architect, opmaak ICT-plannen, opvolgen ICT-leveranciers, … Indien je een externe medewerker hebt die via een dienstverleningsovereenkomst op regelmatige basis ondersteuning biedt, mag die meegerekend worden. We willen een beeld krijgen van de totale omvang van de ICT-capaciteit in je lokaal bestuur. *

Aantal VTE (VolTijds Equivalenten): je mag een grootteorde aangeven
Gebruik een punt voor de decimalen.
De waarde moet een getal zijn

5. Hoeveel van deze menskracht was op 1/10/2021 NIET ingevuld (bijvoorbeeld door openstaande vacatures, langdurig zieken, personeelsleden die wel in het organigram van de ICT-functie voorzien zijn maar daadwerkelijk (een deel van) hun tijd besteden aan andere opdrachten of projecten,…)?

Aantal VTE: dit mag een schatting zijn.
Gebruik een punt voor de decimalen.
De waarde moet een getal zijn

6. Maakt de ICT-verantwoordelijke in jouw lokaal bestuur deel uit van het managementteam?
- Ja
- Neen
- Neen, maar de ICT-verantwoordelijke kan wel autonoom aandachtspunten met betrekking tot ICT agenderen op het managementteam.

III. ICT-visie en -strategie bij jouw lokaal bestuur

7. Werden er op beleidsniveau (bijvoorbeeld in het bestuursakkoord, Meerjarenplan 2020-2025) expliciet doelstellingen met betrekking tot ICT en digitalisering vooropgesteld?
- Ja
- Neen

8. Heeft jouw lokaal bestuur een ICT-strategie/-visie die besproken en gevalideerd is door het managementteam? *
- Ja
- Neen
- Andere

9. Is het duidelijk welke stappen tegen wanneer zullen worden gezet om de doelstellingen van de ICT-strategie/-visie concreet te realiseren? Beschik jij met andere woorden over een ICT-actieplan met concrete timing/mijlpalen?
- Ja
- Neen

IV. Strategie voor digitale transformatie en innovatie in ICT

10. Wanneer jouw lokaal bestuur recent een (grootschalig) ICT-project heeft uitgevoerd (vb migratie van data naar de cloud, vervanging van technische infrastructuur, overstap naar nieuw boekhoudsysteem of systeem voor personeelsadministratie) of bezig is met de voorbereiding van dergelijk ICT-project, heb je dan de risico's van de verandering en van de nieuwe werking al in kaart gebracht?
- Ja
- Neen

11. Is digitalisering van de processen en de dienstverlening momenteel een belangrijk aandachtspunt voor jouw lokaal bestuur?
- Ja
- Neen

AUDIT
VLAANDEREN

V. ICT-risicobeheer bij jouw lokaal bestuur

12. Werd er de voorbije drie jaar een risicoanalyse m.b.t. ICT-risico's uitgevoerd?

- Ja
- Ja, voor een deel van de ICT-risico's
- Neen

13. Werd bij deze risicoanalyse rekening gehouden met volgende elementen?
Meerdere antwoorden zijn mogelijk.

- De bevindingen uit de zelfevaluatie in het kader van organisatiebeheersing
- De bevindingen over de ICT-risico's opgelijst door de DPO en/of de informatieveiligheidscel
- De specifieke projectrisico's gelinkt aan (grote) digitaliseringsprojecten
- De bevindingen uit de omgevingsanalyse voor het meerjarenplan 2020-2025
- De inschatting voor specifieke onderdelen van het thema ICT (bv. cybersecurity)
- Andere

14. Kan je voor onderstaande domeinen van het thema ICT aanduiden of de risico's geïdentificeerd zijn (via een risicoanalyse en/of door incidenten)? Meerdere antwoorden zijn mogelijk.

1. Strategisch ICT-beheer (ICT-governance)
2. Inrichting van de ICT-functie en/of ICT-functie(s) (ICT-organisatie)
3. Afspraken met betrekking tot het digitaal werken binnen de organisatie (bv. opslag bestanden,
1. communicatiekanalen, …)
4. Richtlijnen en afspraken in de organisatie/gedrag van gebruikers/gebruik van internet en mobiele
2. apparatuur
5. ICT-kennis op het vlak van digitaal werken
6. Samenwerking met leveranciers en providers
7. Informatieveiligheid en databeheer
8. Cyberveiligheid
9. Fysieke beveiliging van de technische infrastructuur
10. Toegangsbeheer (tot netwerk en applicaties)
11. Beheer van autorisaties en rechtenbeheer
12. Continuïteit, incidentenbeheer en noodprocedures
13. Applicatielandschap, interfaces (zogenaamde enterprise architectuur)

15. Kan je aangeven in welke mate - volgens jouw beoordeling - de risico's in de onderstaande domeinen van het thema ICT onder controle zijn? Indien geen optie gekozen wordt, gaan we ervan uit dat je het antwoord niet kent.

	Voldoende afgedekt	Nog belangrijke werkpunten	Onvoldoende onder controle
1. Strategisch ICT-beheer (ICT-governance)			
2. Inrichting van de ICTdienst en/of ICT-functie(s) (ICT-organisatie)			
3. Afspraken met betrekking tot het digitaal werken binnen de organisatie (bv. opslag bestanden, communicatiekanalen, …)			
4. Richtlijnen en afspraken in de organisatie/gedrag van gebruikers/gebruik van internet en mobiele apparatuur			
5. ICT-kennis van gebruikers op het vlak van digitaal werken			
6. Samenwerking met leveranciers en providers			
7. Informatieveiligheid en databeheer			
8. Cyberveiligheid			
9. Fysieke beveiliging van de technische infrastructuur			
10. Toegangsbeheer (tot netwerk en applicaties)			
11. Beheer van autorisaties en rechtenbeheer			
12. Continuïteit, incidentenbeheer en noodprocedures			
13. Applicatielandschap, interfaces (zogenaamde enterprise architectuur)			

VI. Inschatting van een aantal beheersmaatregelen

16. Hieronder vind je een steekproef van beheersmaatregelen in het kader van ICT-beheer en risicobeheersing. Wij proberen een beeld te vormen van de mate waarin jouw organisatie deze beheersmaatregel al heeft geïmplementeerd. Kan je voor elk van de volgende beheersmaatregelen aangeven in welke mate deze van toepassing zijn op jouw lokaal bestuur op dit moment? Indien geen optie gekozen wordt, gaan we ervan uit dat je het antwoord niet kent.

	Neen, Helemaal niet	In beperkte mate	Ja, gedeeltelijk	Ja, grotendeels wel	Ja, we zijn een goede praktijk op dit vlak	Geen idee of Niet in te schatten
De ICT-strategie wordt gedragen/is gekend door het bestuur en de ruimere organisatie.						
We volgen nieuwe technologische evoluties en innovatie in ICT actief op.						
Er is een duidelijke visie en er worden bewuste en consequente keuzes gemaakt in de organisatie over wat de ICT-functie doet in eigen beheer en waarvoor de organisatie een beroep doet op de markt.						
In de ICT-functie is er voldoende kennisoverdracht en er worden vervangers voorzien voor personeelsleden die een kritieke functie uitoefenen.						
Rollen en verantwoordelijkheden binnen de ICT-functie, alsook ICT-processen werden gedocumenteerd en zijn duidelijk voor de gehele organisatie.						
Er is een degelijk projectmanagement bij IT-projecten in onze organisatie.						
Er is een goede samenwerking tussen de ICT-functie en de gebruikers bij het in kaart brengen van digitaliseringsnoden.						
De ICT-functie kent de noden van de gebruikers en werkt samen met gebruikers behoefteanalyses, marktconsultaties en bestekken uit.						
Er wordt rekening gehouden met organisatieveranderingsbeheer om digitalisering te verankeren in de organisatie. (vb. invoering digitaal vergaderen).						
De kwaliteit van ICT-functieverlening door externe partijen wordt opgevolgd en gerapporteerd.						
Er is een gedocumenteerd overzicht van het gehele applicatie- en infrastructuurlandschap /architectuur en netwerk van het lokaal bestuur.						
Er is een gedocumenteerd overzicht van de hardware (PC's, laptops, servers, displays, automaten,...) van het lokaal bestuur.						
Er is een gedocumenteerd overzicht van alle bestaande licenties met hun vervaldatum.						
De gebruikers maken enkel gebruik van geautoriseerde en gekende systemen bij de ICT-functie, met andere woorden er wordt geen gebruik gemaakt van schaduwsoftware.						
Er is een duidelijk zicht op de data architectuur/ datastromen, alsook koppelingen met externe bronnen.						

Er is een adequate noodplanning/bedrijfscontinuïteitsplan/ disaster recovery plan aanwezig dat ook voorziet in de aanpak van een ICT-incident (vb een cyberaanval).						
Er is een goed bewustzijn binnen de organisatie rond informatieveiligheid en cyberveiligheid.						
Er is een gedocumenteerd informatieveiligheidsbeleid.						
Er zijn in het arbeidsreglement/ deontologische code richtlijnen opgenomen over het gebruik van ICT door de medewerkers.						
Er zijn goede afspraken over het actueel houden van de IT-omgeving (bv.patch management).						

