4 NOVEMBER 2024

CONCEPT

MANAGEMENT LETTER 2024

Dar N.V.

BDO Audit & Assurance B.V., De Coöperatie 15-14, 7514 JK Enschede, www.bdo.nl

Aan:

de Directie van Dar N.V.
t.a.v.
de heer G.T.M. de Bruin
Postbus 316
6500 AH NIJMEGEN

Enschede, 4 november 2024

Kenmerk:105740813/MZ/RTE

Geachte directie,

U heeft ons gevraagd de jaarrekening 2024 van Dar N.V. (hierna: 'Dar') te controleren. Naar aanleiding van onze interim-controle brengen wij met deze management letter verslag uit over onze bevindingen.

Deze management letter bevat onze belangrijkste bevindingen ten aanzien van de processen binnen Dar en de daarin opgenomen beheersingssystemen.

Tijdens onze bezoeken aan Dar komen wij ook in aanraking met andere ontwikkelingen van uw organisatie en bedrijfsvoering. We bespreken graag een aantal van die andere ontwikkelingen met u. In deze management letter besteden we daarom ook aandacht aan ontwikkelingen op andere gebieden dan de processen.

Het vervolg van onze werkzaamheden voor de controle van de jaarrekening staat gepland in maart 2025. Hier zijn met onze contactpersonen binnen Dar afspraken over gemaakt.

Op basis van Nederlands recht en overige beroepsregels, zoals de 'Verordening inzake de onafhankelijkheid van accountants bij assuranceopdrachten' (ViO), is vereist dat wij onafhankelijk zijn ten opzichte van onze controle-cliënten. Wij zijn van mening dat door ons is voldaan aan deze eisen.

Wij hopen u met dit verslag van dienst te zijn. Wij willen de organisatie bedanken voor de prettige samenwerking en zijn vanzelfsprekend graag bereid een nadere toelichting te verstrekken.

Hoogachtend,

BDO Audit & Assurance B.V.
namens deze,

M. Zoetman - Kiers RA
Partner BDO en extern accountant Dar

Inhoudsopgave

01
Dashboard interim-controle

02
Ontwikkelingen & Aandachtspunten

03
Onze bevindingen

1. Dashboard interim-controle

1.1 Dashboard interim-controle 5

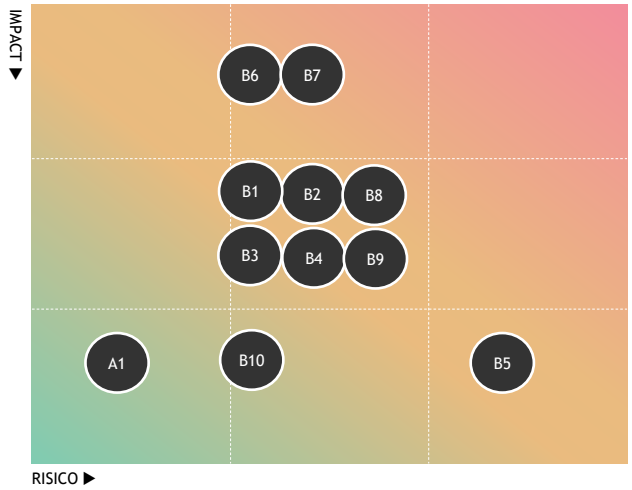
1. Dashboard

Informatiebeveiliging en Network and Information Security Directive (NIS2)

Interne beheersing

- Op basis van onze observaties concluderen wij dat de interne beheersing en controleomgeving van voldoende tot goed niveau is om tot een betrouwbare jaarrekening te komen.
- Voor een organisatie met de ambitie van Dar zou de norm moeten zijn dat de processen in opzet, bestaan en werking (inclusief IT) goed werken en zichtbaar getoetst worden.
- Tijdens onze interim-controle hebben wij voornamelijk bevindingen bij de IT-systemen en interne beheersing hieromtrent. Op IT-gebied zien wij dat voortgang geboekt wordt maar blijven wij aandacht vragen voor onderstaande bevindingen in het licht van de jaarrekeningcontrole.

Interne beheersing in beeld



Actuele ontwikkelingen

- Activiteiten Dar en strategie
- Tussentijdse cijfers 2024 en ontwikkeling werkkapitaal
- Investeringen in relatie tot begroting en duurzame bedrijfsvoering
- Financiële contouren Dar
- Informatiebeveiliging en cybersecurity – NIS2
- Corporate Sustainability Reporting Directive (CSRD) en rapportage over ESG
- Kwalificatie van arbeidsrelaties

