Vlaamse overheid

ICT-veiligheidsaudits

Cyberveilige gemeenten

AUDIT VLAANDEREN

Wat komt aan bod?

1. Programma ‘cyberveilige gemeenten’
2. Inhoud van de ICT-veiligheidsaudits
3. We gaan ervoor… wat nu?
4. Veelgestelde vragen

Programma Cyberveilige gemeenten

CYBERVEILIGE GEMEENTEN

- een ICT-veiligheidsaudit voor alle gemeenten
- een digitale toolbox op maat

Waarom dit programma?

ISO27001/2 : raamwerk voor informatiebeveiliging

2016-2017-2018 : Thema-audit informatiebeveiliging lokale besturen

2017 : massale ransomware-aanvallen (o.a. Maersk)

2019 : opvolging aanbevelingen van o.a. de TA informatiebeveiliging

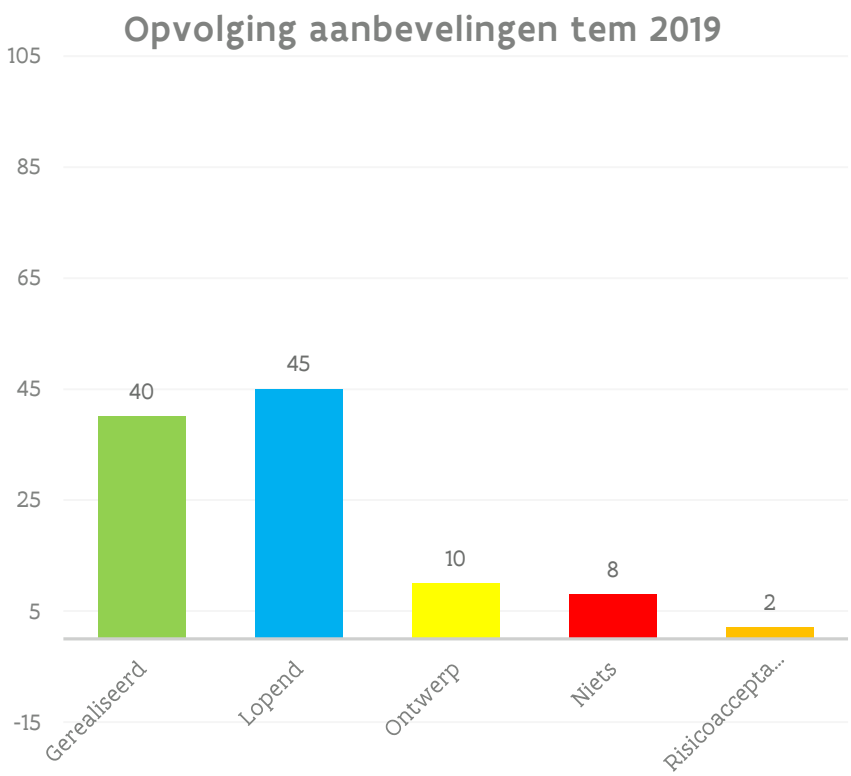
2020 : Thema-audit informatiebeveiliging 2020

2020 : Ransomware-aanval gemeente Willebroek

Resultaten thema-audit Informatiebeveiliging

Globaal rapport (bevindingen 2017-2018)

Beleid en organisatie	Informatiebeveiligingsbeleid
	Rollen en verantwoordelijkheden
	Leveranciersrelaties
	Naleving
Bewustzijn	Veilig personeel (bij en na indiensttreding)
	Omgang met digitale en papieren informatiedragers
Technisch beheer	Cryptografie
	Fysieke beveiliging
	Beveiliging van de IT-omgeving
	Netwerkbeveiliging
	Acquisitie, ontwikkeling en onderhoud van informatiesystemen
Logisch toegangsbeheer	Veilig personeel (bij en na uitdiensttreding)
	Beheer van bedrijfsmiddelen en classificatie van informatie
	Toegangsbeveiliging
Continuïteit	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
Incidentenbeheer	Informatiebeveiligingsincidenten beheren



Risico stijgt – actie nodig

COVID-19 vraagt buitengewone inspanningen van de overheden

- Maatschappij heeft grote behoefte aan goed werkende overheden
- Tegelijkertijd worden de overheden als organisatie geconfronteerd met de impact van de pandemie
  - O.m. massaal thuiswerk
  - Sterke verhoging van risico
- Grote afhankelijkheid van een goed functionerende ICT-omgeving
- Gecombineerd met nog belangrijke openstaande risico's n.a.v. audit informatiebeveiliging lokale besturen

Cybercriminelen verspreiden virussen en ransomware verborgen achter COVID-19 berichten e applicaties – safeonweb.be

De afgelopen week zijn er 44.000 phishingwebsites rond corona gecreëerd.
Geert Baudewijns
CEO bij Secutec

Politie.be
Omwille van de sterke stijging van valse berichten rond het coronavirus en de toename van het aantal valse berichten per sms, herhalen we de nationale sensibiliseringscampagne om de Belgische bevolking opnieuw te sensibiliseren voor phishing.