17. Zowel in 2018 als in 2020 stelde Audit Vlaanderen tijdens de thema-audit Informatieveiligheid bij lokale besturen in Vlaanderen vast dat er dringend meer werk moest worden gemaakt van de informatiebeveiliging. Hebben jullie reeds actie ondernomen op dit vlak?

- Ja
- Neen

18. Indien Ja: op welke wijze ging jouw lokaal bestuur hiermee aan de slag?

19. Indien Neen: Waarom nam jouw lokaal bestuur geen actie?

20. Indien Neen: Wat is er nodig om wel over te gaan tot actie?

BIJKOMENDE INFORMATIE

21. Zijn er volgens jou nog belangrijke organisatiebrede ICT-risico's die niet aan bod kwamen in de vragenlijst?

22. Zijn er goede praktijken die jouw lokaal bestuur wil delen met andere lokale besturen?

23. Heeft jouw lokaal bestuur vragen met betrekking tot ICT-risico's of -risicobeheer waarover je meer informatie wil?

24.Heb je nog andere bedenkingen of aandachtspunten die je wil delen met het auditteam?

25. Kon je deze vragenlijst vlot invullen?

Zeer moeilijk Zeer gemakkelijk

0	1	2	3	4	5	6	7	8	9	10

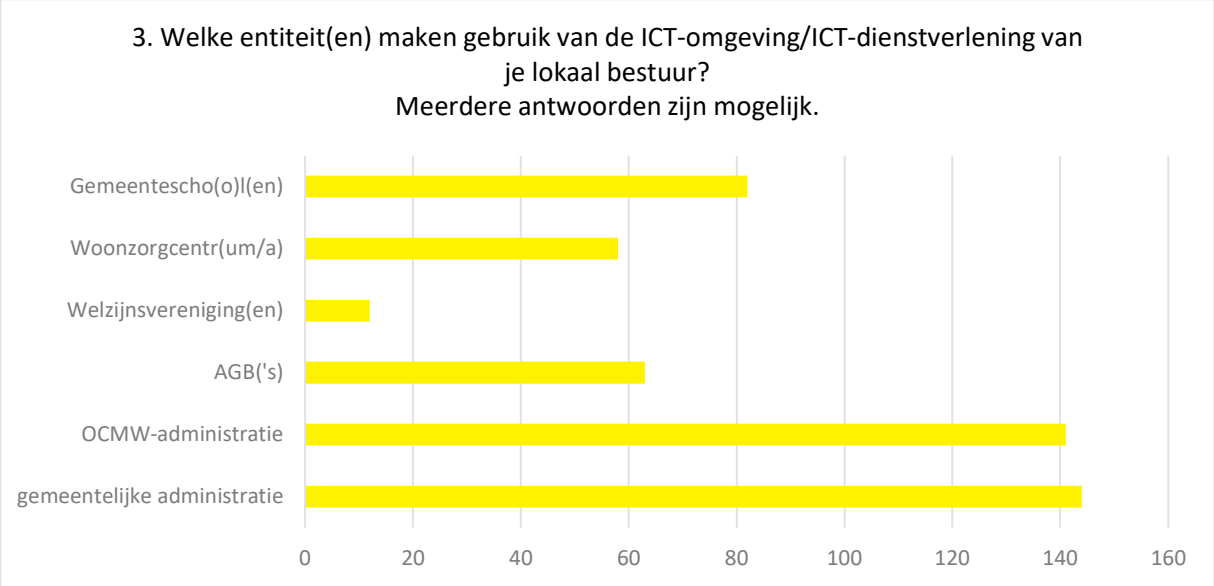
BIJLAGE 4: ONLINE BEVRAGING - RESULTATEN

In de meeste gevallen vulde de ICT-verantwoordelijke de bevraging in. Bij afwezigheid van een ICT-verantwoordelijke werd de bevraging ingevuld door een medewerker die betrokken is het bij ICT-gebeuren in het lokaal bestuur, de algemeen directeur of de financieel directeur van het lokaal bestuur.

I. IDENTIFICATIE

Vraag 1 en 2:
De invuller van de online bevraging vermeldde de naam van het lokaal bestuur en de contactgegevens van de ICT-verantwoordelijke of diegene die de online bevraging invulde.

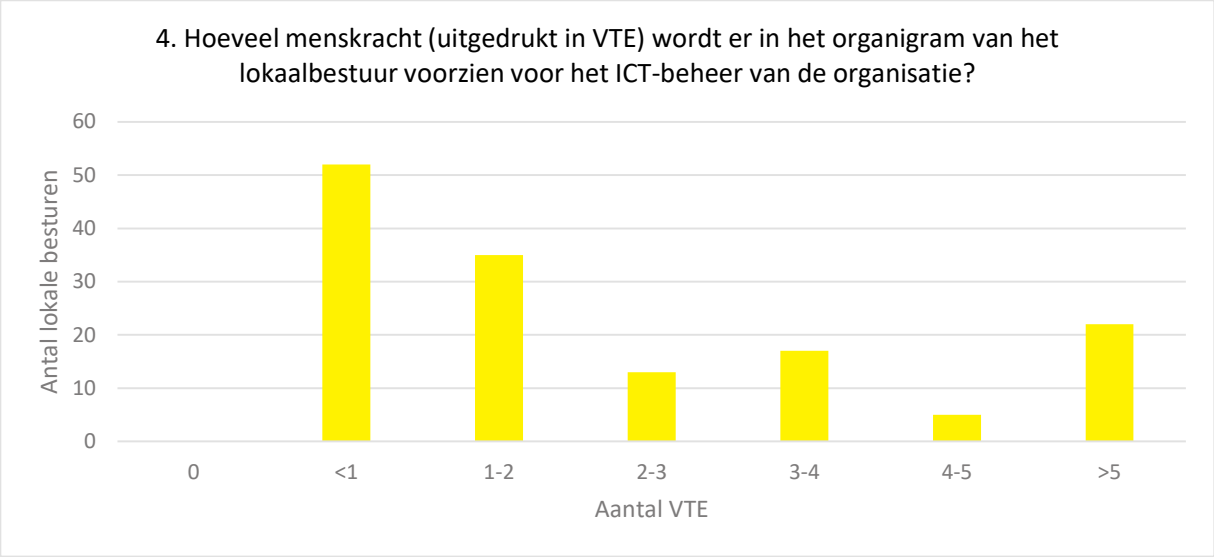
Vraag 3:



Uit de online bevraging blijkt dat de ICT-functie in het lokaal bestuur niet alleen instaat voor de ICT-ondersteuning van de gemeente en het OCMW. De helft van de lokale besturen ondersteunt ook een of meerdere andere entiteiten die geen deel uitmaken van de gemeentelijke of OCMW-administratie, maar die er wel nauw mee verbonden zijn. Het betreft meestal autonome gemeentebedrijven, woonzorgcentra en gemeentescholen.

II. SITUERING VAN DE ICT-FUNCTIE of ICT-VERANTWOORDELIJKE BINNEN DE ORGANISATIE

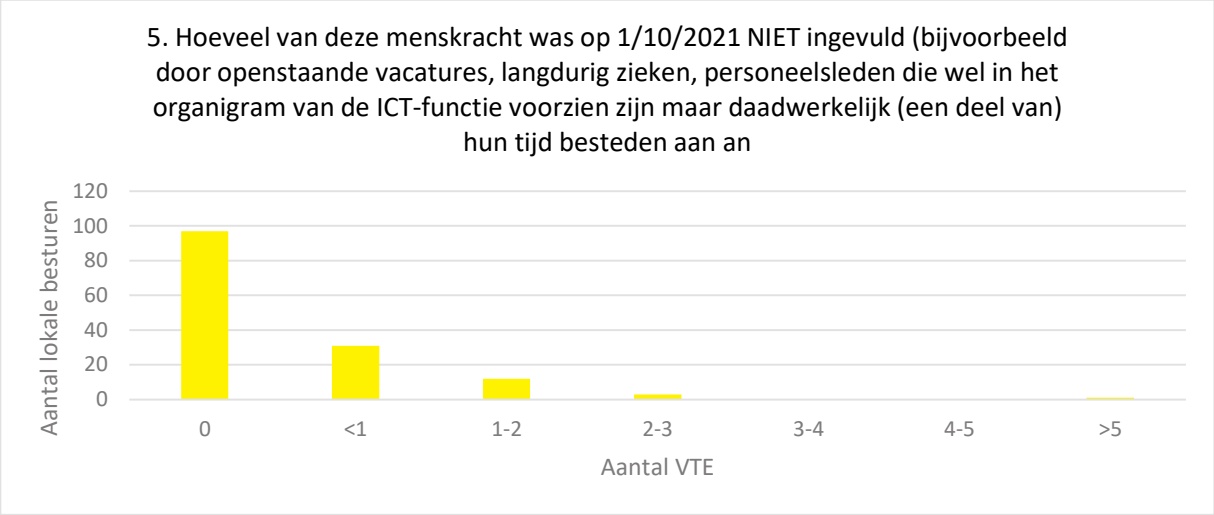
vraag 4:



Een lokaal bestuur voorziet in het personeelsplan (organigram) het aantal VTE dat nodig zal zijn om op een door de organisatie vastgelegde wijze de ICT-ondersteuning te bieden. Het is een inschatting van het aantal vereiste VTE om de taken gekoppeld aan de ICT-ondersteuning die intern zal opgepakt worden, op een behoorlijke manier te voorzien in functie van de hoeveelheid werk en de taken die hierbij verwacht worden. Een lokaal bestuur dat vooraf beslist om de ICT-functie (grotendeels) in te vullen via externe ondersteuning zal minder VTE in het organigram reserveren voor de ICT-functie. De antwoorden van de lokale besturen tonen aan dat er in elk lokaal bestuur een aantal VTE voorzien zijn in het organigram om de ICT-functie in te vullen binnen het lokaal bestuur. Bij 58% van de 144 bevraagde lokale besturen worden 0,02 tot 2 VTE in het organigram voorzien. Bij een derde van de 144 lokale besturen wordt zelfs minder dan 1 VTE voorzien. Bij 4 van de 144 lokale besturen is er 0 VTE voorzien in het organigram voor ICT.

