

The background image shows the interior of an anechoic chamber. The walls, floor, and ceiling are covered with numerous white, pyramid-shaped electromagnetic wave absorbers designed to eliminate reflections. In the center, a person is standing next to a tall, thin measurement device mounted on a red base. A green wireframe structure is visible around the device. The lighting is dim, with some light coming from the top of the chamber.

**Deloitte.**

**Gemeente Eindhoven | IT Audit Management Letter 2019**

02 oktober 2019 | v.90



# Voorwoord

Gemeente  
Eindhoven  
Postbus 90150  
5600 RB Eindhoven  
Nederland

## Contact

Voor vragen over deze managementletter kunt u contact opnemen met:

[Redacted contact information]

[Redacted contact information]

[Redacted contact information]



Geachte [Redacted],

In het kader van de jaarrekeningcontrole over het boekjaar 2019 heeft Deloitte IT-audit werkzaamheden uitgevoerd bij de Gemeente Eindhoven.

In deze rapportage die wij in het kader van de jaarrekeningcontrole uitbrengen, leest u onze observaties ten aanzien van de opvolging van de 2018 IT observaties. Wij hebben daarbij uitsluitend die maatregelen beoordeeld die relevant zijn in het kader van de jaarrekeningcontrole en wij rapporteren hierbij uitsluitend de daarbij geconstateerde observaties. De werkzaamheden zijn niet specifiek ontworpen om fraude op te sporen. Zodoende geven wij geen verklaring af over de effectiviteit van de interne beheersingsmaatregelen.

## Verspreiding

Deze rapportage is bedoeld voor intern gebruik door de Gemeente Eindhoven. Zonder uitdrukkelijke en voorafgaande schriftelijke toestemming van Deloitte is het niet toegestaan deze rapportages, dan wel delen daaruit, te gebruiken voor andere doeleinden dan overeengekomen, aan derden te verspreiden of openbaar te maken, aan de rapportage te refereren of uit de rapportage te citeren.

Graag willen wij hier onze waardering en dank uitspreken voor de medewerking die aan ons is verleend gedurende onze werkzaamheden in 2019. Mocht u naar aanleiding van deze rapportage nog vragen en/of opmerkingen hebben, neemt u dan s.v.p. contact op met ondergetekende.

Met vriendelijke groet,

Deloitte Risk Advisory B.V.

[Redacted signature]

[Redacted signature]

\*\*

# Inhoudsopgave



1. Management Samenvatting

Pag. 04



2. Detail Observaties Algemene IT Beheersmaatregelen

Pag. 12

\*\*\* en  
\*\*\*\*



3. Detail Observaties IT Governance

Pag. 28

\*\*\* en  
\*\*\*\*



4. Detail Observaties Cyber Security

Pag. 36

\*\*\* en  
\*\*\*\*

Bijlage

Pag. 43

\*\*\* en  
\*\*\*\*



# 1 Managementsamenvatting



# Introductie

---

## Doelstelling

Ingevolge artikel 2:393, lid 4 BW, dient de accountant in zijn verslag aandacht te besteden aan de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. In dit kader heeft Deloitte IT-audit werkzaamheden uitgevoerd bij de Gemeente Eindhoven met als doel om:

- De opvolging van de 2018 IT observaties door de Gemeente Eindhoven te beoordelen.
- Bepalen of de IT beheersmaatregelen in voldoende mate de risico's mitigeren die een impact hebben op de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

---

## Scope

De opvolging van de 2018 IT observaties kan als volgt worden onderverdeeld:

Deelgebieden:

- Algemene IT Beheersmaatregelen
- IT Governance
- Cyber Security

Diepgang:

- Opzet: beschrijving van de wijze waarop beheersmaatregelen dienen te werken.
- Bestaan: de beheersmaatregelen die daadwerkelijk in de praktijk zijn geïmplementeerd op een bepaald testmoment.

Systemen:

- Decade: inkoopproces en het uitvoeren van betalingen.
- Suites: uitkeringen, WMO en PGB.
- Windows Active Directory: eerste stap om toegang te krijgen tot de IT systemen.

Wij hebben geen testwerkzaamheden uitgevoerd omtrent algemene beheersmaatregelen op de databases van de applicaties in scope.

# Introductie

---

## Aanpak

De beoordeling van de opvolging van de IT observaties 2018 hebben wij uitgevoerd op basis van interviews met relevante medewerkers van de Gemeente Eindhoven, alsmede inspectie van relevante documenten en systeeminstellingen.

