Vlaamse overheid
Havenlaan 88 bus 100
1000 Brussel

VERSLAG

VERGADERING AUDITCOMITE VAN DE VLAAMSE ADMINISTRATIE VAN 7 MAART 2023

Plantentuin Meise – Vlaamse Hoeve 12.30-18.00 uur

Namen deel:

Johan Christiaens (JC)
Miet Vandersteegen (MV)
Martin Ruebens (MR)
Wies Herpol (WH)
Lieze Moeyersons(LM)
Iwona Muchin (IM)
Steven Dessein (SD) – Plantentuin Meise
Mark Andries (MA), administrateur-generaal VLAIO en voorzitter Stuurorgaan Vlaams Informatie- en IT-beleid
Fatima Zohra Amziab - Audit Vlaanderen (AV)
Inge Blauwhoff - Audit Vlaanderen (AV)
Lien Boutsen - Audit Vlaanderen (AV)
Karel Bruneel - Audit Vlaanderen (AV)
Maarten Deboosere - Audit Vlaanderen (AV)
Erwin Driessen - Audit Vlaanderen (AV)
Karen Peleman - Audit Vlaanderen (AV)
Patricia Van de Capelle - Audit Vlaanderen (AV)
Jo Fransen - Audit Vlaanderen (AV)
Mark Vandersmissen - Audit Vlaanderen (AV)

Voorzitter: Jean-Pierre Garitte, voorzitter auditcomité Vlaamse Administratie (JPG)
Secretaris: Joris Scheers, Departement Kanselarij en Buitenlandse Zaken (DKBUZA)

0. Inleiding

De voorzitter en Mark Vandersmissen heten iedereen welkom en geven duiding bij het opzet van de vergadering. Dank aan Steven Dessein, CEO van de Plantentuin, die meteen het woord krijgt.

1. Toelichting Plantentuin Meise

SD geeft een uiteenzetting over de historiek, de werking, planning, organisatiebeheersing, risicomanagement en het auditgebeuren van de Plantentuin Meise.

Er volgt een vragen- en reflectieronde over volgende mogelijke verbeterpunten die SD aanreikt:

- De nood aan een beter uitgewerkt kader voor risicomanagement binnen de VO. De huidige toolbox is beperk, waar er bij de leidraad organisatiebeheersing meer instrumenten beschikbaar waren)
- Betere doorstroming van risico's en beheersmaatregelen van diensten waarvan entiteiten gebruik moeten van maken (DCB, AGO, selectie en rekrutering,...)
- VO-brede risico's op een hoger niveau aanpakken (cybersecurity, war for talent,...), cf. globaal risicomanagement.

Daarnaast kwam het vrijwilligersbeleid en de daarmee gepaard gaande risico's aan bod en werd ook stilgestaan bij de link met de politieke besluitvorming.

2. Toelichting en bespreking globale resultaten beleidsgerichte rapporten 2022

AV geeft een toelichting, waarbij de volgende onderdelen aan bod komen:

1° het doel en het verloop van de aanpak van de beleidsgerichte rapporten

2° de globale VO-brede resultaten op basis van de resultaten van de beleidsgerichte rapporten:

- Enkele algemene trends inzake risicomanagement en de realisatie van aanbevelingen
- Zes vastgestelde transversale knipperlichten:
    - Het bestaan van 'high risk' entiteiten te wijten aan o.a. fusies en reorganisaties
    - Kwetsbaarheid voor security incidenten
    - Nevenprocessen bij dienstencentra zijn vaak onvoldoende onder controle
    - Ketenprocessen zijn sterk vatbaar voor risico's
    - Cruciaal belang van tone @ the top
    - Te weinig gedeelde risico-acceptatie politiek – administratie

3° toekomstperspectief van de beleidsgerichte rapporten

- Welke lessen trekt AV uit de opmaak van de beleidsgerichte rapporten en waar zet AV verder op in

De toelichting sluit af met enkele verwachtingen en vragen voor het ACVA.

JPG dankt AV voor dit bijzonder interessant overzicht en geeft aan dat op basis van de geformuleerde bevindingen een verdere reflectie en bespreking zal volgen.

Er wordt even stil gestaan bij de werking van het Vlaams IT-stuurorgaan, met verwijzing naar bestaande kaders, een begeleidende WIKI-omgeving en het dashboard.

LM stelt vast dat de aanpak binnen de verschillende entiteiten sterk verschilt en wijst op de rol van de leidend ambtenaren ter zake. Het overzicht is interessant en geeft focus mee. Ook de knipperlichten vragen aandacht.

LM vraagt welke impact deze resultaten hebben op zowel de auditcapaciteit van AV als op het te auditen veld van entiteiten. AV geeft aan dat dit deel uit maakt van de courante opvolging.

JC benadrukt het sterke punt van het helikopterzicht, net als de zeer waardevolle ketenbenadering (transversale audits).

Er ontstaat een gedachtewisseling over de impact van fusies.

JPG merkt op, dat naast het risicobeheer zelf, ook de identificatie ermee daalt, wat merkwaardig te noemen is. Hij vraagt zich af of dit dan aan de fusieoperatie ligt.