Het aantal VTE voorzien in het organigram is onder meer afhankelijk van het aantal inwoners. De details hiervan zijn terug te vinden in bijlage 2.

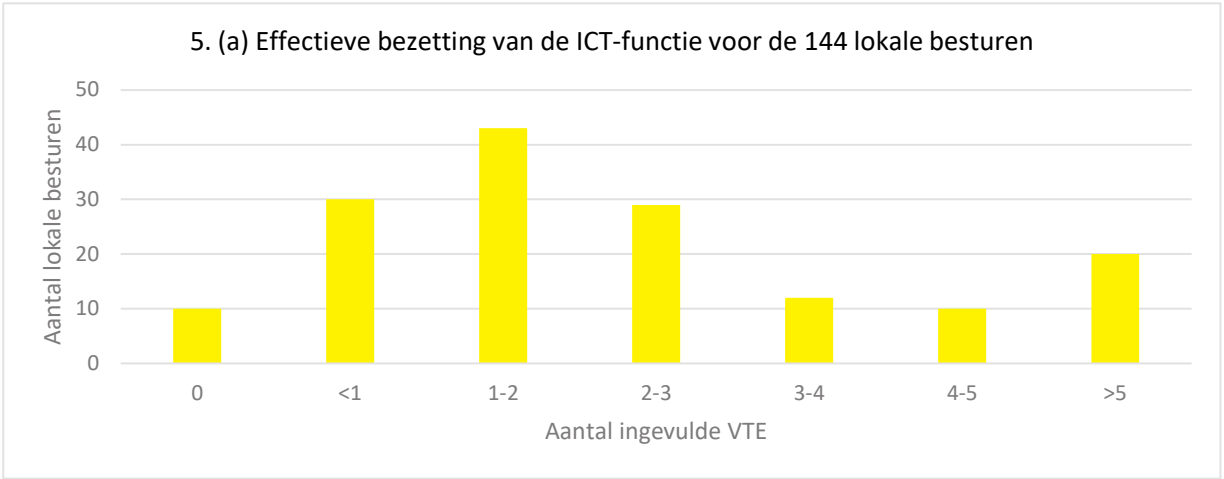
vraag 5:



Elk lokaal bestuur voorziet een aantal VTE in het organigram om de ICT-functie in te vullen. Op basis van de antwoorden varieerde het aantal voorzien VTE van 0,02 VTE tot 250 VTE. 4 lokale besturen voorzien geen enkele VTE in hun organigram. Evenwel slaagt niet elk lokaal bestuur erin om deze VTE ook effectief volledig in te vullen. Bij 33% van 144 lokale besturen was de voorzien ICT-functie niet ingevuld. 3% van de lokale besturen voorziet geen enkele VTE in het organigram voor de ICT-functie en bij de overige 74 % van de lokale besturen was het aantal voorziene VTE volledig ingevuld.

De redenen die aangehaald werden (waarom de ICT-functie niet volledig was ingevuld) werd tijdens de diepte-interviews bevraagd bij 45 lokale besturen. Redenen die het vaakst werden aangehaald:

- langdurige afwezigheid van de ICT-medewerker omwille van ziekte, loopbaanonderbreking, ...;
- openstaande vacature die moeilijk tot niet in te vullen zijn;
- plaatsen in het organigram waarvoor nog geen vacature werd uitgeschreven.



De antwoorden op vraag 5 en 6 samen geven een beeld van het aantal effectieve VTE die op het moment van de online bevraging de ICT-functie in de 144 lokale besturen verzorgde. Hierbij valt op dat de meeste lokale besturen geen tot 2 VTE in dienst hebben. Een beperkt aantal heeft 5 of meer VTE in dienst.

Het aantal VTE voorzien in het organigram is afhankelijk van 4 factoren. De details hiervan zijn terug te vinden in bijlage 2.

vraag 6:

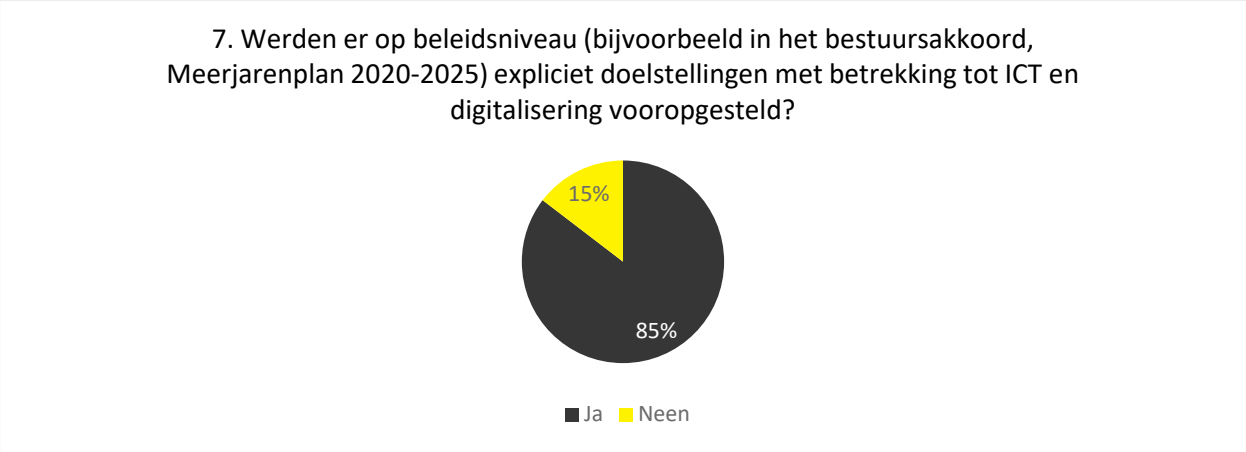
Slechts 23% van de ICT-verantwoordelijken bij de 144 lokale besturen blijkt deel uit te maken van het managementteam van het lokaal bestuur. Daarnaast heeft iets meer dan een kwart de mogelijkheid om autonoom ICT-gerelateerde punten op de agenda van het management te zetten. Bij 51 % maakt de ICT-verantwoordelijke geen deel uit managementteam.

In de diepte-interviews (bij 45 lokale besturen) -werd vooral gepeild hoe de relatie met het managementteam was en of dit een invloed had op het beslissingsproces voor ICT-gerelateerde zaken. Uit de antwoorden bleek vooral dat in de meeste gevallen het managementteam weinig ICT-kennis heeft en veelal steunt op de adviezen van de ICT-verantwoordelijke. Wanneer de ICT-verantwoordelijke geen deel uitmaakt van het management kan hij/zij vaak wel een toelichting geven aan het managementteam omdat hij/zij uitgenodigd wordt op het managementteam of omdat hij/zij vooraf een schriftelijk advies kan aanleveren. In een aantal gevallen werd aangegeven dat het niet mogelijk was of niet gebruikelijk was dat een ICT-verantwoordelijke op het managementteam punten kan komen toelichten. Dit vertaalde zich - volgens de bevraagde ICT-verantwoordelijken – in een stroef beslissingsproces. Hierdoor werden soms inefficiënte beslissingen genomen of moesten punten opnieuw geagendeerd worden.

Anderzijds gaven ICT-verantwoordelijken ook aan dat 'deelnemen aan het managementteam' geen heiligmakende oplossing is, omdat veel aandachtspunten die daar besproken worden geen weerslag hebben op ICT of digitalisering. Het is dus belangrijk een goede balans te vinden tussen wat op het managementteam wordt geagendeerd en het aandachtsgebied voor de ICT-verantwoordelijke. Uit de diepte-interviews bleek dat in een aantal gevallen de algemeen directeur of de clustermanager succesvol een brugfunctie opneemt tussen de behoeften van de zogenaamde business of de gebruikers (lees het managementteam) en de meer technisch georganiseerde ICT-dienst.

III. ICT-visie en -strategie bij jouw lokaal bestuur

vraag 7:



Deze vraag peilde bij de 144 lokale besturen of ze specifiek voor ICT en digitalisering reeds doelstellingen hadden geformuleerd. Er werd niet bevraagd of deze doelstelling concreet of eerder zeer algemeen geformuleerd. 85% van de lokale besturen gaf aan dat ze al doelstellingen voorzien hadden.

