BK
BO

Bureau voor Kwaliteitsborging
bij de Overheid

Presentatie voor CISO netwerkdag SEP
24 mei 2023

Agenda

1. **Introductie BKBO bv**
2. Wat is er gebeurd in een notendop?
3. Wat gaat er veranderen?
4. Wat levert het ons op?
5. Frustraties van de auditor
6. Wat zouden we moeten doen?
7. Vragen, discussie

BK
BO
Bureau voor Kwaliteitsborging bij de Overheid

Introductie

Bureau voor Kwaliteitsborging Bij de Overheid bv

www.bkbo.nl info@bkbo.nl 073 – 211 03 37

- 11 medewerkers, waarvan 2 RE's, 4 CISA's
- Marktsegmenten: overheid, zorg en IT leveranciers
- Nichemarkt: standaard IT audits
- Ruim 230 klanten waarvan circa 60 gemeenten voor ENSIA, 100 gemeenten voor Wpg en 35 leveranciers

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Agenda

1. Introductie BKBO bv
2. **Wat is er gebeurd in een notendop?**
3. Wat gaat er veranderen?
4. Wat levert het ons op?
5. Frustraties van de auditor
6. Wat zouden we moeten doen?
7. Vragen, discussie

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Wat is er gebeurd in een notendop?

- ENSIA sinds 2017
- Audit is beperkt tot DigiD en Suwi
- Verticale en horizontale verantwoording staat centraal

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Agenda

1. Introductie BKBO bv
2. Wat is er gebeurd in een notendop?
3. **Wat gaat er veranderen?**
4. Wat levert het ons op?
5. Frustraties van de auditor
6. Wat zouden we moeten doen?
7. Vragen, discussie

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Wat gaat er veranderen?

DigiD:

- vanaf verantwoordingsjaar 2023 controle op werking voor 5 uitvoeringsnormen als proef en vanaf 2024 als verplichting
- Wettelijk verankerd; wordt veiligheidsaudit onder de Wdo

Suwi:

- mogelijk controle op werking

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Agenda

1. Introductie BKBO bv
2. Wat is er gebeurd in een notendop?
3. Wat gaat er veranderen?
4. **Wat levert het ons op?**
5. Frustraties van de auditor
6. Wat zouden we moeten doen?
7. Vragen, discussie

BK
BO
Bureau voor Kwaliteitsborging bij de Overheid

Wat levert het ons op? (1)

Voor verticale toezichthouders?

- Stelselverantwoordelijke BZK (Logius)
- Stelselverantwoordelijke SZW

Wat levert het ons op? (2)

Voor College van B&W:

- Verhoging van het niveau van beveiliging bij webapplicaties
- Wat inzicht in de informatiebeveiliging van de gemeentelijke ICT
- Schijnzekerheid

Wat levert het ons op? (3)

Neveneffecten

- webapplicaties zijn veel veiliger geworden
- alle cowboy aanbieders zijn verdwenen van de markt
- meer bewustwording
- meer grip op leveranciers
- steeds meer standaard en steeds meer SaaS
- kleinere rol functioneel beheer

Agenda

1. Introductie BKBO bv
2. Wat is er gebeurd in een notendop?
3. Wat gaat er veranderen?
4. Wat levert het ons op?
5. **Frustraties van de auditor**
6. Wat zouden we moeten doen?
7. Vragen, discussie

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Frustraties van de auditor?

- Veel administratieve rompslomp
- Gering lerend effect
- Geringe groei in volwassenheid
- Weinig samenwerking om tot verbetering te komen

Agenda

1. Introductie BKBO bv
2. Wat is er gebeurd in een notendop?
3. Wat gaat er veranderen?
4. Wat levert het ons op?
5. Frustraties van de auditor
6. **Wat zouden we moeten doe**
7. Vragen, discussie

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Wat zouden we moeten doen? (1)

- Het volwassenheidsniveau van informatiebeveiliging bij gemeenten versterken
- Een betere verdediging tegen ransomware bereiken
- Ons gezamenlijk voorbereiden op NIS2
- Het i-bewustzijn bij medewerkers en het management verhogen

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Wat zouden we moeten doen? (2)

Een volwassen organisatie wil haar IT beheersen, kan zelf beheersdoelstellingen bepalen, kan zelf beheersmaatregelen bepalen, kan zelf meten of deze doelstellingen worden behaald.

En heeft alleen een IT auditor nodig om bestuur/inwoners/klanten/toezichthouders zekerheid te geven dat het ambtelijk zelfbeeld volledig en correct is.

BKBO
Bureau voor Kwaliteitsborging bij de Overheid

Wat zouden we moeten doen? (3)

Dus: waarom niet samen met gemeente, VNG, toezichthouders en auditors het volwassenheidsniveau van individuele gemeenten bepalen en vervolgens via een cafetariamodel het niveau van verantwoording zo modelleren dat de goede gemeenten beloond worden en de zwakkere broeders/zusters extra verplichtingen krijgen opgelegd?

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Wat zouden we moeten doen? (4)

Of: de sterke gemeenten voor een vergelijkbaar bedrag op andere voor de organisatie zelf meer relevante items toetsen in plaats van de huidige toetsing

Zoals een netwerkaudit en scan, beoordeling segmentatie, inrichting en veiligheid LAN en Wifi, offsite back-up etc

Als belangrijke verdedigingslinie tegen ransomware aanvallen

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Wat zouden we moeten doen? (5)

Of: relatie leggen met NIS2 die een hoger niveau van cyberbeveiliging voorschrijft voor de lokale overheid

In de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) is het aan de Rijksinspectie Digitale Infrastructuur om het toezicht te regelen

Mijn verwachting is dat het toezicht arrangement van DigiD ook hier wordt ingezet

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Agenda

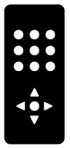
1. Introductie BKBO bv
2. Wat is er gebeurd in een notendop?
3. Wat levert het ons op?
4. Frustraties van de auditor
5. Wat zouden we moeten doen?
6. **Vragen, discussie**

BK BO
Bureau voor Kwaliteitsborging bij de Overheid

Vragen en discussie?

Meer informatie

Check onze website www.bkbo.nl



Bel 073 -211 03 37

Of stuur een mailtje met je vraag naar info@bkbo.nl

BK BO
Bureau voor Kwaliteitsborging bij de Overheid