Werken op afstand maakt je kwetsbaar voor cybercriminelen - vlaio

Vlaamse overheid

AUDIT VLAANDEREN

Vlaamse regering biedt extra ondersteuning

Bart Somers
@BartSomers

Onze lokale besturen zijn cruciale actoren in het oplossen v/d crisis waarin we ons bevinden. We moeten kost wat kost vermijden dat zij nu slachtoffer worden van cybercriminelen. Daarom ondersteunen we hen met bijkomende middelen voor de veiligheid van hun ICT-systemen.

Agentschap Binnenlands Bestuur (ABB)
@ABB_Vlaanderen

De bescherming van gegevens is cruciaal bij een digitale werking en dienstverlening van lokale besturen. We maken daarom 2.000.000 euro aan extra middelen vrij voor audits en werken met @vvsg een toolkit voor maximale cyberveiligheid uit👉bit.ly/2VR45L4

Start van het Programma cyberveilige gemeenten

Op 30 april besliste de Vlaamse Regering op initiatief van minister Somers om bijkomende ondersteuning aan te bieden aan alle lokale besturen om hun cyberveiligheid aan te pakken.

Deze ondersteuning wordt gegroepeerd onder het programma ‘cyberveilige gemeenten’ en bestaat uit 2 sporen:

- de uitwerking van een actieplan cyberveiligheid onder coördinatie van de VVSG;
- cofinanciering voor het uitvoeren van een ICT-veiligheidsaudit in alle lokale besturen

Samenwerking voor sterke, cyberveilige Vlaamse steden en gemeenten!

AGENTSCHAP BINNENLANDS BESTUUR

Vlaamse overheid

vvsg

AUDIT VLAANDEREN

howest hogeschool

AGENTSCHAP FACILITAIR BEDRIJF

Actieplan cyberveiligheid

Initiatieven de komende 2 jaar (t.e.m. mei 2022):

- Traject ethisch hacken in lokale besturen (jaarlijks in het najaar) (in samenwerking met Howest)
- De ontwikkeling van een digitale toolkit cyberveiligheid (met een stuurgroep, klankbordgroep en taskforce)
- Informeren en inspireren via events (in samenwerking met partners, met een dedicated aanspreekpunt bij VVSG)

ICT-veiligheidsaudits met cofinanciering

AUDIT VLAANDEREN

- **Basisaudit** (minimaal):
  op basis van de belangrijkste kwetsbaarheden en quick wins
  met technische testen naar analogie van deze in de thema-audits
  beproefde aanpak gecoördineerd door Audit Vlaanderen
  2/3e cofinanciering vanuit Vlaamse overheid

- **Aanvullende audit** (optioneel):
  mogelijkheid om in functie van de eigen noden aanvullende
  auditwerkzaamheden m.b.t. ICT-veiligheid te bestellen
  50% cofinanciering vanuit Vlaamse overheid

Inhoud van de ICT-veiligheidsaudits

CYBERVEILIGE GEMEENTEN

- een ICT-veiligheidsaudit voor alle gemeenten
- een digitale toolbox op maat

Principes van de ICT-veiligheidsaudits

Een uniforme basisaudit voor elk lokaal bestuur.

Bestelling van 6 dagen + overkoepelende begeleiding Audit Vlaanderen = beperkte kost voor het bestuur:

- 1.817,02 euro Deloitte 0f
- 1.591,15 euro EY (of Grant Thornton).

Betaalbaar omdat de scope van de basisaudit beperkt is tot de belangrijkste risico's en het testwerk gebeurt op de relevantste systemen binnen de kern van het lokaal bestuur.

Cofinanciering voor aanvullende auditwerkzaamheden: voor extra ondersteuning en/of om in te kunnen spelen op specifieke situaties van lokale besturen.