Tijdens de diepte-interviews gaven de 45 lokale besturen aan dat – als er doelstellingen geformuleerd waren - deze doelstellingen vaak vrij breed geformuleerd waren zodat meerdere initiatieven van uiteenlopende aard hieronder konden geplaatst worden. Ze vermeldden ook dat het hebben van doelstellingen in bv. het Meerjarenplan wel als een ankerpunt fungeerde om ICT-gerelateerde beslissingen of -budgetten te kunnen laten goedkeuren. Enkele lokale besturen gaven aan dat het niet hebben van doelstellingen (bv. in het Meerjarenplan) er vaak toe leidde dat het nemen van ICT-gerelateerde beslissingen of het verkrijgen van budgetten bemoeilijkt werd.

vraag 8:

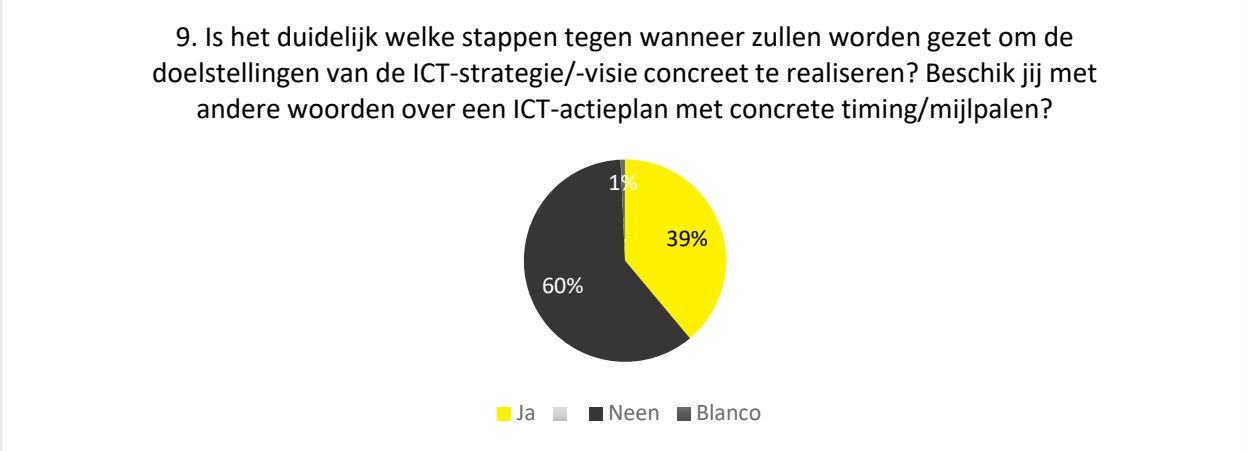
Lokale besturen formuleren een ICT-visie/strategie om een leidraad te hebben waarin de ICT binnen het lokaal in de eerstvolgende periode zal evalueren. Meestal is deze ICT-visie/strategie gekoppeld aan de doelstellingen die het lokaal bestuur formuleerde.
Van de 144 bevraagde lokale besturen gaf 46% aan te beschikken over een gevalideerde ICT-visie/strategie. 39% blijkt geen ICT-visie/strategie bepaald te hebben. Daarnaast gaf 15% het antwoord “andere” wat duidt op het mogelijk wel hebben van een ICT-visie/strategie zonder dat deze gedocumenteerd of gevalideerd is door de organisatie.

Lokale besturen die aangaven geen expliciete doelstellingen te hebben voor ICT of digitalisering hebben meestal ook geen gevalideerde ICT-visie/strategie. Wanneer er wel doelstellingen zijn vastgelegd, wordt dit niet altijd vertaald in of gekoppeld aan een ICT-visie/strategie voor het lokaal bestuur. Van de lokale besturen die wel doelstellingen bepaalden, heeft iets minder dan de helft geen ICT-visie/strategie opgemaakt.

Tijdens de diepte-interviews met de 45 lokale besturen werd dieper ingegaan op de ICT-visie/strategie. Een aantal verwees naar de doelstellingen als ICT-visie/strategie. De meerderheid had naast de doelstellingen een uitgeschreven en ICT-visie/strategie. Deze ICT-visie/strategie werd bij het ene lokale bestuur opgemaakt op basis van de doelstellingen, bij andere lokale besturen zorgde de bestaande ICT-visie/strategie voor het formuleren van de doelstellingen voor deze legislatuur. Wanneer de vraag gesteld werd of de bestaande ICT-visie/strategie periodiek geactualiseerd wordt, waren de antwoorden zeer uiteenlopend. Een aantal lokale besturen had een actualisatie nog niet voorzien, andere stuurden de ICT-visie/strategie continu bij. In uitzonderlijke gevallen was voorzien in een periodieke actualisatie gekoppeld aan een evaluatie en een overzicht van de realisaties.

De lokale besturen die tijdens het diepte-interview bevestigden dat ze over een ICT-visie/strategie beschikten, werd gevraagd om deze aan het auditteam te bezorgen. De meeste van de lokale besturen ging hierop in. De maturiteit van de ICT-visie/strategie werd op basis van de ontvangen documenten beoordeeld door het auditteam. Het resultaat daarvan is terug te vinden in het Globaal rapport "Thema-audit Beheer van ICT-risico's bij lokale besturen".

vraag 9:

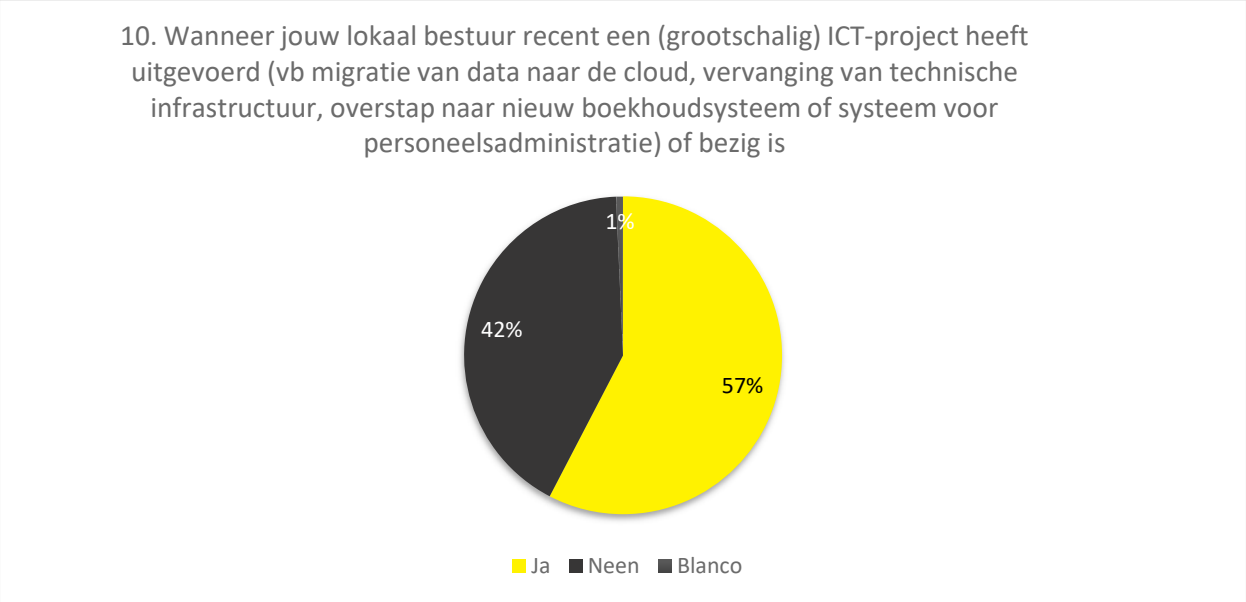


Om de ICT-visie/strategie in realiteit om te zetten zullen acties gepland en uitgevoerd moeten worden. 39% van de 144 lokale besturen gaf aan dat ze hiervoor een concreet actieplan met mijlpalen en een timing hadden uitgewerkt. In de meerderheid van de lokale besturen was dit echter niet voorzien.

Lokale besturen die geen doelstellingen voor ICT en digitalisering bepaald hadden, hadden bijna nooit een actieplan uitgewerkt. Wanneer ze wel een actieplan hadden dan hadden ze meestal ook een ICT-visie/strategie bepaald.
Lokale besturen die doelstellingen bepaalden voor ICT en digitalisering, had minder dan de helft een actieplan uitgewerkt. Van de lokale besturen die doelstellingen en ook een ICT-visie/strategie bepaalden had meer dan de helft een actieplan ter beschikking.

