

## 4. IT-beheersing

- 4.1 [IT-beheersing](#)
- 4.2 [Bevindingen IT-beheersing](#) | [Key2Financiën](#)
- 4.3 [Bevindingen IT-beheersing](#) | [Key2Belastingen](#)
- 4.4 [Bevindingen IT-beheersing](#) | [ADP](#)
- 4.5 [Bevindingen IT-beheersing](#) | [Suite4SociaalDomein](#)
- 4.6 [Bevindingen IT-beheersing](#) | [Continuïteit](#)
- 4.7 [Ontwikkelingen en risico's van cloudoplossingen](#)

## 4.1 IT-beheersing

Wij beoordelen de betrouwbaarheid en continuïteit IT voor zover relevant voor de controle van de jaarrekening

Beoordeelde systemen:

- Key2Financiën
- Suite4SociaalDomein
- Key2Belastingen
- ADP

### IT-werkzaamheden en onze controlerende rol

Ingevolge artikel 2:393, lid 4 BW, dient de accountant in zijn verslag aandacht te besteden aan de bevindingen die naar voren zijn gekomen uit de beoordeling van de automatiseringsomgeving wat betreft de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

Wij benadrukken dat onze jaarrekeningcontrole gericht is op het geven van een oordeel omtrent de jaarrekening zelf en zich niet primair richt op het doen van uitspraken omtrent de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking als geheel of van onderdelen daarvan. De IT-auditwerkzaamheden zijn geïntegreerd in de controleaanpak van de jaarrekening.

Het inzicht in de betrouwbare werking van IT-systemen en applicaties en het gebruik daarvan door de organisatie, vormen een onderdeel van de kwaliteit van de interne beheersing en de administratieve organisatie. Algemene IT-beheersmaatregelen rond uw kritieke systemen leveren daarnaast een belangrijke bijdrage aan het mitigeren van de risico's op onbeheerste wijzigingen, ongeautoriseerde handelingen en het optreden van verstoringen met impact op de gegevensverwerking.

De bevindingen zoals gerapporteerd in deze management letter zijn gericht geweest op het beoordelen van de opzet en het vaststellen van het bestaan van algemene IT-beheersmaatregelen. Wij hebben in samenwerking met onze IT-auditors een aantal van deze maatregelen beoordeeld voor Key2Financiën, Suite4SociaalDomein, Key2Belastingen en ADP. Dit om de impact van de risico's van onbeheerste wijzigingen, ongeautoriseerde handelingen en verstoringen te kunnen vaststellen voor die systemen die gekoppeld zijn aan de voor ons relevante processen en posten (zie hoofdstuk 3).

In dit hoofdstuk geven wij een samenvatting van onze bevindingen voor de genoemde applicaties. De detailbevindingen rondom deze systemen zijn afgestemd middels notulen met de betrokkenen. De detailbevindingen rondom deze systemen zijn opgenomen in bijlage B.

Op het moment dat de intern getroffen algemene IT-beheersmaatregelen rondom de applicaties in scope niet (bewijsbaar) voldoende aanwezig zijn, zijn in het kader van de controle van de jaarrekening 2020 aanvullende (gegevensgerichte) werkzaamheden noodzakelijk om aan te tonen dat er zich geen risico's of fouten hebben voorgedaan.

