Vlaamse overheid

Cyberveilige gemeenten

ICT-veiligheidsaudits met cofinanciering
Globaal rapport 2020-2022

144 lokale besturen

AUDIT
VLAANDEREN

Agenda

1. Over de ICT-veiligheidsaudits
2. Globale resultaten uitgevoerde testen
3. Globale resultaten bedrijfscontinuïteitsplan
4. Globale resultaten zicht op de ICT-risico's
5. Globale resultaten aanpak organisatiebeheersing
6. Informatie en inspiratie

1. Over de ICT-veiligheidsaudits

Belangrijkste te beheersen risico's

Wanneer onvoldoende beveiligingsmaatregelen zijn getroffen bestaat het risico dat met een beperkt aantal middelen of informatie (bv geslaagde phishing aanval) toegang tot het netwerk en de informatie van het lokaal bestuur wordt verworven om vervolgens het netwerk over te nemen of te beschadigen en/of informatie te stelen of te beschadigen.

Wanneer het IT-netwerk onvoldoende beschermd wordt (bv. firewall, sterke wachtwoorden, multifactor authenticatie, beperking op inlogpogingen, ..) bestaat het risico dat onbevoegden van buitenaf zich toegang verschaffen tot het netwerk van het lokaal bestuur om vervolgens het netwerk over te nemen of te beschadigen en/of informatie te stelen of te beschadigen.

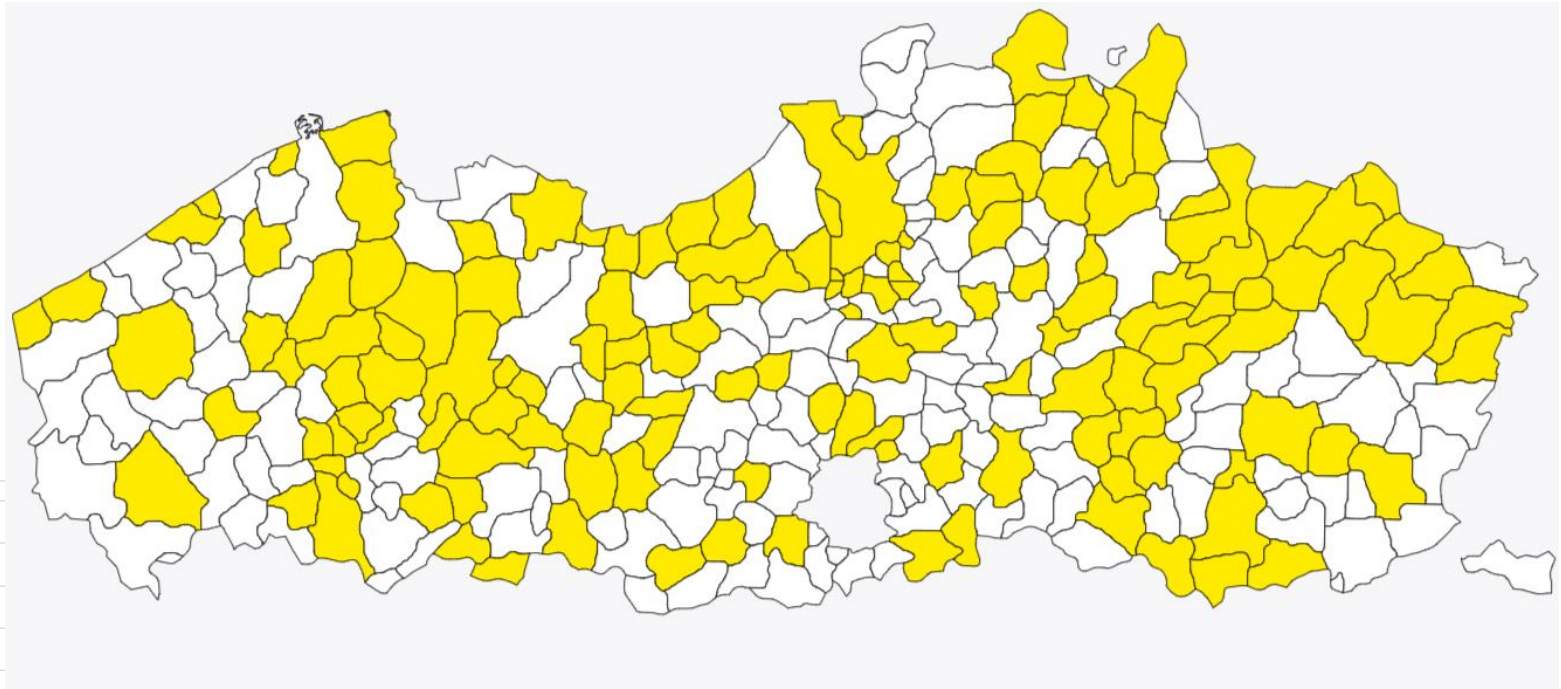
Wanneer het lokaal bestuur niet beschikt over een (bedrijfs- én ICT-)continuïteitsplan zijn de volgende risico's onvoldoende afgedekt:

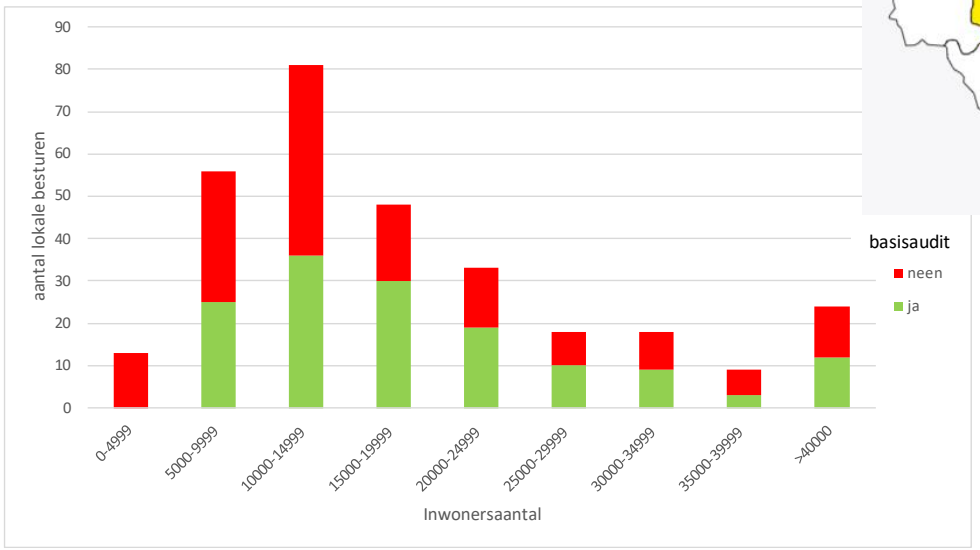
- Bij een incident kan het lokaal bestuur de continuïteit niet blijven garanderen omdat er geen procedures zijn voor het nemen van maatregelen bij een incident;
- De systemen van een lokaal bestuur zijn niet beschikbaar door een incident waardoor het lokaal bestuur haar werking niet kan verzekeren;
- Een adequaat herstel van de informatie na verlies, schade of diefstal kan niet worden gegarandeerd.

Door het ontbreken van een zicht op de ICT-risico's in een lokaal bestuur bestaat het risico dat de aanwezige beheersmaatregelen onvoldoende zijn en niet geëvalueerd kunnen worden om deze risico's te beheersen.

Door het ontbreken van een duidelijke aanpak voor de organisatiebeheersing wordt de werking onvoldoende in vraag gesteld en werkt een lokaal bestuur onvoldoende effectief, efficiënt, integer en kwaliteitsvol.