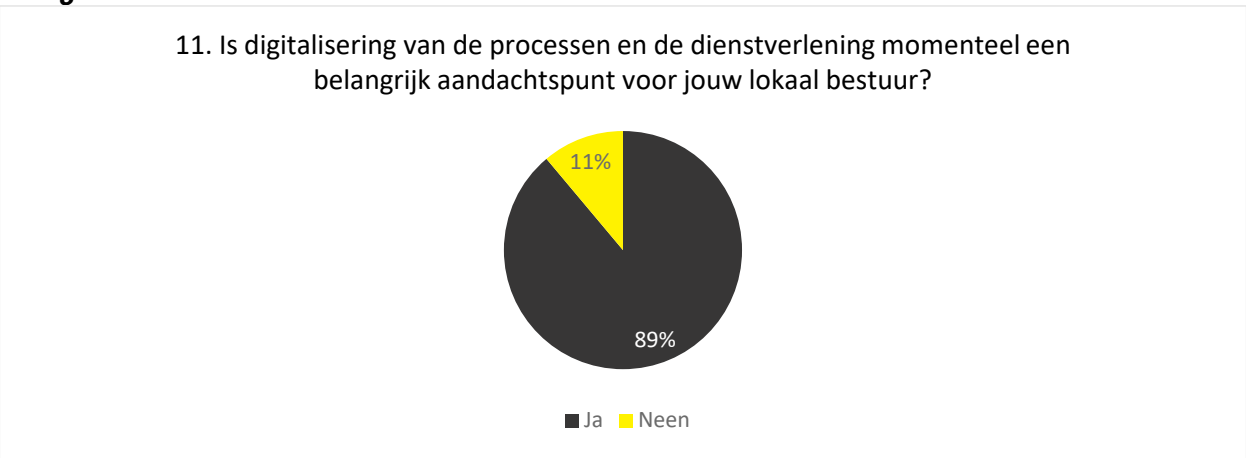
IV. Strategie voor digitale transformatie en innovatie in ICT

vraag 10:



Veranderingen als gevolg van een nieuw uitgevoerd ICT-project, maar ook even goed een andere manier van werken of samenwerken met externen, kan ervoor zorgen dat er bepaalde risico's beheerst worden, maar andere risico's ontstaan (risicotransfer). Hetzelfde geldt door het uitbesteden van bepaalde taken. Met deze vraag werd getracht in te schatten of lokale besturen zich daarvan bewust zijn en daar actief meer rekening houden. 57% gaf aan de nieuwe risico's in kaart te brengen wanneer er een (grootschalig) project werd uit gevoerd. Evenwel 43% dit niet te doen of beantwoordde deze vraag niet.

vraag 11:



Bijna 90% van de 144 lokale besturen bevestigt dat digitalisering een belangrijk aandachtspunt te zijn.

Tijdens de diepte-interviews werd gepeild naar de ICT-projecten die de aflopen 3 jaar werden uitgevoerd door de 45 bevraagde lokale besturen of op dit moment lopende zijn. Hieruit blijkt dat tal van lokale besturen reeds inzetten op digitalisering. Zo blijkt dat:

- 20% een e-loket opzette, uitbreidde of vernieuwde;
- 36% had initiatieven genomen om het werken op afstand mogelijk te maken of te verbeteren;
- 51% werkte aan de (gedeeltelijke) digitalisering van een of meerdere processen;

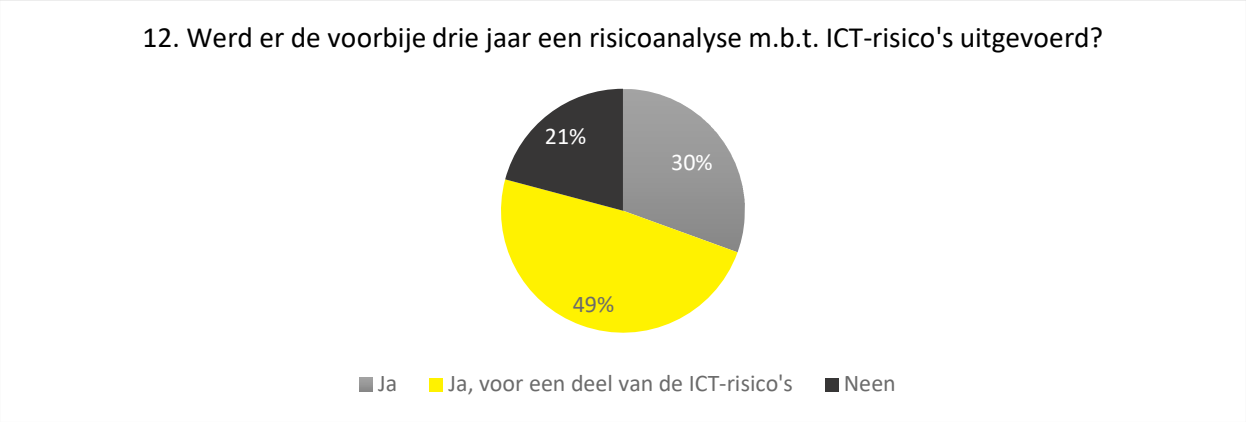
– 4% vermeldde de invoering de digitale handtekening of digitale notulering.

Andere projecten die aangehaald werden en die (mogelijk) inzetbaar zijn voor een verdere digitalisering van de werking: cloudmigratie (38%), vernieuwing infrastructuur (36%) en vernieuwing van een of meer softwarepakketten (36%).

De 45 lokale besturen werden daarnaast bevraagd over de acties die gepland waren voor de volgende jaren voor hun top 3 van risicodomeinen. Ook hier werden vaak digitaliseringsprojecten aangehaald.

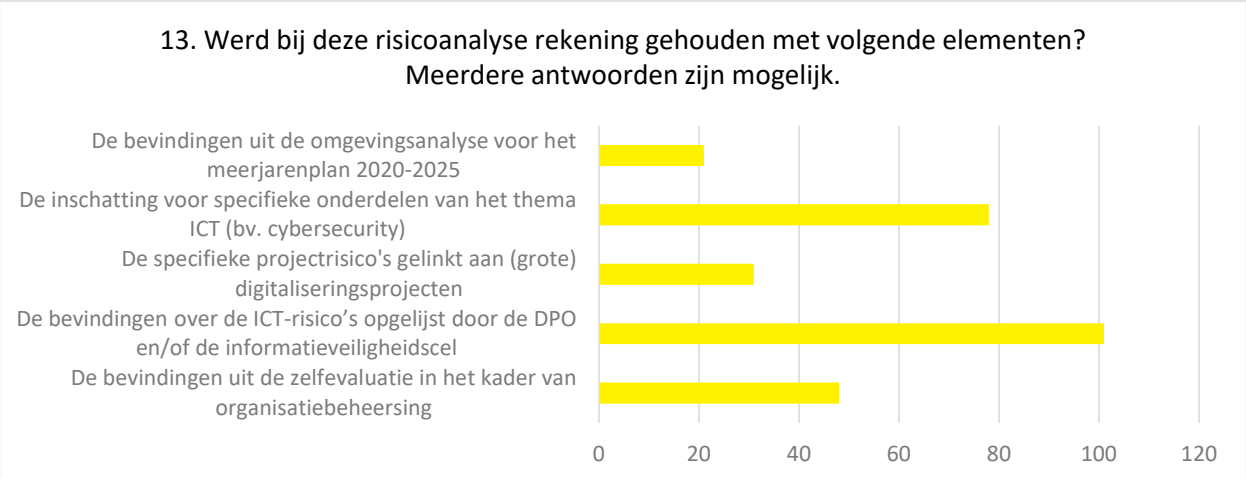
V. ICT-risicobeheer bij jouw lokaal bestuur

vraag 12:



De 144 lokale besturen werd gevraagd over het al of niet beschikbaar zijn van een recente ICT-risicoanalyse. Uit de antwoorden van de lokale besturen blijkt dat 79% van de lokale besturen beschikt over een risicoanalyse voor alle of een deel van ICT-risico's. 21% blijkt geen risicoanalyse te hebben.

vraag 13:



Uit de antwoorden van de 144 lokale besturen die wel over een risicoanalyse beschikten (79% van de 144), blijkt dat de meerderheid de ICT-risico's gerelateerd aan informatieveiligheid en voor specifieke onderdelen van het thema ICT in kaart gebracht heeft. Een beperkter aantal heeft ook het aspect organisatiebeheersing of specifieke project risico's mee in rekening gebracht.

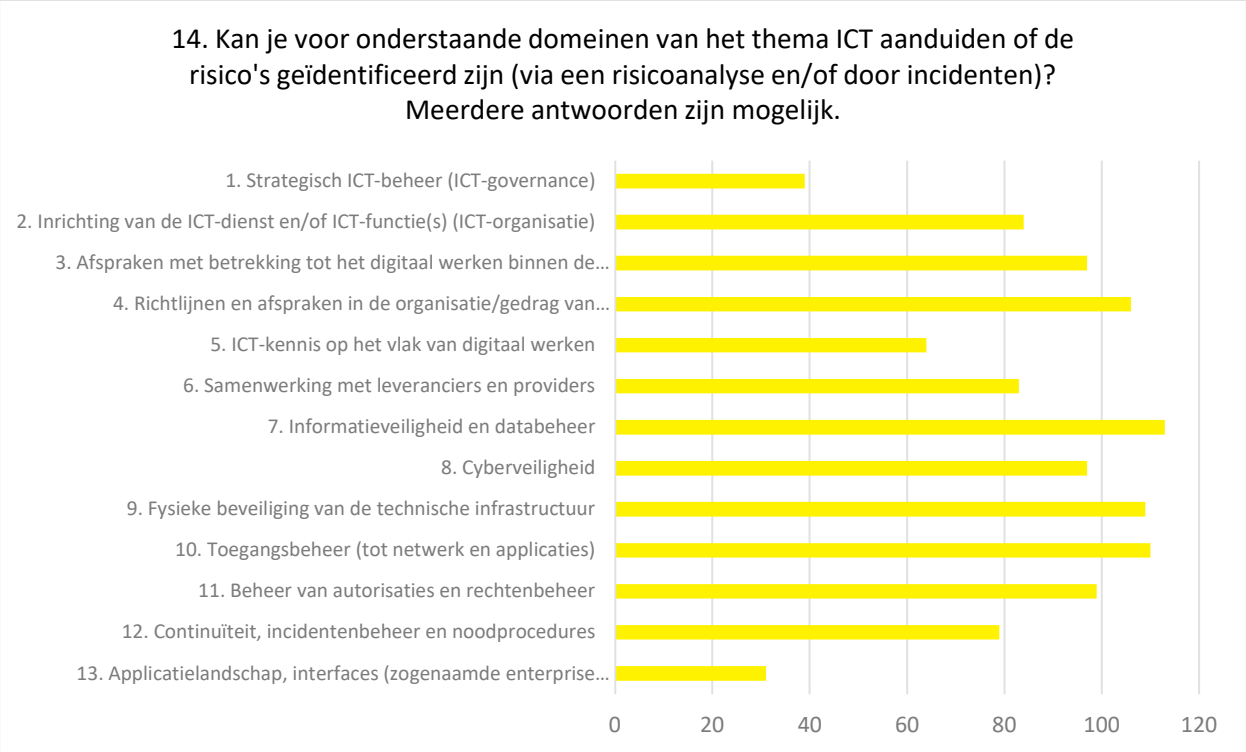
De diepte-interviews met 45 van deze lokale besturen lijkt deze tendens te bevestigen. In 58% van de gevallen de risicoanalyse is opgesteld in het kader van informatieveiligheid. Vaak is de functionaris voor gegevensbescherming (data protection officer of DPO) ook de coördinator voor de opmaak