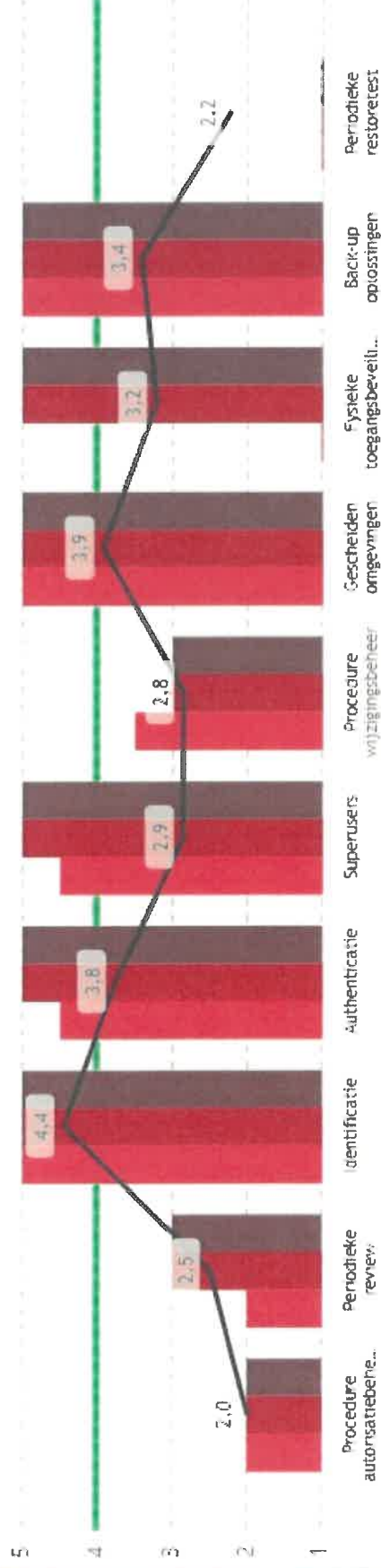
Wij vervolgen het hoofdstuk van IT beheersing met de benchmark waarin wij onze kennis en inzichten die wij hebben opgedaan bij de uitvoering van IT audits bij andere klanten binnen de lokale overheidsector afzetten tegen onze bevindingen binnen uw organisatie. Vervolgens beschrijven wij onze detailbevindingen per beoordeeld systeem. Tenslotte gaan wij vanuit onze natuurlijke adviesfunctie in op de ontwikkelingen en risico's van cloudoplossingen. Cloudoplossingen zijn een hot topic in de sector.

## 4.1 IT-beheersing

### Gemiddelde en verloop

● 2018 ● 2019 ● 2020 — Benchmark

Benchmark lijn Jaartal: 2019



De GRD heeft in de afgelopen jaren een constante score.

Ten opzichte van de benchmark zijn de scores in veel gevallen beter.

### Uw scores

Uw IT-beheersing behoeft nog verdere aandacht. Zie hiervoor ook de detailbevindingen in hoofdstuk 4.2.



Logische Toegangsbeveiliging



1 5



Wijzigingsbeheer



1 5



Continuïteit



1 5

### Uitleg Benchmark



Op basis van onze kennis en inzichten die wij hebben opgedaan bij de uitvoering van IT audits hebben wij een benchmark ontwikkeld. Deze benchmark geeft inzicht in de IT audit resultaten van uw organisatie afgezet tegen het gemiddelde van vijftig van onze klanten binnen de Overheidssector.

Bovendien laat deze benchmark zien hoe uw organisatie zich heeft ontwikkeld op het gebied van IT-beheersing over de periode vanaf 2018 tot en met 2020.

Hierin is een score van 1 tot en met 5 per norm weergegeven waarbij BDO een score van minimaal 4 toereikend acht.

## 4.2 Bevindingen IT-beheersing | Key2Financiën

Logische toegangs-  
beveiliging K2F  
(criteria 1-2) nog  
deels ontoereikend

Change management  
(criteria 6) nog deels  
ontoereikend.