Bestelde en uitgevoerde ICT-veiligheidsaudits





144 lokale besturen bestelden een ICT-veiligheidsaudit met cofinanciering in de periode 2020-2023

AUDIT VLAANDEREN

Bestelde en uitgevoerde ICT-veiligheidsaudits

- Basisaudit :

  → 144 basisaudits uitgevoerd bij 144 lokale besturen

- Aanvullende audit :

  → 21 aanvullende audits bij 21 (van de 144 lokale besturen die een basisaudit lieten uitvoeren)

	Lokaal besturen (euro)	Vlaamse overheid (cofinanciering in euro)	Totaal (euro)
Basisaudits (144)	255.270,05	510.540,09	764.810,14
Aanvullende audits (21)	196.140,16	196.140,16	392.280,32

Inhoud basisaudit

Controleprogramma:

- **Interne penetratietesten op min. 3 systemen**
  Simulatie van een aanval van een kwaadwillend persoon op geselecteerde, via het interne netwerk benaderbare systemen. Hierbij werd enerzijds getest vanuit het perspectief van een aanvaller die toegang kan krijgen tot het interne netwerk zonder verdere rechten, anderzijds werd getest vanaf een gecompromitteerd werkstation of gebruikersaccount. Deze testen hebben als doel kwetsbaarheden te identificeren in beveiligingsmaatregelen getroffen op het niveau van het netwerk en besturingssysteem van deze systemen.
- **Externe penetratietesten op min. 3 systemen**
  Simulatie van een aanval van een kwaadwillend persoon op geselecteerde, via het Internet benaderbare systemen via beschikbaar gestelde IP-adressen en poorten van het lokaal bestuur. Deze testen hebben als doel kwetsbaarheden te identificeren in beveiligingsmaatregelen getroffen op het niveau van het netwerk en besturingssysteem van deze systemen. De test is 'black box' uitgevoerd (geen informatie betreffende de infrastructuur is op voorhand gedeeld).
- **Controle op het gebruik van zwakke wachtwoorden**
  Tijdens de toegangscontrole securitytest wordt een analyse uitgevoerd op de gebruikersaccounts van het lokaal bestuur. Deze test geeft een inzicht op de centraal beheerde accounts en hoe deze zijn beveiligd. Als deel van deze test wordt er ook gekeken of de gebruikte wachtwoorden gekende patronen bevatten.
- **Controle op het gebruik van zwakke wachtwoorden bij admin accounts**
  OF Controle op toegangen en rechten
  Test waarbij de actieve accounts op de active directory konden toegewezen worden aan personeelsleden in dienst bij het lokaal bestuur.

Inhoud basisaudit (vervolg)

Controleprogramma:

- **Nazicht op basis van aangeleverde documenten van het lokaal bestuur:**
  - → **Volwaardig ICT-bedrijfscontinuïteitsplan**
    Hierbij werd nagegaan of het bestuur beschikt over een bedrijfscontinuïteitsplan waarin ook de heropstart van het ICT-netwerk en toepassingen is voorzien. Een bedrijfscontinuïteitsplan stelt het bestuur in staat om na een incident op een adequate manier haar werking terug op te starten en de door haar beheerde informatie te herstellen.
  - → **Actueel en volledig zicht op de ICT-risico's**
    Hierbij werd nagegaan of het lokaal bestuur een volledig en actueel zicht heeft op de ICT-risico's binnen haar organisatie.
  - → **Aanpak organisatiebeheersing**
    Hierbij werd nagegaan of het lokaal bestuur beschikt over een adequaat en goedgekeurd kader voor organisatiebeheersing, over een recente organisatiebrede zelfevaluatie en op een degelijke manier jaarlijks rapporteert aan de raden over organisatiebeheersing.
- **Ondersteuning bij aanpakken vastgestelde kwetsbaarheden/risicobeheersing:** in te vullen op maat/vraag van het bestuur
  In overleg met het lokaal bestuur werd bepaald welke testen, ondersteuning, … met betrekking tot cyberveiligheid nodig had. De meeste lokale besturen opteerden voor een van volgende acties :
  - → Cyberawareness workshop voor leidinggevenden
  - → Uitwerken van een bedrijfscontinuïteitsplan
  - → Hertest van de interne of externe penetratietesten na het wegwerken van eerder gedetecteerde kwetsbaarheden.