ervan. In de andere gevallen werden werd aangehaald dat de risicoanalyse opgesteld binnen het kader van organisatiebeheersing 4%), door derde partij al dan niet in het kader van een thematisch audit (245%) of op initiatief van de ICT-verantwoordelijke (2%).

De meeste risicoanalyses bij de 45 bevraagde lokale besturen dateren van 2019 (42%). Een aantal beschikte over recentere risicoanalyses uit 2020 (22%) en 2021 (18%). Bij de overige lokale besturen was er geen risicoanalyse beschikbaar of was deze verouderd (voor 2018).

De 45 lokale besturen die tijdens het diepte-interview bevestigden dat ze over een risicoanalyse beschikten, werd gevraagd om deze aan het auditteam te bezorgen. De meeste van de lokale besturen ging hierop in. De maturiteit van de risicobeoordeling werd op basis van de ontvangen documenten beoordeeld door het auditteam. Het resultaat daarvan is terug te vinden in het Globaal rapport "Thema-audit Beheer van ICT-risico's bij lokale besturen".

vraag 14



Vervolgens werd aan de 144 lokale besturen gevraagd welke risico's uit de 13 opgesomde risicodomeinen reeds geïdentificeerd waren. Deze 13 risicodomeinen vertegenwoordigen slechts een beperkte set aan risicodomeinen voor ICT. Het zijn in hoofdzaak de organisatiebrede ICT-risicodomeinen, dus geen specifieke risico's die betrekking hebben op een bepaalde dienst, dienstverlening of 1 bepaalde applicatie van het lokaal bestuur. Deze vraag kon ook beantwoord worden door lokale besturen die op vraag 12 antwoordden dat ze niet over een risicoanalyse beschikten. Mogelijk werd bij deze lokale besturen reeds nagedacht over risico's, doch niet in de formele context van een risicoanalyse waardoor ze dan ook niet gedocumenteerd zijn.

Uit de antwoorden blijkt dat de lokale besturen aangaven dat ze reeds de risico's gerelateerd aan volgende risicodomeinen in kaart gebracht hadden:

- 58% voor risicodomein 2. Inrichting van de ICT-dienst en/of ICT-functie(s) (ICT-organisatie);
- 67% voor risicodomein 3. Afspraken met betrekking tot het digitaal werken binnen de organisatie (bv. opslag bestanden, communicatiekanalen, ...);

- 74% voor risicodomein 4. Richtlijnen en afspraken in de organisatie/gedrag van gebruikers/gebruik van internet en mobiele apparatuur;
- 58% voor risicodomein 6. Samenwerking met leveranciers en providers;
- 78% voor risicodomein 7. Informatieveiligheid en databeheer;
- 67% voor risicodomein 8. Cyberveiligheid;
- 76% voor risicodomein 9. Fysieke beveiliging van de technische infrastructuur;
- 76% voor risicodomein 10. Toegangsbeheer (tot netwerk en applicaties);
- 69% voor risicodomein 11. Beheer van autorisaties en rechtenbeheer;
- 55% voor risicodomein 12. Continuïteit, incidentenbeheer en noodprocedures.

De risico's uit de overige risicodomeinen zijn bij minder dan de helft van de lokale besturen in kaart gebracht.

Lokale besturen zijn reeds met risicobeheer bezig. Uit de online bevraging blijkt dat al meer dan de helft van de lokale besturen (58%) al minstens 8 of meer van deze 13 risicodomeinen in kaart gebracht te hebben. De risicodomeinen waarvan de risico's het vaakst in kaart gebracht zijn, blijken nauw verwant met digitale of fysieke beveiliging van data en infrastructuur (risicodomeinen 7, 8, 9, 10 en 11).

vraag 15:

De 144 lokale besturen werden bevraagd in welke mate de risico's gekoppeld aan deze 13 risicodomeinen afgedekt waren. Uit de antwoorden blijkt dat de risicodomeinen waarvoor ze de ICT-risico's het vaakst in kaart brachten dat deze als "voldoende afgedekt" ingeschat worden door de

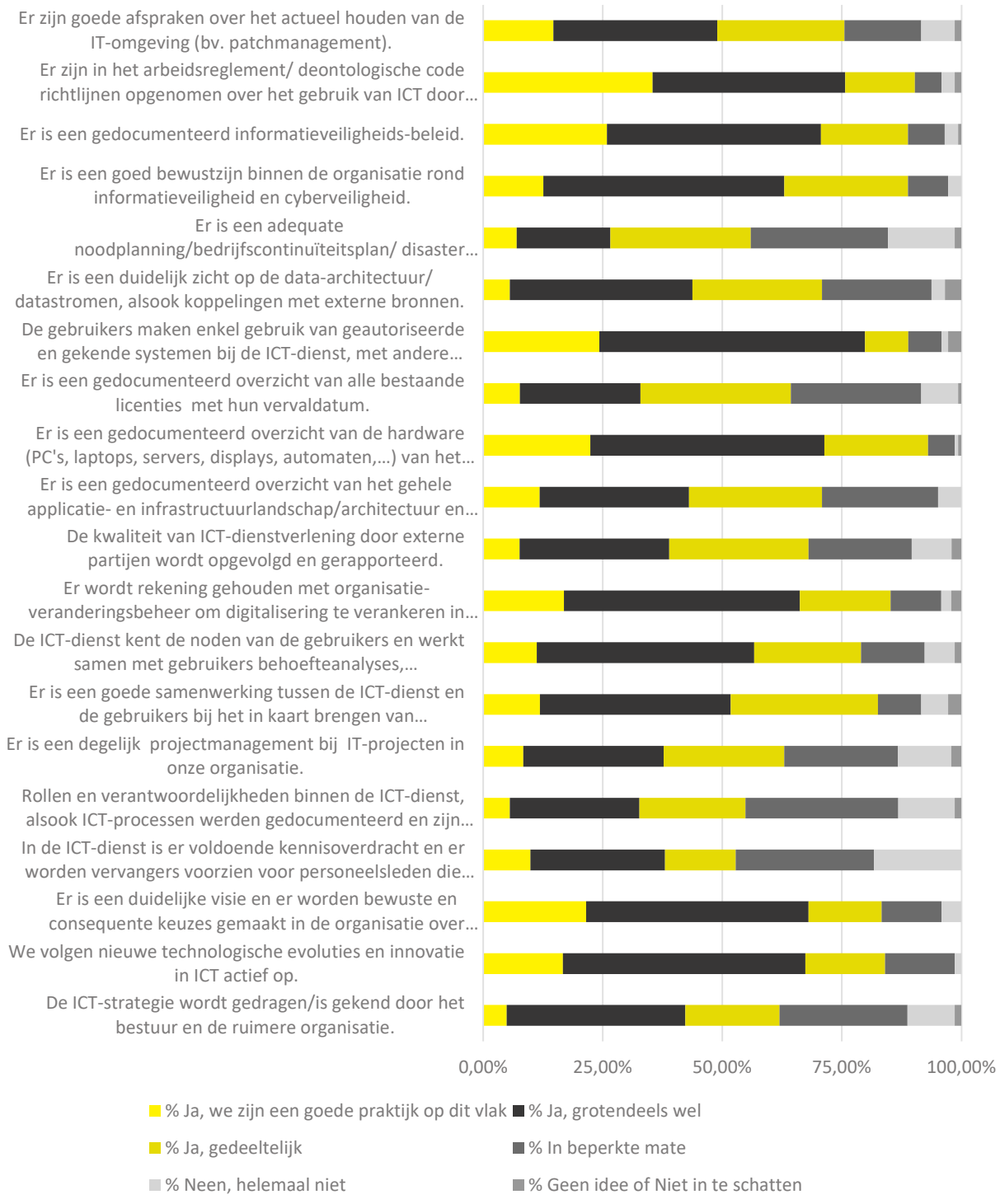
lokale besturen. Ook hier blijkt dat deze risicodomeinen nauw verwant zijn met digitale of fysieke beveiliging van data en infrastructuur (risicodomeinen 7, 8, 9, 10 en 11). Waarbij wel opvalt dat voor risicodomein 7 (informatieveiligheid en databeheer) en 8 (cyberveiligheid) er bij meer dan de helft nog belangrijke werkpunten zijn. Daarnaast blijkt risicodomein 4 (richtlijnen en afspraken in de organisatie/gedrag van gebruikers/gebruik van internet en mobiele apparatuur) bij meer dan de helft in geschat als voldoende afgedekt.
Evenwel schatten de lokale besturen in dat 9 van de 13 risicodomeinen onvoldoende beheerst of nog belangrijke werkpunten hebben.
Uit de diepte-interviews met 45 lokale besturen werd hen gevraagd aan te geven welke 3 van de 13 risicodomeinen de domeinen zijn die voor hen het belangrijkste waren.