LM geeft aan dat de *'tone at the top'* hier zeer belangrijk is, net als de rol van de ankerpunten die dit binnen de organisatie opnemen.

JPG stelt dat gedeeld risico een belangrijk aandachtspunt is dat verder moet worden besproken. Het beeld van risicomanagement is nl. verschillend bij leidend ambtenaren en politici, gelet op de verschillende horizon.

JPG stelt dat het goed is te mikken op de implementatie van de aanbevelingen.

De bespreking en discussie zal verdergezet worden op de vergadering van het auditcomité van de Vlaamse administratie van 30 maart 2023.

3. Toelichting door Mark Andries, administrateur-generaal VLAIO en voorzitter Stuurorgaan Vlaams Informatie en IT-beleid

MA geeft een presentatie over de eerdere fusies, de werking, planning, organisatiebeheersing en het auditgebeuren bij VLAIO. Hij staat ook even stil bij het stuurorgaan en eindigt met 5 stellingen voor gedachtewisseling:

- Bij de Vlaamse overheid is er een goed evenwicht tussen operationele autonomie en aanspreekbaarheid van het management
- Het is mogelijk om inzake organisatiebeheersing ambitieus én pragmatisch te zijn
- Bezig zijn met de risico's van je organisatie, je proces, je project,…is nodig maar ook moeilijk
- "single audit" is tot nu toe een illusie gebleken
- Er is nood aan een lerend netwerk bij de (top van de) Vlaamse overheid rond risicomanagement

JC merkt in het kader van de single audit het verschil tussen financiële en organisatieaudits op. Hij benadrukt de positieve evolutie naar levenslang leren en houdt een pleidooi voor goed ondersteunde lerende netwerken. Samen met het aanbieden van cursussen kan het tekort aan auditoren hiermee deels opgevangen worden.

MA geeft aan dat het van mekaar leren ook nog niet volledig uitgeput is binnen de VO.

De vergadering is het er over eens dat binnen de Vlaamse overheid de ondersteuning van het risicomanagement versterkt en verbeterd dient te worden.

IM geeft aan dat er een breed palet aan algemene risico's bestaat en dat een gebrek aan globaal risicomanagement er toe leidt dat dit bij AV terecht komt.

MV vraagt of dit te maken kan hebben met het ontbreken van een overkoepelend strategisch management op VO-niveau. MA nuanceert in zijn antwoord en vindt responsabilisering ter zake ook niet zo slecht. Eigen initiatief nemen is ook waardevol, aangevuld met een lerend netwerk en *best practices*.

MV geeft aan dat men de impact van het opdelen van het beleid in organisatorische fracties niet mag onderschatten. IM sluit hierbij aan en duidt op de meerwaarde van een community die samen valideert en dus ook opvolgt.

JPG stelt dat risico te zeer vanuit een negatief oogpunt bekeken wordt. Ook opportuniteiten kunnen meegenomen worden om naar risico's ter kijken. MA reflecteert hierbij met de 'wat als ik mijn eigen klant zou zijn'-vraag en besluit dat risico management niet zou opgelegd moeten worden, maar gewoon moet deel uitmaken van de normale beslissingsprocedures. Een manager van processen is niet alleen *process owner*, maar tegelijk ook *risk owner*. MA geeft aan dat risico op fraude ook zo'n risico is en dat meer aandacht en ook meer onderzocht moet worden.

JPG stelt dat de aanbevelingen, geformuleerd door auditoren vanuit 'de schoenen' van de managers dient te gebeuren.

WH vraagt of het IT stuurorgaan een rol opneemt richting ondersteuning IT-security. MA beaamt. Er is een strategie en globale *security officer* die rapporteert aan stuurgroep.

Ook staat op de vergaderingen *IT-security* standaard op de agenda. Naast sensibilisering en technologie moet ook BCM verder hoger op de agenda komen. Naast aanvallen en diefstal van gegevens is ook het dysfunctioneren van het ganse overheidsapparaat ten zeerste van belang. Hiervoor moet op niveau van de VO ook de nodige aandacht zijn. De suggestie van digitale rampoefening wordt gedaan. Ook het beleid inzake backups wordt besproken.

IM vraagt wat de bereidheid van de administratie is om centrale IT-security diensten aan te bieden. Lokale besturen beantwoorden vandaag zelfs niet aan de basisvereisten van IT-security. Op welk niveau moet dit best georganiseerd worden?

MA geeft aan dat er een initiatief werd opgezet door de VO. Er is een *security respons team* voor lokale besturen. Recent, naar aanleiding van de bekende incidenten, is er een shift vanuit lokale besturen waar te nemen met vraag naar meer centrale ondersteuning.

De vergadering erkent ook de nadelen van centraliseren, waarbij interessante schotten ook verdwijnen. Zo wordt verwezen naar het niet-geïmpacteerd zijn van de Antwerpse haven en politiediensten.

Slim decentraliseren waarbij de contaminatie van problemen wordt beperkt is dus aan de orde. Controle en detectie kunnen wel centraal georganiseerd worden, zonder volledig de IT-werking te centraliseren.

JPG sluit de vergadering