Inhoud aanvullende audit

- **21 lokale besturen lieten (naast de basisaudit) ook nog een aanvullende audit aangepast aan de behoeften van het lokaal bestuur uitvoeren.**

- **Controleprogramma : verschillend per bestuur**
  - → Bewustzijn medewerkers onderzoeken
    bv. phishingtest, cybercrisis simulatie oefening
  - → Evaluatie van ICT-beleid en maatregelen
    bv. audit op basis van ISO27001/2 raamwerk
  - → Testen op het ICT-netwerk, verbindingen en beveiliging
    bv. netwerkarchitectuur, Wifi, cameranetwerk, IT-netwerkbeveiliging, …
  - → Ondersteuning ICT-dienst
    bv. opmaak disaster recovery plan, ondersteuning bij cyberincident

- **Door de diversiteit in uitgevoerde aanvullende audit kunnen geen algemene trends in de resultaten weergegeven worden.**

2. Globale resultaten testen uitgevoerd in 2020-2022

Resultaten basisaudits

Resultaten voor 144 lokale besturen	Aantal systemen getest	Geen vastgestelde kwetsbaarheden	Laag risico Aantal kwetsbaarheden	Midden risico Aantal kwetsbaarheden	Hoog risico Aantal kwetsbaarheden
Interne penetratietesten	732 (gemiddeld 5,1)	Bij 0 lokale besturen	797 (gemiddeld 5,5)	1197 (gemiddeld 8,3)	682 (gemiddeld 4,7)
Externe penetratietesten	483 (gemiddeld 3,4)	Bij 12 lokale besturen (waarvan 4 zonder extern bereikbare systemen op het ogenblik van de testen)	505 (gemiddeld 3,5)	157 (gemiddeld 1,1)	126 (gemiddeld 0,9)

Een aantal lokale besturen maakten gebruik van de ruimte voor maatwerk binnen de basisaudit om een hertest op de geteste systemen te laten uitvoeren nadat ze een aantal aanpassingen deden aan de interne en externe systemen binnen de looptijd van de audit. Hieruit bleek dat een significante vermindering van de kwetsbaarheden werd vastgesteld.

Gemiddeld : gemiddeld per lokaal bestuur

Resultaten basisaudits

Resultaten	Test uitgevoerd (aantal lokale besturen)	Test stelde geen zwakheden vast (aantal lokale besturen)	Gemiddeld % per lokaal bestuur
Zwakke wachtwoorden	107 lokale besturen (waarvan het wachtwoordbeleid een minimale sterkte vooropstelt)	1 lokaal bestuur	Gemiddeld 46,04 % (min. 0% - max 84%)
Zwakke wachtwoorden admin accounts	90 lokale besturen	6 lokale besturen	Gemiddeld 32,24% (min. 0% - max 67%)
Actieve accounts die niet gekoppeld kunnen worden aan iemand op de personeelslijst	53 lokale besturen	0 lokale besturen	Gemiddeld 25,04% (min. 0,24% - max 69%)

Beheersmaatregel “Beperking op inlogpogingen” vastgesteld bij 20 lokale besturen

AUDIT VLAANDEREN

Resultaten basisaudits

Resultaten voor 144 lokale besturen	**Heel wat zinvolle beheersmaatregelen worden onvoldoende benut**

- Actueel houden van IT-systemen
- Multifactor-authenticatie bij inloggen
- Beperken van toegang tot beheerdersinterfaces
- Netwerkbeveiliging, bv. door netwerksegmentatie

3. Globale resultaten bedrijfscontinuïteitsplan in 2020-2022

Resultaten basisaudits

Resultaten voor 144 lokale besturen	Volwaardig en actueel BCP	Elementen van een BCP	Geen BCP beschikbaar
Bedrijfscontinuïteitsplan (BCP)	0,7%	18,1%	81,3%

22 (van de 144) lokale besturen maakten van de ruimte voor maatwerk binnen de basisaudit gebruik om een BCP te laten opstellen.