VI. Inschatting van een aantal beheersmaatregelen

Een gedegen risicoanalyse is geen doel op zich en wint enkel aan waarde als er ook effectieve beheersmaatregelen worden gepland en uitgerold. In het kader van deze audit werd nagegaan in welke mate beheersmaatregelen werden uitgerold door de lokale besturen in de diverse risicodomeinen. Hiervoor werden 20 courante beheersmaatregelen gerelateerd aan de risicodomeinen (uit voorgaande vragen) voorgelegd aan de lokale besturen.

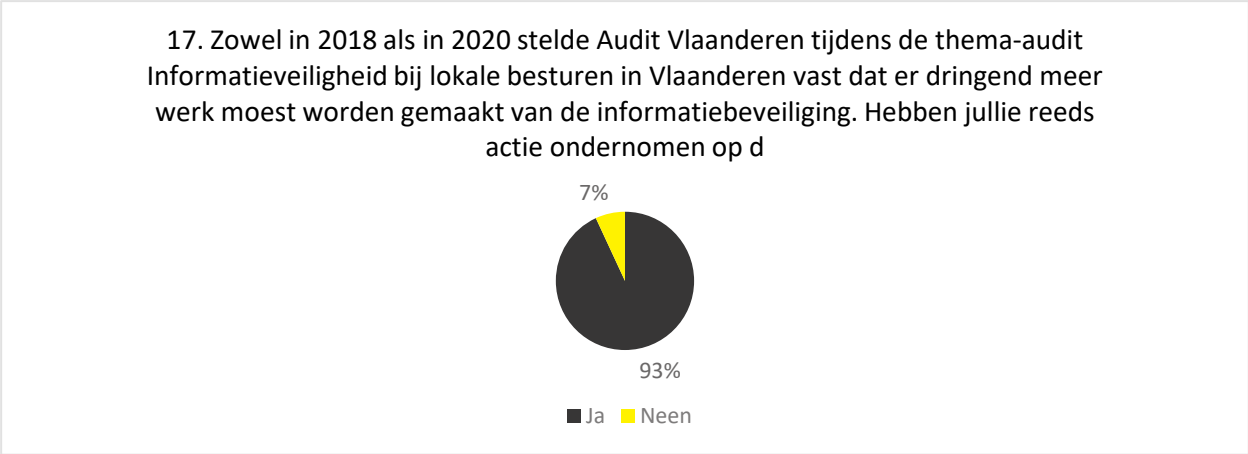
vraag 16:

16. Hieronder vind je een steekproef van beheersmaatregelen in het kader van ICTbeheer en risicobeheersing. Wij proberen een beeld te vormen van de mate waarin jouw organisatie deze beheersmaatregel al heeft geïmplementeerd. Kan je voor elk van de volgend



In de online bevraging werd de 144 lokale besturen gevraagd om voor 20 courante beheersmaatregelen om bepaalde ICT-risico's rond ICT-governance te beheren, in te schatten in hoeverre deze beheersmaatregelen al zijn geïmplementeerd in de lokale besturen. Uit de antwoorden blijkt dat voor nagenoeg alle beheersmaatregelen de lokale besturen aangeeft dat deze al minstens gedeeltelijk, grotendeels of volledig (zodat ze als goede praktijk kunnen aanzien worden) geïmplementeerd zijn in het lokaal bestuur. De vermelde beheersmaatregelen rond het bedrijfscontinuïteitsplan en kennisoverdracht aan personeelsleden worden het laagst ingeschat. Ze blijken bij slechts iets meer dan de helft van de lokale besturen als minstens gedeeltelijk geïmplementeerd te zijn.

vraag 17:



De globale rapporten van de thema-audits informatieveiligheid van Audit Vlaanderen werden in 2018 en begin 2021 verspreid naar de lokale besturen. Deze rapporten bevatten de auditbevindingen van een reeks individuele thema-audits bij lokale besturen samen. Hierbij blijkt dat voor het merendeel van de geauditeerde besturen informatieveiligheid (informatiebeveiliging) op meerdere vlakken een uitdaging is. Bijna alle lokale besturen gaven aan dat ze met deze informatie (aanbevelingen) aan de slag gingen om de informatiebeveiliging te verbeteren. Enkele lokale besturen bestelden een ICT-veiligheidsaudit, 134 gaven aan overige acties te hebben ondernomen, 10 lokale besturen[2] gaven aan geen acties te hebben ondernomen.

vragen 18 tot 20:

18. op welke wijze ging jouw lokaal bestuur hiermee aan de slag?
19. Waarom nam jouw lokaal bestuur geen actie?
20. Wat is er nodig om wel over te gaan tot actie?

Vervolgens werden aan de lokale besturen gevraagd hoe ze hiermee aan de slag zijn gegaan of waarom dat nog niet het geval was. De lokale besturen konden deze vragen vrij invullen of ze onbeantwoord laten. Op basis van de ontvangen antwoorden blijkt dat de lokale besturen die wel al aan de slag gingen met de aanbevelingen uit de globale rapporten van de thema-audits informatieveiligheid dit op diverse manieren hebben aangepakt. De meest uitgevoerde acties waren:

- een functionaris voor gegevensbescherming (dpo) aanstellen;
- een externe audit, onderzoek of testen op de ICT-systemen laten uitvoeren;
- een risicoanalyse uitvoeren;

[2] Tussen het moment van de online bevraging en de afwerking van dit globaal rapport hebben 4 van deze 10 lokale besturen een ICT-veiligheidsaudit met cofinanciering besteld.

- duidelijkheid verschaffen aan de medewerkers wat er van hen verwacht werd in het kader van informatieveiligheid (richtlijnen, arbeidsreglement, rechtspersoonlijkheidsregeling, sensibilisering);
- aanscherpen van het toegangsbeheer voor medewerkers;
- invoeren van een wachtwoordbeleid;
- opvolgen van leveranciers (contract, toegang, …).

Lokale besturen die nog niet aan de slag gingen met de aanbevelingen geven aan dat dit vooral te wijten is aan de omstandigheden en dat het door aanpassing van de planning nog niet gebeurd was. Om toch met deze aanbevelingen aan de slag te kunnen gaan, hadden ze meer tijd en resources nodig en ook een bijsturing van de huidige prioriteiten op het vlak van ICT. Dit sluit aan bij de algemene bevinding van deze audit dat de invulling van de ICT-functie bij lokale besturen vaak een structureel probleem is.

BIJKOMENDE INFORMATIE

vraag 21:

21. Zijn er volgens jou nog belangrijke organisatiebrede ICT-risico's die niet aan bod kwamen in de vragenlijst?

Op deze open vraag antwoordden slechts een beperkt aantal lokale besturen. Ze vermeldden hierbij volgende onderwerpen waarvan de organisatiebrede risico's nog onvoldoende aan bod kwamen:

- personeel en werkbelasting;
- werken op afstand;
- opvolging leveranciers;
- kostprijs voor ICT (hardware, software);
- omgang van de gebruikers met digitale tools.

vraag 22:

22. Zijn er goede praktijken die jouw lokaal bestuur wil delen met andere lokale besturen?

Op deze open vraag antwoordden slechts een beperkt aantal lokale besturen. Volgende antwoorden werden opgetekend bij een of meerdere besturen:

- voor de werking van de ICT-functie:
  - voldoende medewerkers voor de invulling van de ICT-functie
  - helpdeskopvolgingstoepassing;
  - beheerstool voor data in cloud
  - documenteer informatie, overzichten, procedures, processen, …
  - kennisdeling
  - trainingssoftware
- voor de infrastructuur en software pakketten:
  - ontdubbeling servers
  - NAC-systeem
  - datamigratie naar de cloud,
  - monitoring van het netwerk
  - gebruik van virtuele desktops
  - toegangsbeheer, multifactor-authenticatie
  - toegang voor thuiswerken
  - update van infrastructuur
  - overschakelen op O365
  - beheer van firewall

  - voor continuïteit dienstverlening en werking:
    - Backupbeheer
    - bedrijfscontinuïteitsplan
- voor werken met externe partijen:
    - opvolging samenwerking met externe partijen
    - opvolging accounts leveranciers
    - gebruik maken van raamcontracten
- voor gebruikers:
    - arbeidsreglement en deontologische code
    - reglement werken op afstand

vraag 23:

23. Heeft jouw lokaal bestuur vragen met betrekking tot ICT-risico's of -risicobeheer waarover je meer informatie wil?

Slechts enkele lokale besturen beantwoordden deze open vraag. Volgende onderwerpen waarover ze nog vragen hadden werden vermeld:

- impact op de organisatie en de ICT door het invoeren van O365;
- goede praktijk voor het benoemen en inschatten van ICT-risico's;
- het uitwerken van een goedwerkend bedrijfscontinuïteitsplan;
- de veiligheid en wettelijke conformiteit van cloudopslag;
- gebruiksgemak passwordless login (bv. biometrie) voor systeembeheerder.