| PROCES                                                            | 2019 | 2020 |
|-------------------------------------------------------------------|------|------|
| 1. Procedure autorisatiebeheer                                    |      |      |
| 2. Periodieke controle op juistheid ingerichte autorisaties       |      |      |
| 3. Identificatie van gebruikers voor toegang tot systemen en data |      |      |
| 4. Wachtwoordbeleid (authenticatie)                               |      |      |
| 5. Administrators en superusers                                   |      |      |
| 6. Wijzigingenbeheer                                              |      |      |
| 7. Gescheiden omgevingen (ontwikkel-test-productie)               |      |      |

onvoldoende

verbeterpunten

voldoende

Niet beoordeeld

### KORTE OMSCHRIJVING RESULTATEN

- 1 Geen formeel geaccordeerde normpositie.
- 2 Er is geen periodieke review uitgevoerd op de juistheid van autorisaties in Key2Finance aangezien er geen normpositie beschikbaar is. Echter is wel een periodieke review uitgevoerd op de actualiteit van gebruikers in Key2Finance.
- 3 Generieke gebruikers zijn verklaard en persoonlijke gebruikers hebben allemaal een eigen unieke account.
- 4 De wachtwoordeisen in Key2Finance voldoen aan de minimale te stellen eisen van BDO.
- 5 Superuser-rechten worden alleen toegekend aan medewerkers binnen de van het team 'Ontwikkeling en Functioneel beheer' (van de afdeling financiën) van het Servicecentrum Drechtsteden (SCD). Dit zijn geen eindgebruikers van Key2Financiën.
- 6 Testwerkzaamheden en goedkeuring op de wijzigingen worden niet structureel geregistreerd.
- 7 Iedere applicatie in scope een logisch gescheiden test- en productie omgeving ingericht. De software wordt ontwikkeld in een ontwikkelomgeving bij de leveranciers, waardoor er functiescheiding tussen de ontwikkelaar en in-productienemer (GRD) aanwezig is.

## 4.3 Bevindingen IT-beheersing | Key2Belastingen

Logische toegangs-  
beveiliging K2B  
(criteria 1-2) nog  
deels ontoereikend

Change management  
(criteria 6) nog deels  
ontoereikend.

| PROCES                                                            | 2019 | 2020 |
|-------------------------------------------------------------------|------|------|
| 1. Procedure autorisatiebeheer                                    |      |      |
| 2. Periodieke controle op juistheid ingerichte autorisaties       |      |      |
| 3. Identificatie van gebruikers voor toegang tot systemen en data |      |      |
| 4. Wachtwoordbeleid (authenticatie)                               |      |      |
| 5. Administrators en superusers                                   |      |      |
| 6. Wijzigingenbeheer                                              |      |      |
| 7. Gescheiden omgevingen (ontwikkel-test-productie)               |      |      |

onvoldoende

verbeterpunten

voldoende

Niet beoordeeld

### KORTE OMSCHRIJVING RESULTATEN

- 1 Geen formeel geaccordeerde normpositie.
- 2 Er is geen periodieke review uitgevoerd op de juistheid van autorisaties in Key2Belastingen aangezien er geen normpositie beschikbaar is. Echter is wel een periodieke review uitgevoerd op de actualiteit van gebruikers in Key2Belastingen.
- 3 Generieke gebruikers zijn verklaard en persoonlijke gebruikers hebben allemaal een eigen unieke account.
- 4 De wachtwoordeisen in Key2Belastingen voldoen aan de minimale te stellen eisen van BDO.
- 5 Superuser-rechten worden alleen toegekend aan medewerkers van applicatiebeheer. Dit zijn geen eindgebruikers van Key2Belastingen.
- 6 Testwerkzaamheden en een goedkeuring op de wijziging worden niet structureel geregistreerd.
- 7 Iedere applicatie in scope een logisch gescheiden test- en productie omgeving ingericht. De software wordt ontwikkeld in een ontwikkelomgeving bij de leveranciers, waardoor er functiescheiding tussen de ontwikkelaar en in-productienemer (GRD) aanwezig is.