Wanneer een lokaal bestuur over een volwaardig en actueel ICT-bedrijfscontinuïteitsplan is het lokaal bestuur beter gewapend om op een snelle en efficiënte manier haar werking opnieuw op te starten na het uitvallen van het ICT-netwerk als gevolg van een incident (bv. cyberaanval), evenals een adequaat herstel van de informatie na verlies, schade of diefstal.

4. Globale resultaten zicht op de ICT-risico's in 2020-2022

Resultaten basisaudits

Resultaten voor 144 lokale besturen	Volledig	Gedeeltelijk	Onvoldoende/Niet (of geen info verstrekt)
ICT-risico's in kaart gebracht	7,6%	75,7%	16,7%

Lokale besturen hebben meestal een goed zicht op de ICT-risico's gekoppeld aan informatieveiligheid (cf. Algemene Verordening Gegevensbescherming). Evenwel zijn er toch nog een aantal andere belangrijke risico's die niet voldoende in kaart gebracht werden (bv. de opvolging van externe leveranciers)

Een onvoldoende degelijk en actueel zicht op alle ICT-risico's waarmee een lokaal bestuur geconfronteerd wordt, zorgt ervoor dat het lokaal bestuur moeilijk in staat is om in te schatten of de aanwezige beheersmaatregelen voldoende zijn deze risico's te beheersen.

6. Globale resultaten aanpak organisatiebeheersing in 2020-2022

Resultaten basisaudits

Resultaten voor 144 lokale besturen	Voldoende adequate aanpak	Gedeeltelijk adequate aanpak	Geen adequate aanpak (of geen info verstrekt)
Aanwezigheid minimale voorwaarden voor een gestructureerde aanpak organisatiebeheersing	31,9%	56,3%	11,8%

Lokale besturen met een betere score op de aanpak organisatiebeheersing hebben vaker een beter zicht op hun ICT-risico's.

Tijdens de ICT-veiligheidsaudits werd een beperkte evaluatie uitgevoerd op basis van documenten over de aanpak organisatiebeheersing (bv. aanwezigheid van een goedgekeurd kader, uitvoering zelfevaluatie en uitvoering jaarlijkse rapporteringsverplichting).

Een degelijke aanpak voor de organisatiebeheersing zorgt ervoor dat het lokaal bestuur de eigen werking regelmatig in vraag gesteld, risico's in kaart brengt, voldoende beheersmaatregelen invoert waardoor het lokaal bestuur haar eigen werking meer effectief, efficiënt, integer en kwaliteitsvol kan organiseren.

7. Informatie en inspiratie

Inspiratie om te werken aan organisatiebeheersing?

- Website Audit Vlaanderen: rapporten en publicaties
  - → Leidraad Organisatiebeheersing
  - → Globale rapporten (en bijhorende kennisdeling):
    Thema-audit Informatiebeveiliging 2017-2018
    Thema-audit Informatiebeveiliging 2020
    Thema-audit Beheer van ICT-risico's (2023)
  - → Nieuwsbrieven
  - → Publicaties (o.a. jaarverslag)
  - → …
- Goede praktijken (o.a. informatieveiligheid, bedrijfscontinuïteitsplan)
- Zelfevaluatie-instrumenten (o.a. ICT-risico's, budgetbeheer, aankoop – en contractbeheer)

Vlaamse overheid

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

AUDIT
VLAANDEREN