In het kader van het onderzoek is op 17 september 2019 gesproken met de volgende medewerkers van de Gemeente Eindhoven:

- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]

Op 30 september 2019 is gesproken met:

- I [REDACTED]
- I [REDACTED]

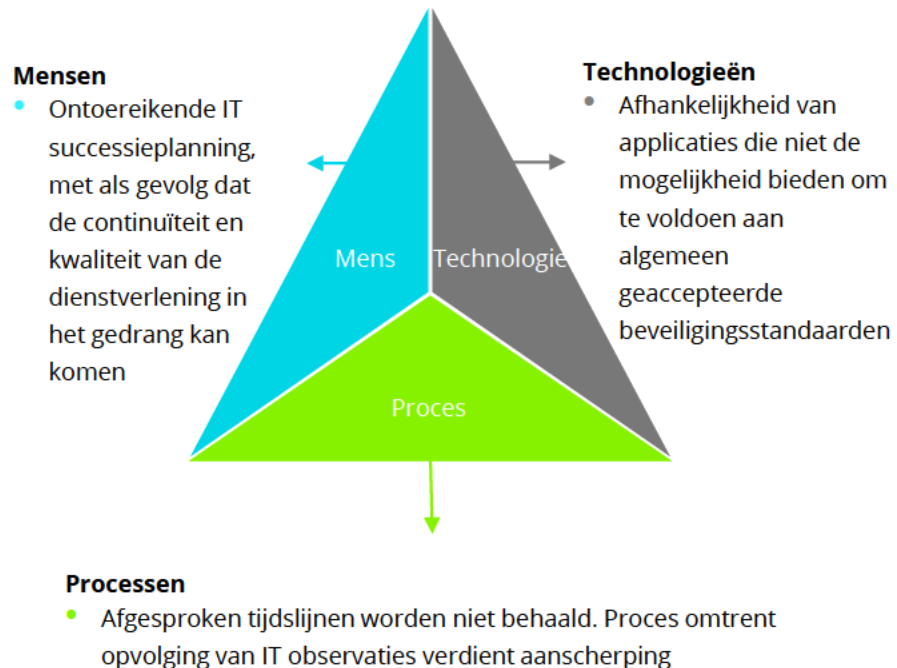
Voor Deloitte Risk Advisory hebben de volgende personen geparticipeerd:

- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]

\*\*

# Conclusie

## Risico thema's



## Toelichting

In de management reactie op de IT management letter 2018 is overeengekomen dat de IT observaties allen per Q3 2019 opgelost zouden zijn. Wij hebben vastgesteld dat deze doelstelling niet is behaald. Van de 22 gerapporteerd observaties zijn slechts 3 volledig opgelost (2 met betrekking tot de algemene IT maatregelen en 1 omtrent IT Governance). Om deze reden zal een gegevensgerichte aanpak worden gehanteerd voor de jaarrekeningcontrole en niet worden gesteund op de geautomatiseerde gegevensverwerking.

Als reden voor het niet behalen van deze doelstelling zien we de frequente wisselingen op de CIO en CISO posities. Daarnaast waren beide posities in de loop van 2019 tijdelijk niet ingevuld. Om de impact van dit soort wisselingen te beperken verdient het aanbeveling om verbeteringen door te voeren in de processen omtrent planning van projecten, en een successieplan op te stellen voor cruciale posities binnen de bedrijfsorganisatie. Hiermee kunnen verstoringen in de bedrijfsvoering worden geminimaliseerd.

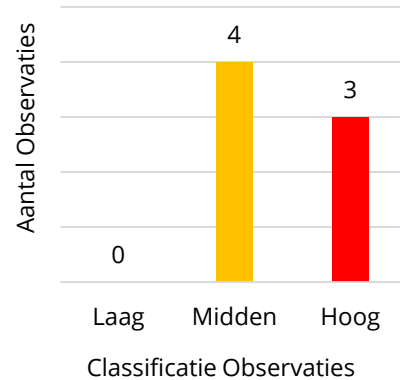
Binnen het domein Cyber Security ligt de focus van de Gemeente Eindhoven momenteel vooral op het implementeren van de Baseline Informatiebeveiliging Overheid (BIO). Aangezien deze regelgeving per 1 januari 2020 een wettelijk eis is voor de Gemeente begrijpen we dat hier de focus ligt vanuit de Gemeente. Het feit dat de implementatie van de BIO de volledige aandacht vergt van de CISO afdeling is echter een verdere indicatie dat de projectplanning en de bemensing binnen de I&B sector van de Gemeente Eindhoven dient te worden verbeterd.