Inhoud basisaudit

- **Zelfevaluatie**: gestructureerde vragenlijst die peilt naar de bestaande beheersmaatregelen binnen het bestuur m.b.t. ICT-risico's
- **Nazicht** bedrijfscontinuïteitsplannen, opvolging ICT-risico's en kader voor organisatiebeheersing
- **Technische testen**: kwetsbaarheidsscans intern en extern en check wachtwoordbeleid (cf. thema-audits informatieveiligheid)
- **Rapport** met bevindingen
- **1 dag begeleiding** zodat de ICT-verantwoordelijke kan samenzitten met een gespecialiseerd ICT-auditor om samen de meest prioritaire verbeteracties op te starten

Basisaudit - technische testen

Interne intrusietesten van de active directory-omgeving:

- maximaal 3 belangrijke systemen, te bepalen in overleg met het bestuur
- onderzoeken op aanwezige kwetsbaarheden
- aan de hand van technieken en tools voor netwerkmapping en kwetsbaarheidsanalyses (Nessus-scan)

Externe intrusietesten van maximaal 5 extern bereikbare IP-adressen:

- onderzoeken op aanwezige kwetsbaarheden zonder enige voorkennis
- aan de hand van technieken en tools voor kwetsbaarheidsanalyses

Basisaudit - technische testen

Testen van het wachtwoordbeheer, aanvullende authenticatiemechanismen en overkoepelend logisch toegangsbeheer

- niveau active directory en maximaal 2 kritische applicaties
- welke wachtwoordregels zijn ingesteld
- welke accounts een wachtwoord hebben dat niet aan deze regels voldoet of eenvoudig kan worden achterhaald
- welke multifactorauthenticatie wordt gebruikt
- nakijken van de actualiteit van de bestaande logische toegangen, die werknemers hebben op het overkoepelende niveau (active directory)

Aandacht voor netwerksegmentatie

Voor het uitvoeren van de technische testen wordt de opzet van het netwerk nagegaan, inclusief eventuele maatregelen m.b.t. netwerksegmentatie en/of intrusiedetectie.

Aanvullende audit

Volledig op maat van het bestuur

Voorbeelden van optionele aanvullende auditwerkzaamheden :

- interne kwetsbaarheidsscan van systemen in een afzonderlijk netwerksegment (bv. nog een afzonderlijk OCMW-netwerk)
- externe kwetsbaarheidsscan van nog meer extern bereikbare systemen
- uitvoeren van een analyse van logbestanden
- een audit op basis van de ISO27001-, ISO27002- en/of ISAE3000-raamwerken.
- Inhoud bepalen o.b.v. de vaststellingen uit de basisaudit
- …

ICT-veiligheidsaudits te midden een ruimer aanbod

Doel = verbetering bewerkstelligen => voorbereiding is nuttig, bv. via het ethische hacking-traject aangeboden via VVSG.

Tijdens de dag begeleiding kan concrete ondersteuning worden geboden en kunnen besturen die om hulp vragen, worden gewezen op andere ondersteuningsinitiatieven i.h.k.v. cyberveilige gemeenten.

Daarbij kunnen ook leveranciers, de digitale toolbox cyberveiligheid en de Vlaamse overheid een belangrijke rol spelen.

Na de gecofinancierde ICT-veiligheidsaudit is het nuttig om (periodiek) te checken of er nog problemen opduiken, bv. via het ethische hacking-traject aangeboden via VVSG.

Rol van Audit Vlaanderen

- Beschikbaar stellen van de raamovereenkomsten: uitvoering audits door externe auditfirma's
- Coördinatie van de basisaudits i.f.v. een uniforme aanpak
- Behandeling van de aanvragen voor cofinanciering voor basisaudits en aanvullende audits.
- Uitvoering van documentanalyse m.b.t. bedrijfscontinuïteitsplannen, opvolging van ICT-risico's en kader voor organisatiebeheersing.
- Geen audit van Audit Vlaanderen, bijgevolg zijn de traditionele rapporteringslijnen niet van toepassing. Het bestuur kiest zelf wie het rapport ontvangen.
- Audit Vlaanderen verzamelt alle bevindingen => bundelen van globaal beeld in globaal rapport, inclusief goede praktijken en aandachtspunten

We gaan ervoor...
Wat nu?

CYBERVEILIGE GEMEENTEN

- een ICT-veiligheidsaudit voor alle gemeenten
- een digitale toolbox op maat

Hoe bestellen?

Raamovereenkomst = enkel een goedgekeurde bestelbrief nodig!