## 4.5 Bevindingen IT-beheersing | Suite4SociaalDomein

Logische toegangs-  
beveiliging S4SD  
(criteria 1-2) nog  
deels ontoereikend

Change management  
(criteria 6) nog deels  
ontoereikend.

| PROCES                                                            | 2019 | 2020 |
|-------------------------------------------------------------------|------|------|
| 1. Procedure autorisatiebeheer                                    |      |      |
| 2. Periodieke controle op juistheid ingerichte autorisaties       |      |      |
| 3. Identificatie van gebruikers voor toegang tot systemen en data |      |      |
| 4. Wachtwoordbeleid (authenticatie)                               |      |      |
| 5. Administrators en superusers                                   |      |      |
| 6. Wijzigingenbeheer                                              |      |      |
| 7. Gescheiden omgevingen (ontwikkel-test-productie)               |      |      |

onvoldoende

verbeterpunten

voldoende

Niet beoordeeld

### KORTE OMSCHRIJVING RESULTATEN

- 1 Er is per 2020 een normpositie van rollen per applicatie. Deze is nog niet zichtbaar goedgekeurd door het MT". Op basis van 1 indienstreding is vastgesteld dat rollen/rechten niet op basis van deze autorisatiematrix zijn toegekend.
- 2 Er is geen periodieke review uitgevoerd op de juistheid van autorisaties in S4SD. Echter is wel een periodieke review uitgevoerd op de actualiteit van gebruikers in S4SD.
- 3 Binnen S4SD is één generiek account actief welke op basis van functie gepersonaliseerd dient te zijn.
- 4 De wachtwoordeisen in S4SD voldoen aan de minimaal te stellen eisen van BDO.
- 5 Superuser-rechten worden alleen toegekend aan medewerkers binnen de van het team 'Functioneel beheer' van het Servicecentrum Drechtsteden (SCD). Dit zijn geen eindgebruikers van S4SD.
- 6 Testwerkzaamheden en goedkeuring op de wijzigingen worden niet structureel geregistreerd.
- 7 Iedere applicatie in scope een logisch gescheiden test- en productie omgeving ingericht. De software wordt ontwikkeld in een ontwikkelomgeving bij de leveranciers, waardoor er functiescheiding tussen de ontwikkelaar en in-productienemer (GRD) aanwezig is.

# 4.6 Bevindingen IT-beheersing | Continuïteit

| KORTE OMSCHRIJVING RESULTATEN |                                                                                                                                                                                                          |  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 1                             | Geen bevindingen.                                                                                                                                                                                        |  |
| 2                             | Geen bevindingen.                                                                                                                                                                                        |  |
| 3                             | Er wordt geen uitwijktest uitgevoerd, waardoor niet getest is of de productie-data binnen eisen omtrent maximale data-verties en maximale hersteltijd teruggezet kan worden in geval van een calamiteit. |  |

Continuïteit (criteria 3)  
nog deels ontoereikend

| PROCES                                 | 2019 | 2020 |
|----------------------------------------|------|------|
| 1. Fysieke toegangsbeveiliging         |      |      |
| 2. Back-up & monitoring                |      |      |
| 3. Periodieke hersteltest (of uitwijk) |      |      |

onvoldoende

verbeterpunten

voldoende

Niet beoordeeld

DASHBOARD

INTERNE CONTROLE

IT-BEHEERSING

BIJLAGEN

## 4.7 Ontwikkelingen en risico's van cloudoplossingen

"The cloud is just  
someone else's  
computer"

### Digitale overheid

Cloud computing is inmiddels stevig ingeburgerd bij overheidsinstanties en wordt steeds innovatiever toegepast, denk aan Smart Cities. Steeds meer overheidsinstanties gaan over tot het opstellen van grondige cloud strategieën.

Inmiddels gebruikt ruim driekwart van de organisaties een hybride cloud- of multi-cloud-model. Deze modellen bieden de voordelen van cloud computing, maar streven tegelijkertijd na de hieruit voortvloeiende risico's te mitigeren. Te denken valt hierbij aan risico's op het gebied van cybersecurity en dataprivacy, maar ook aan overmatige afhankelijkheid van leveranciers.