# Algemene IT Beheersmaatregelen

## Observaties

Van de 9 gerapporteerde observaties in 2018 zijn 2 observaties volledig opgelost. Dit resulteert in 7 (gedeeltelijk) openstaande observaties:



## Achtergrond

De Algemene IT Beheersmaatregelen (ook wel General IT Controls genoemd of 'GITC's') zijn de basis om te steunen op de geautomatiseerde gegevensverwerking in IT systemen. Indien de Algemene IT Beheersmaatregelen effectief zijn kan –bij correcte inrichting van het IT systeem– in de audit ook gebruik worden gemaakt van de geautomatiseerde 'Business Controls' in de IT systemen, ook wel aangeduid als applicatie controles.

## Resultaten

Op basis van onze IT audit werkzaamheden hebben wij vastgesteld dat 2 van de 9 Algemene IT observaties volledig zijn opgelost. Voor de overige 7 observaties zijn veelal stappen ondernomen om verbeteringen door te voeren, echter zijn deze in veel gevallen nog niet afgerond. We concluderen wij dat de kwaliteit van de Algemene IT Beheersmaatregelen voor Decade en Suite op dit moment nog onvoldoende is om in het kader van de audit een systeemgerichte aanpak te ondersteunen. Derhalve zal de jaarrekeningcontrole gegevensgericht worden uitgevoerd.

In onze optiek zijn de observaties die wij hebben vastgesteld goed oplosbaar, mits hieraan de juiste prioriteit en middelen worden toegekend. De Gemeente heeft in haar management reactie aangegeven de ambitie te hebben om alle aanbevelingen op korte termijn op te lossen. Het verdient aanbeveling om een concreet plan van aanpak - inclusief tijdslijnen - op te stellen.

Op de volgende pagina noemen wij de IT observaties geprioriteerd op basis van impact en kans. Hierbij geven wij ook aan wat de status is van de opvolging van de observaties.

# Algemene IT Beheersmaatregelen

## Legenda

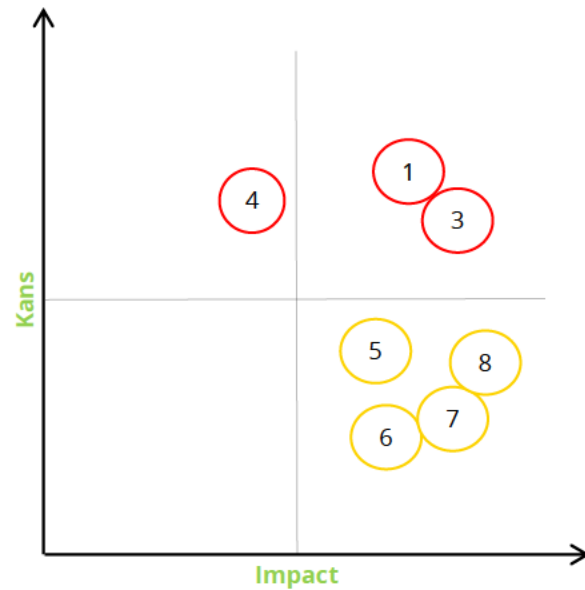
Belangrijke observatie met een hoog risico en potentieel grote impact op de verslaggeving, compliance en/of operationele prestaties.

Middelgrote observatie met een gemiddeld risico en potentieel gemiddelde impact op de verslaggeving, compliance en/of operationele prestaties.

observatie met een laag risico en een mogelijke lagere impact op de verslaggeving, compliance en/of operationele prestaties.

## Toelichting

Om de observaties te prioriteren in het kader van de ondersteuning van de audit hebben wij de observaties geclassificeerd op impact en kans. Onderstaand overzicht toont de observaties welke gedurende de audit zijn geconstateerd. Observaties #2 en #9 zijn opgelost en staan daarom niet in onderstaande grafiek.



	Observaties	Applicatie	Status 2019
1	Onvoldoende aandacht voor functiescheiding bij toekennen van rechten	Decade Suites	Onderhanden
2	Rechten worden niet tijdig verwijderd in Decade	Decade	Opgelost
3	Periodieke review op autorisaties ontbreekt	Decade Suites	Niet opgelost
4	Wachtwoordvereisten verdienen aanscherping	Decade Suites Netwerkomgeving	Gedeeltelijk opgelost
5	Accounts met een generieke naamgeving in gebruik	Suites	Onderhanden
6	Accounts met hoge rechten niet beperkt tot strikt noodzakelijke gebruik en monitoring ontbreekt	Decade Suites	Gedeeltelijk opgelost
7	Vastlegging (audit trail) binnen het wijzigingsbeheerproces niet altijd gewaarborgd	Decade Suites	Niet opgelost
8	Back-up niet afgestemd met wensen eindgebruikers en geen recovery test niet uitgevoerd	Algemeen	Gedeeltelijk opgelost
9	Geen vastlegging periodieke review fysieke toegang data center en geen controle assurance-verklaring	Algemeen	Opgelost