Bestelprocedure:

Stap 1: contact opnemen met auditfirma (volgens rangschikking): nagaan mogelijke timing, nagaan belangenconflicten,...

Stap 2a: bestelbrief invullen = sjablonen gebruiken of eigen bestelbrief + verwijzen naar sjabloon + in bijlage mee opsturen

Stap 2b: goedkeuring volgens delegatieregeling eigen bestuur

Stap 3: bezorg de goedgekeurde bestelbrief aan:
ICT-veiligheidsaudits@vlaanderen.be

Stap 4: start audit

STAP 1 : contacteer de auditfirma('s)

Volgende raamovereenkomst is van toepassing:
2019/HFB/OP/52630 - bestek

Opgelet: het is mogelijk dat je moet inloggen voor je toegang krijgt. Indien er problemen zijn: contacteer dan Facilipunt (online https://overheid.vlaanderen.be/facilipunt, via 32000@vlaanderen.be of via 02 553 20 00).

⇒ Contacteer als 1e Deloitte
beauditvlcyber@deloitte.com (Jan Vanhaecht of Sara De Mulder)

⇒ Indien timing niet past of ze eigen werk zouden moeten auditeren: contacteer vervolgens EY

⇒ Indien ook bij hen timing niet past of ze eigen werk zouden moeten auditeren: contacteer vervolgens Grant Thornton

Voor details rangschikking + contactgegevens klik hier

STAP 1 : contacteer de auditfirma('s)

Te bespreken met auditfirma:

- gewenste timing
- mogelijkheden en timing aanvullende auditwerkzaamheden
- de kenmerken van de eigen ICT-omgeving (netwerksegmenten, aantal systemen, betrokken leveranciers en afspraken tussen bestuur en leveranciers over wie wat beheert, aantal extern bereikbare IP-adressen…
- praktische elementen, ook gelet op Covid-19
- … (wat je verder van vragen hebt)

⇒ De aanvullende audit moet niet samen met de basisaudit besteld worden. Het kan zinvol zijn om eerst de resultaten van de basisaudit af te wachten.

⇒ Ook stapsgewijs bestellen van aanvullende auditwerkzaamheden is mogelijk.

⇒ Let wel voor aanvullende audits: wanneer het krediet op is, is geen bijkomende cofinanciering meer mogelijk.

STAP 2 : regel de bestelling

Sjabloonbestelbrief bevat alle vereiste bepalingen.
-> Als je een eigen bestelbrief gebruikt, voeg dan de ingevulde sjabloonbestelbrief als bijlage toe om zeker te zijn dat niks werd vergeten.

Bestelgegevens van de verschillende firma's vind je hier terug.
De van toepassing zijnde dagprijzen (1 dag = 8u) vind je terug via deze link.

Berekening prijs basisaudit:
3 dagen A-/junior-profiel x dagprijs A-/junior-profiel
2 dagen B-/senior-profiel x dagprijs B-/senior-profiel
1 dag C-/manager-profiel x dagprijs C-/manager-profiel

Prijzen basisaudits

Overzicht van de betrokken auditfirma's en hun prijzen (afname moet in onderstaande volgorde gebeuren) – prijs is inclusief btw

Auditfirma (in cascade)	Door het lokaal bestuur te betalen voor een basisaudit	Totale kostprijs	Contactgegevens
Deloitte	1.817,02 euro	5.451,05 euro	beauditvlcyber@deloitte.com
EY	1.591,15 euro	4.773,45 euro	yannick.scheelen@be.ey.com
Grant Thornton	1.429,41 euro	4.288,24 euro	michael.eeckhaut@be.gt.com

Stap 2: regel de bestelling

Totaalbedrag op de bestelbrief!

Door toepassing gesplitste facturatie komt factuur voor 2/3e rechtstreeks bij Audit Vlaanderen en krijgt jouw bestuur een factuur voor slechts 1/3e van het totaalbedrag.

Voor **aanvullende auditwerkzaamheden** reken je analoog met het aantal dagen per profiel dat je wilt bestellen en ga je uit van 50% cofinanciering (factuur voor Audit Vlaanderen mits cofinanciering kan worden toegezegd en aan de voorwaarden wordt voldaan).

Bestellingen met cofinanciering zijn in principe mogelijk tot einde 2021

Goedkeuring bestelbrief volgens eigen delegatieregeling.

Stap 3 & stap 4

Stap 3: bezorg de goedgekeurde bestelbrief aan:
ICT-veiligheidsaudits@vlaanderen.be

Audit Vlaanderen antwoordt zo snel mogelijk over de toewijzing van de cofinanciering.