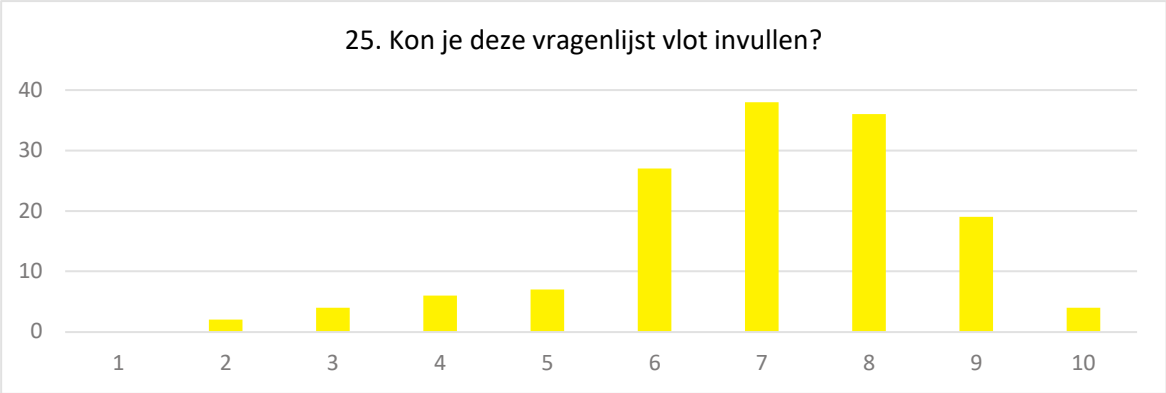
vraag 24:

24. Heb je nog andere bedenkingen of aandachtspunten die je wil delen met het auditteam?

Ook op deze open vraag werd slechts door enkele lokale besturen een antwoord ingevuld. Zij gaven volgende bedenkingen mee aan het auditteam:

- de risico's verbonden bij een overstap naar SharePoint;
- de valkuilen voor het uitbesteden van de server infrastructuur;
- aanpak van het menselijk gedrag en menselijke fouten is geen eenmalige inspanning, maar een continu proces;
- wettelijke verplichtingen inzake beheer en documentatie;
- SLA's en veiligheidsafspraken met leveranciers.

vraag 25:



Zeer moeilijk										zeer gemakkelijk
0	1	2	3	4	5	6	7	8	9	10

Meer dan de helft van de 144 lokale besturen gaven aan dat ze de online bevraging vlot kon invullen.

BIJLAGE 5: DE GEAUDITEERDE LOKALE BESTUREN

Audit Vlaanderen bevroeg in de periode november 2021-januari 2022 via een online bevraging 144 lokale besturen gespreid over Vlaanderen. Bij 45 van deze lokale besturen werd een diepte-interview afgenomen met de ICT-verantwoordelijke of andere medewerker(s) betrokken bij het beheer van ICT-risico's.
Hieronder een lijst van de lokale besturen per provincie. Bij de lokale besturen aangeduid met (*) werd een diepte-interview afgenomen.

provincie Antwerpen: 30 lokale besturen
- Arendonk (*)
- Baarle-Hertog
- Beerse
- Boechout
- Bonheiden
- Bornem (*)
- Brasschaat (*)
- Brecht
- Duffel
- Edegem (*)
- Grobbendonk (*)
- Heist-op-den-Berg
- Herentals (*)
- Herselt
- Hulshout
- Kapellen
- Lier
- Meerhout
- Nijlen (*)
- Putte (*)
- Puurs-Sint-Amands
- Ranst
- Retie
- Rumst
- Vorselaar (*)
- Vosselaar
- Wijnegem
- Willebroek
- Wommelgem
- Wuustwezel

provincie Limburg: 15 lokale besturen
- As
- Borgloon (*)
- Genk (*)
- Halen (*)
- Herk-de-Stad (*)
- Herstappe
- Hoeselt
- Houthalen-Helchteren (*)
- Kinrooi (*)
- Kortessem (*)
- Lummen
- Maasmechelen
- Tongeren (*)
- Voeren
- Zonhoven

provincie Oost-Vlaanderen: 23 lokale besturen

- Aalter
- Beveren
- Dendermonde (*)
- Evergem
- Gent (*)
- Geraardsbergen
- Haaltert
- Hamme
- Horebeke
- Kaprijke (*)
- Lede
- Lierde (*)
- Maarkedal
- Maldegem
- Melle
- Merelbeke (*)
- Ninove (*)
- Oudenaarde (*)
- Sint-Laureins
- Sint-Lievens-Houtem
- Wichelen (*)
- Zelzate (*)
- Zwalm

provincie Vlaams-Brabant: 39 lokale besturen

- Affligem (*)
- Asse (*)
- Beersel
- Begijnendijk
- Bertem
- Bever
- Bierbeek
- Boortmeerbeek
- Diest
- Dilbeek (*)
- Drogenbos
- Geetbets
- Haacht (*)
- Halle
- Herent
- Holsbeek
- Kampenhout (*)
- Kapelle-op-den-Bos
- Keerbergen
- Kortenberg
- Kraainem
- Lennik
- Linkebeek
- Linter (*)
- Londerzeel (*)
- Lubbeek
- Merchtem
- Opwijk
- Oud-Heverlee
- Pepingen
- Roosdaal (*)
- Sint-Genesius-Rode
- Steenokkerzeel
- Tervuren
- Tielt-Winge (*)
- Wezembeek-Oppem
- Zaventem (*)
- Zemst
- Zoutleeuw (*)

provincie West-Vlaanderen: 37 lokale besturen

- Alveringem
- Ardooie
- Avelgem
- Brugge
- De Haan
- Deerlijk (*)
- Dentergem
- Harelbeke
- Heuvelland
- Hooglede
- Ichtegem
- Jabbeke
- Koekelare
- Kortemark
- Kortrijk
- Langemark-Poelkapelle
- Ledegem
- Lo-Reninge (*)
- Menen (*)
- Mesen (*)
- Middelkerke (*)
- Moorslede
- Nieuwpoort (*)
- Oostende
- Oudenburg
- Pittem
- Poperinge (*)
- Roeselare
- Spiere-Helkijn
- Staden (*)
- Veurne
- Vleteren
- Waregem
- Wielsbeke
- Zonnebeke
- Zuienkerke
- Zwevegem

BIJLAGE 6: ICT-RISICO'S

Welke risico's in kaart brengen om als lokaal bestuur een voldoende zicht op alle actuele ICT-risico's te hebben ?

Niet-limitatieve lijst van mogelijke ICT-risico's :

- Risico's mbt het niet beschikken over een duidelijke ICT-visie/strategie op korte en langere termijn
  - as is situatie;
  - to be situatie en/of gewijzigde situatie.
- Risico's mbt technologische aspecten van cyberveiligheid (cybersecurity)
  - technisch;
  - toegangsbeheer;
  - bewustzijn gebruikers (ook informatieveiligheid).
- Overige risico's mbt informatieveiligheid
  - persoonsgegevens (Algemene Verordening Gegevensbescherming);
  - gevoelige gegevens.
- Risico's mbt ICT-infrastructuur, hardware en software
  - performantie;
  - compatibiliteit;
  - beheer ICT-middelen;
  - duurzaamheid en continuïteit.
- Risico's mbt samenwerking met externen (ruimer dan AVG en verwerkingsovereenkomst)
  - Wederzijdse verwachtingen, assumpties en afspraken.
  - Opvolging (incl. contractbeheer) van ICT-ondersteuning uitgevoerd door externen.
  - Opvolging (incl. contractbeheer) van ICT-leveranciers waarmee men een onderhoudscontract en/of SLA heeft afgesloten.
- Risico's mbt rollen en verantwoordelijkheden
  - intern versus extern;
  - competenties;
  - positionering ten opzichte van het managementteam.
- Risico's mbt infrastructuur- en architectuurkeuzes, technologische keuzes of vendor lock-in
  - op korte termijn;
  - op langere termijn.
- Risico's mbt de monitoring van de ICT-werking
  - performantie;
  - kosten;
  - planning.
- Risico's mbt de ondersteuning van de werking en dienstverlening
  - Afstemming op de werking en gebruiksvriendelijkheid.
  - Geïntegreerd of koppelbaar.

Welke randvoorwaarden zijn er voor een goede ICT-risicoanalyse ?

- voldoende actueel;
- voldoende afgestemd op de reële situatie in het lokaal bestuur (op maat);
- voldoende afgestemd op de organisatiedoelstellingen van het lokaal bestuur;
- wijzigingen aan infrastructuur, architectuur, werkmethodes, invulling ICT-functie, samenwerking met externen, … worden zo snel mogelijk erin verwerkt;
- goed gedocumenteerd;
- vertaald naar een concreet actieplan met prioriteiten en tijdspad.

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 beschikbaar op www.auditvlaanderen.be