De voortgaande digitalisering gaat geen enkel organisatieproces voorbij. Ook de inrichting en het beheer van de IT-infrastructuur niet; in toenemende mate wordt de infrastructuur software-defined. Beschikbaarheid van IT blijft derhalve kostbaarder worden. Dit onderstreept te meer de noodzaak van het in staat zijn om data binnen korte tijd volledig te kunnen herstellen. Public cloud-leveranciers bieden hiertoe kwalitatief goede mogelijkheden.

### Cloud computing is niet zonder risico's

#### Transitie naar cloud

Een veel voorkomende valkuil is het onderschatten van de data-migratie en het realiseren van de aansluiting van de cloud op bestaande oplossingen. Dit resulteert in hogere kosten dan begroot. Daarnaast vergt de 'nieuwe' regie-rol op ICT wezenlijk andere competenties dan het traditioneel functionerend houden van de IT-omgeving.

#### Leverancier 'lock-in'

Ook neemt de afhankelijkheid van leverancier ten opzichte van on-premise software toe. Dit kan zich in geval van gebrekkige governance uiten in onverwacht hoge kosten en hogere drempels om van leverancier te wisselen.

#### Informatiebeveiliging en privacy

Een ander groot risico is dat de data onvoldoende beveiligd is. Als gegevens onvoldoende beveiligd zijn kunnen ze gehackt worden of in handen komen van derden met enorme imagoschade en boetes als gevolg. Ook is vaak onbekend waar de data wordt opgeslagen. Het kan dus zo zijn dat uw data wordt opgeslagen in een land waar ze het niet zo nauw nemen met de privacy-wetgeving.



## 4.7 Ontwikkelingen en risico's van cloudoplossingen

"The cloud is just someone else's computer"

### De 7 aandachtsgebieden van cloud

Wij hebben zeven aandachtsgebieden geformuleerd om grip te houden op cloud risico's:

- 1. Cloud Governance:** Duidelijke afstemming en vastlegging van verantwoordelijkheden tussen uw organisatie en de cloudleverancier zijn belangrijk om efficiënte bedrijfsvoering en informatiebeveiliging te borgen in de processen. Heldere afspraken omtrent performance, processen en escalaties met de cloudleverancier en een exit procedure zijn key;
- 2. Access Management:** Toegang tot de cloudoplossing heeft u meestal zelf in beheer. Een helder proces zorgt ervoor dat medewerkers alleen toegang hebben tot de data die zij nodig hebben voor hun functie en dat ongeautoriseerde personen er niet bij kunnen;
- 3. Compliance:** Het gebruik van cloudoplossingen is steeds meer aan regels gebonden, ook in internationale context. Een overzicht van welke cloudoplossingen u gebruikt en in welke landen de data wordt opgeslagen en verwerkt helpt u om te bepalen welke wet- en regelgeving op uw organisatie van toepassing is;
- 4. Leveranciersmanagement:** Als regioorganisatie dient u actief de dienstverlening, performance, beveiliging en kosten van uw belangrijkste cloudleveranciers te monitoren. Dat kan bijvoorbeeld door het opvragen, beoordelen en opvolgen van service level rapporten en assurancerapporten;
- 5. Secure Configuration:** Voorkomen is beter dan genezen: het veilig configureren van cloudsysteem helpt u om uw bedrijfsvoering veilig te houden. De systemen in de cloud worden veilig geconfigureerd volgens geldende standaarden en periodiek geëvalueerd;

**6. Network Security:** Er moet een veilige verbinding zijn met de cloudoplossing zodat verkeer niet onderschept kan worden. Penetratietesten helpen u om zowel externe als interne kwetsbaarheden op te sporen;

**7. Security Monitoring:** Een SOC- of SIEM-oplossing monitort verdacht verkeer en rapporteert over verdachte events, zodat u op de hoogte bent wat in uw IT-omgeving plaatsvindt.