Stap 4: start audit:

- Obv de afgesproken timing met de auditfirma
- Bij de start van de audit:
  - ondertekenen van de afsprakennota tussen auditfirma en lokaal bestuur (minstens ondertekend door algemeen directeur)
  - via een link vul je de zelfevaluatie in
  - je bezorgt relevante documenten aan de auditfirma voor de documentanalyse
  - de nodige voorzieningen voor de hackers/IT-auditoren worden klaargemaakt tegen hun geplande bezoek

Facturatie

Audit Vlaanderen krijgt factuur voor bedrag cofinanciering

Lokaal bestuur krijgt factuur voor restbedrag

Veelgestelde vragen

CYBERVEILIGE GEMEENTEN

- een ICT-veiligheidsaudit voor alle gemeenten
- een digitale toolbox op maat

Moet een lokaal bestuur eerst toetreden tot de raamovereenkomst via een gemeenteraadsbeslissing vooraleer het mag bestellen?

Neen dit is niet nodig voor deze raamovereenkomsten.

- Sjabloon bestelbrief gebruiken of toevoegen aan eigen bestelbrief
- Bestelling intern laten goedkeuren conform de interne afspraken en delegaties voor het bestellen van diensten via een raamovereenkomst.

Je kan ook via deze raamovereenkomsten (ICT- e.a.) audits bestellen los van het programma Cyberveilige gemeenten – maar dan zonder cofinanciering.

Mag het lokaal bestuur rechtstreeks de auditfirma (volgens het cascadesysteem) contacteren voor een offerte voor de audit of verloopt dit via Audit Vlaanderen?

Ja. Het lokaal bestuur neemt zelf rechtstreeks contact op met de auditfirma om een basisaudit en/of aanvullende audit af te spreken. Audit Vlaanderen is daar als alles goed loopt niet bij betrokken.

Zijn de 6 dagen van de basisaudit aaneensluitend?
Dit is niet verplicht en wordt best afgesproken met de auditfirma.

Mijn lokaal bestuur heeft eind 2019 al een externe audit laten uitvoeren op vlak van cyberveiligheid. Kan het lokaal bestuur dit bv. in tweede helft van 2021 inplannen?
Ja, dat kan. De cofinanciering voor de ICT-veiligheidsaudits is mogelijk tot 31.12.2021.

Opgelet: voor de basisaudit blijft de cofinanciering zeker tot eind 2020 gegarandeerd (graag een seintje indien je deze nog in 2021 wil bestellen). Voor de aanvullende audit is dit afhankelijk van het resterend beschikbare budget op het moment dat er besteld wordt.

Worden er relevante aanbevelingen en praktisch bruikbare oplossingen aangereikt n.a.v. de bevindingen die uit de audit duidelijk worden?

Ja. In de basisaudit is één dag begeleiding voorzien om het lokaal bestuur te ondersteunen het zoeken naar oplossingen om de vastgestelde zwakheden weg te werken. Daarbij wordt zowel geput uit de technische expertise van de IT-auditoren als uit de digitale toolbox die wordt opgesteld door de initiatieven via VVSG.

Hoeveel aanvullende audits kan je bestellen?

Sowieso moet worden gestart met de basisaudit.

Daarbij of later – bv. afhankelijk van de bevindingen uit de basisaudit – kunnen aanvullende auditwerkzaamheden worden besteld.

Technisch is er geen probleem om de aanvullende auditwerkzaamheden in meerdere schijven te bestellen.

Het is wel mogelijk dat het cofinancieringsbudget na verloop van tijd uitgeput geraakt en er voor latere bestellingen geen cofinanciering meer mogelijk is.

Is deze ICT-veiligheidsaudit verplicht voor elk lokaal bestuur?

Neen. Het aanbod voor een ICT-veiligheidsaudit met cofinanciering is een aanbod, geen verplichting. Het aanbod om een ICT-veiligheidsaudit met cofinanciering te laten uitvoeren is een opportuniteit voor het lokaal bestuur en is tot 31.12.2021 beschikbaar.

Vlaamse overheid

Vragen Bedenkingen

?

De firma waar u de mogelijke bestelling mee bespreekt.

2e lijn: ICT-veiligheidsaudits@vlaanderen.be

lydia.putseys@vlaanderen.be
liesbeth.vanderstukken@vlaanderen.be
gunter.schryvers@vlaanderen.be

AUDIT VLAANDEREN