



Vlaamse
overheid

Cyberveilige gemeenten

**ICT-veiligheidsaudits met cofinanciering
Globaal rapport 2023-2025**



77 lokale besturen en 12 intercommunales

AUDIT
VLAANDEREN

AGENTSCHAP
BINNENLANDS
BESTUUR

Agenda

1. Over de ICT-veiligheidsaudits
2. Globale resultaten testen uitgevoerd in 2023 - 2025
3. Globale resultaten bedrijfscontinuïteitsplan in 2023 - 2025
4. 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 wachtwoorden eenvoudig kunnen achterhaald worden, is er een groter risico dat gebruikersaccounts overgenomen worden met alle bijhorende toegangen en rechten. Ook het gebruik van multifactorauthenticatie kan het risico op overname van accounts verminderen.



Wanneer kwetsbaarheden in de gebruikte ICT-systemen niet tijdig geïdentificeerd en beheerst worden, kunnen deze misbruikt worden om de werking te verstoren en/of om informatie te stelen.



Wanneer het lokaal bestuur niet beschikt over een bedrijfscontinuïteitsplan zijn de volgende risico's onvoldoende afgedekt:

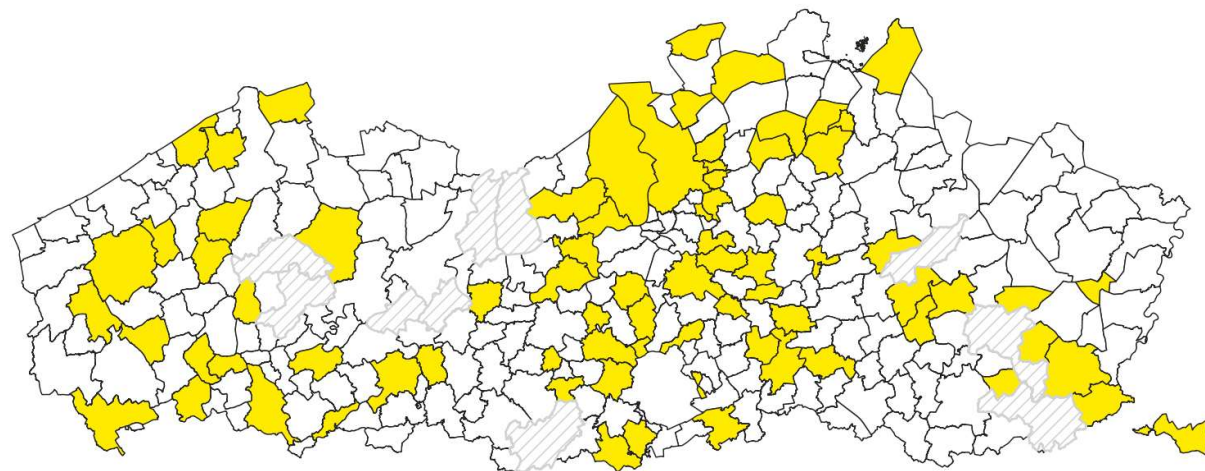
- Bij een incident kan het lokaal bestuur de continuïteit niet blijven garanderen omdat er geen procedures zijn voor het nemen van maatregelen bij een incident;
- De systemen van een lokaal bestuur zijn niet beschikbaar door een incident waardoor het lokaal bestuur haar werking niet kan verzekeren;
-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

Uitgevoerde ICT-veiligheidsaudits

77

LOKALE BESTUREN

Voerden een ICT-
veiligheidsaudit
met
cofinanciering uit



 Lokaal bestuur die
een ICT-audit liet
uitvoeren

 Fusiegemeente sinds 1
januari 2025

Daarnaast lieten
ook

12

Intercommunales

een ICT-
veiligheidsaudit
met
cofinanciering
uitvoeren.

Bestelde en uitgevoerde ICT-veiligheidsaudits

► Basisaudit:

→ 64 basisaudits uitgevoerd bij 52 lokale besturen en 12 intercommunales.

► Aanvullende audit:

→ 28 aanvullende audits bij 27 lokale besturen die eerder een basisaudit lieten uitvoeren.
Enkele lokale besturen lieten meer dan één aanvullende audit uitvoeren.

	Lokaal besturen (euro)	Vlaamse overheid (euro)	Totaal (euro)
Basisaudits (64)	127.632,44	255.264,87	382.897,31
Aanvullende audits (27)	220.977,86	220.977,86	441.955,72

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**

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.
- ▶ **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.

Merk op dat de technische elementen die opgenomen zijn in deze basisaudit maar een deel van de te beheersen ICT-risico's uitmaken en dat de beheersing van ICT-risico's maar een deel van de ruimere organisatiebeheersing uitmaakt. De evaluatie daarvan vereist een uitgebreidere audit dan waar in de periode 2023-2025 cofinanciering voor mogelijk was.

Inhoud aanvullende audit

- ▶ **27 lokale besturen lieten één (of meer) aanvullende audit(s) uitvoeren. In sommige gevallen waren die aanvullend op een basisaudit in de eerdere periode 2020-2022.**
- ▶ **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 audits kunnen geen algemene trends in de resultaten weergegeven worden.**



2. Globale resultaten testen uitgevoerd in 2023-2025

Resultaten basisaudits en hertest – Lokale besturen

Resultaten voor 70 lokale besturen	Aantal systemen getest (*)	Geen vastgestelde kwetsbaarheden	Laag risico Aantal kwetsbaarheden	Midden risico Aantal kwetsbaarheden	Hoog risico Aantal kwetsbaarheden
Interne penetratietesten	15.725 (gemiddeld 224,6)	Bij 0 lokale besturen	401 (gemiddeld 5,7)	850 (gemiddeld 12,1)	332 (gemiddeld 4,7)
Externe penetratietesten	154 (gemiddeld 2,2)	Bij 0 lokale besturen	259 (gemiddeld 3,7)	36 (gemiddeld 0,5)	21 (gemiddeld 0,3)

(*) In 2024-2025 zijn gemiddeld 224,6 interne en 2,2 externe systemen per lokaal bestuur getest.