# IT Governance

## Volwassenheidsniveau

Deelgebied	Niveau
Performance Measurement	Repeatable
Risk Management	Repeatable
Value Delivery	Repeatable
Strategic Alignment	Repeatable
Resource Management	Repeatable

In de bijlage staat de toelichting op de betekenis van de volwassenheidsniveaus.

## Achtergrond

Een effectief functionerende IT Governance structuur is de basis voor een optimale inzet en beheersing van IT middelen. Effectieve IT Governance vormt mede de basis voor de betrouwbaarheid van financiële informatie en verslaglegging en is daarmee een belangrijke factor voor de jaarrekeningcontrole.

In het kader van de audit 2019 hebben wij opvolging gegeven aan de 2018 observaties omtrent IT Governance.

## Resultaten

Op het gebied van IT Governance heeft de Gemeente aandacht besteed aan het uitwerken van de IT strategie en planning voor de nabije toekomst. Het vertalen van de strategie naar de concrete doelen is echter uitgesteld tot na het starten van de nieuwe interim CIO, per 1 oktober 2019. Dit heeft tot gevolg dat de volwassenheidsniveaus gelijk zijn gebleven.

De Gemeente kan de slagvaardigheid van de IT-functie verbeteren door taken en verantwoordelijkheden verder uit te werken en overeen te komen binnen de organisatie. Een IT Governance model is binnen uw gemeente in brede zin vormgegeven, maar nog informeel doordat eigenaarschap, formele risicoanalyses en strikte tijdslijnen niet zijn geactualiseerd. Om de volwassenheidsniveaus te verhogen is het cruciaal om de gemaakte plannen in werking te stellen en concrete resultaten te bewerkstelligen. Het is noodzakelijk om afspraken en werkwijzen meer te formaliseren, het eigenaarschap te beleggen en tijdslijnen op te stellen en na te leven.

Voor meer details refereren we naar sectie 3 van deze rapportage.



# Cyber Security

## Volwassenheidsniveau

Deelgebied	Niveau
Organization & Governance	Repeatable
Behavior & Culture	Repeatable
Risk Analysis	Ad hoc
Third Party Management	Repeatable
Detection:	Repeatable
Response:	Ad hoc

In de bijlage staat de toelichting op de betekenis van de volwassenheidsniveaus.

## Achtergrond

Cyber is een onlosmakelijk deel van onze samenleving. Door bijvoorbeeld gebruik van internet, bedrijfsnetwerken en -applicaties hebben organisaties te maken met aan cyber gerelateerde risico's zoals hacks of andere vormen van cybercrime. Als cyberrisico's zich voordoen, kunnen deze een significante impact hebben op (financiële) systemen, de interne beheersing en daarmee uiteindelijk de jaarrekening(controle).

In het kader van de audit 2019 hebben wij opvolging gegeven aan de 2018 observaties omtrent Cyber Security.

## Resultaten

Het belang van cyber weerbaarheid is door de gemeente onderkend. Wij hebben vastgesteld dat er verschillende maatregelen zijn getroffen, zoals het invullen van de functies van Chief Information and Security Officer (CISO) ondersteund door een Information Security Officer per domein. Overall zien wij dat de beheersing van cyber risico's nog niet het gewenste niveau heeft en concluderen wij dat de aanwezige cyber security beheersing (te) beperkt is qua aard, reikwijdte en/of diepgang voor ongeautoriseerde wijzigingen in systemen, het openbaar worden van persoonsgegevens, vertrouwelijke gegevens of door het verstoren van de bedrijfsvoering. Wij hebben een aantal verbetermogelijkheden met de organisatie besproken en gedeeld, zoals het periodiek uitvoeren van risicoanalyses, het maken van schriftelijke afspraken met derden partijen en het periodiek evalueren van het ontstaan en de opvolging van incidenten.

In sectie 4 van deze rapportage zijn de detailobservaties opgenomen met betrekking tot Cyber Security.



2

## Detail Observaties Algemene IT Beheersmaatregelen





### 3 Detail Observaties IT Governance



## 4 Detail Observaties Cyber Security



## 5 Bijlage