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.

Resultaten basisaudits en hertest – Intercommunales

Resultaten voor 12 intercommunales	Aantal systemen getest (*)	Geen vastgestelde kwetsbaarheden	Laag risico Aantal kwetsbaarheden	Midden risico Aantal kwetsbaarheden	Hoog risico Aantal kwetsbaarheden
Interne penetratietesten	335 (gemiddeld 27,9)	Bij 0 intercommunales	60 (gemiddeld 5)	127 (gemiddeld 10,6)	49 (gemiddeld 4,1)
Externe penetratietesten	51 (gemiddeld 4,3)	Bij 0 intercommunales	38 (gemiddeld 3,1)	8 (gemiddeld 0,7)	2 (gemiddeld 0,2)

(*) In 2024-2025 zijn gemiddeld 27,9 interne en 4,3 externe systemen per intercommunale getest.

Resultaten basisaudits en hertest – interne en externe penetratietesten



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, ..) 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 kwetsbaarheden in de gebruikte ICT-systemen niet tijdig geïdentificeerd en beheerst worden, kunnen deze misbruikt worden om de werking te verstoren en/of om informatie te stelen.

Resultaten basisaudits en hertest – wachtwoorden

Resultaten uit 83 basisaudits of hertest	Aantal lokale besturen waar geen zwakheden werden vastgesteld	Gemiddeld % per lokaal bestuur
Zwakke wachtwoorden	0	Gemiddeld 30% (min. 4% - max. 81%)
Zwakke wachtwoorden admin accounts	29	Gemiddeld 18% (min. 0% - max. 64%)

Een goed wachtwoordbeleid legt verplichtingen op omtrent de minimale complexiteit en maximale geldigheidsduur van wachtwoorden. Door dergelijk wachtwoordbeleid technisch af te dwingen (samen met een aanpassing van de bestaande wachtwoorden en sensibilisering over hoe goede wachtwoorden kunnen worden bedacht), worden zwakke wachtwoorden tegengegaan.

Het beperken van inlogpogingen, het monitoren van potentieel gevaarlijk (aanmeld)gedrag en het gebruik van multifactorauthenticatie kunnen het risico op misbruik van accounts verder helpen beperken.



Wanneer wachtwoorden eenvoudig kunnen achterhaald worden, is er een groter risico dat gebruikersaccounts overgenomen worden met alle bijhorende toegangen en rechten. Ook het gebruik van multifactorauthenticatie kan het risico op overname van accounts verminderen.

Resultaten basisaudits en hertest

Resultaten voor
70 lokale besturen
en 12 intercommunales

Heel wat zinvolle beheersmaatregelen worden onvoldoende benut

- ▶ Actueel houden van IT-systemen
- ▶ Beperken van toegang tot beheerdersinterfaces
- ▶ Netwerkbeveiliging, bv. door netwerksegmentatie



3. Globale resultaten bedrijfscontinuïteitsplan in 2023-2025

Resultaten basisaudit en hertest

Resultaten voor 70 lokale besturen en 12 intercommunales	BCP beschikbaar	Geen BCP beschikbaar
Lokale besturen	41%	59%
Intercommunales	33%	67%

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.



Wanneer het lokaal bestuur niet beschikt over een bedrijfscontinuïteitsplan 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.

A man in a dark suit is shown from the chest up, holding a green pen in his right hand and gesturing with his left hand. He is wearing a black smartwatch on his left wrist. The background is a blurred green, suggesting an outdoor setting. A semi-transparent dark grey rectangular box is overlaid across the middle of the image, containing the text '7. Informatie en inspiratie' in yellow and white.

7. Informatie en inspiratie

Meer inspiratie om verder te werken aan organisatiebeheersing en digitale veiligheid?



01 Audit Vlaanderen

Rapporten, goede praktijken en zelfevaluatie-instrumenten voor sterke organisatiebeheersing.

[Kennisdeling vanuit audits | Audit Vlaanderen](#)

02 Agentschap Binnenlands Bestuur (ABB)

Faciliteert o.a. het delen van procesinformatie via het Open Proces Huis, met een procesinventaris, -bibliotheek en community van lokale besturen

[Open Proces Huis | Agentschap Binnenlands Bestuur](#)

03 Vlaams Centrum voor Digitale Veiligheid (VCDV) bij Digitaal Vlaanderen

Richtlijnen, toolboxen, sjablonen en diensten voor compliance, bewustzijn en preventie.

[Vlaams Centrum voor Digitale Veiligheid | Digitaal Vlaanderen](#)

COLOFON

VERANTWOORDELIJKE UITGEVER

Mark Vandersmissen
Administrateur-generaal Audit Vlaanderen

CONTACT

Audit Vlaanderen
Havenlaan 88
1000 Brussel
02 553 45 55

Deze publicatie is beschikbaar op www.auditvlaanderen.be

AUDIT
VLAANDEREN