TOELICHTING BEVINDINGEN
A1. Bankrechten in bankapplicatie
B1. Procedure autorisatiebeheer - Voor Exact Synergy, Exact Globe, BORVision en Clear is geen formele normpositie, goedgekeurd door het management, beschikbaar
B2. Procedure autorisatiebeheer - Voor BORVision en Clear worden gebruikersaccounts niet ten alle tijden op of voor de uitdienstdatum geblokkeerd
B3. Periodieke controle op juistheid ingerichte autorisaties - Een periodieke controle voor Exact Synergy, Exact Globe, BORVision en Clear wordt niet uitgevoerd
B4. Identificatie van gebruikers voor toegang tot systemen en data - Voor Exact Global zijn handelingen en transacties van generieke accounts niet herleidbaar naar een individuele gebruiker
B5. Authenticatie - Binnen de Active Directory zijn enkele administrator accounts welke zijn uitgezonderd van het periodiek wijzigen van wachtwoorden
B6. Administrator- en Superuser-accounts - In de Active Directory en Clear zijn beheerdersbevoegdheden belegd binnen de gebruikersorganisatie
B7. Database autorisaties - In de database van BORVision zijn beheerdersbevoegdheden belegd in de gebruikersorganisatie
B8. Wijzigingsbeheer - Voor Exact Synergy en Exact Globe wordt geen ISAE 3402 rapportage opgevraagd en beoordeeld
B9. Gescheiden omgevingen – Binnen BORVision zijn autorisaties met betrekking tot ontwikkelen en doorvoeren van wijzigingen zijn niet inzichtelijk.
B10. Restore-test - Van de uitgevoerde restoretest zijn de uitkomsten niet gedocumenteerd

2. Ontwikkelingen & Aandachtspunten

2.1 Actuele ontwikkelingen 7

2.1 Actuele ontwikkelingen

Activiteiten DAR en strategie

Het strategisch plan van Dar dient als basis voor het jaarlijkse bedrijfsplan. Wij merken daarbij op dat het strategisch plan in 2024 opnieuw wordt uitgewerkt voor de jaren 2024-2028, aangezien 2024 het vierde en laatste jaar is van het huidige strategisch plan ‘Dar, dat zijn wij!’.

Het bedrijfsplan 2024 is uitgewerkt met een doorkijk naar 2026 en voorgelegd ter vaststelling aan de Algemene vergadering van Aandeelhouders. Hierin zijn de plannen voor 2024 opgenomen, evenals een begroting voor de exploitatie en voor investeringen, waarbij rekening wordt gehouden met de winstdoelstelling van 5%. In het bedrijfsplan is rekening gehouden met externe omstandigheden, zoals mogelijke kostenstijgingen door arbeidsmarktkrapte, een nieuw af te sluiten CAO en hogere prijzen. Tot slot is uitgegaan van structurele tariefsverhogingen in afstemming met gemeenten.

Langs vier strategische lijnen heeft Dar in het bedrijfsplan 2024 uiteengezet hoe ingezet wordt op kwaliteitsverbetering van grondstoffen, groei van Road2Work@Dar, digitalisering van IBOR-werkzaamheden. Tevens wordt ingegaan op hoe de bedrijfsvoering meer duurzaam wordt vormgegeven met projecten zoals het huisvestingsproject en de implementatie van de CSRD, en met programma’s zoals Samen Beter voor de werving van nieuw personeel en borging van veilig werken van personeel. Voor de strategische periode 2024-2028 is een vijfde lijn toegevoegd om de klantgerichtheid te versterken. Voor de andere vier lijnen heeft herijking plaatsgevonden.

Tussentijdse cijfers tot ten met september en ontwikkeling werkkapitaal

Wij hebben de maandrapportage tot en met augustus beoordeeld en besproken met het management. Het resultaat tot en met september 2024 bedraagt € 0,2 miljoen positief en ligt € 0,2 miljoen achter op de begroting. Het begrote rendement van 5,1% wordt niet behaald: het rendement bedraagt 1,9%.

Een belangrijke oorzaak hiervan ligt in hogere kosten inhuur voertuigen en hogere onderhoudskosten voor het wagenpark als gevolg van uitgestelde levering van nieuwe vervoersmiddelen).

In 2024 is € 5 miljoen financiering van de Gemeente Nijmegen ontvangen als onderdeel van de financieringsafspraak van € 15,2 miljoen voor de investeringen in huisvesting. De solvabiliteit is mede hierdoor per eind september 2024 afgenomen van 51,8% eind 2023 naar 50,3%. De current ratio is per eind september 2024 verbeterd van 0,7 eind 2023 naar 1,0 met name vanwege afgenomen kortlopende schulden. Het saldo liquide middelen bedraagt per eind september € 4,0 miljoen, waarvan in oktober € 2,5 miljoen in een deposito is geplaatst.

De operationele kasstroom bedraagt per ultimo september 2024 € 1,1 miljoen positief. Vanwege omvangrijke investeringen, in onder andere het wagenpark, vertonen de totale liquiditeiten sinds het voorjaar van 2023 een dalende lijn. In 2024 is daarom voor het eerst gebruik gemaakt van de rekening-courant kredietfaciliteit van de Rabobank. In het najaar van 2024 is de liquiditeitsbehoefte opnieuw bepaald en op basis hiervan is een aanvraag bij gemeente Nijmegen ingediend voor het verhogen van de financiering met € 2,5 miljoen naar € 4,5 miljoen. Hiermee wordt voldoende ruimte gecreëerd om de geplande investeringen te doen met een toereikende liquiditeitspositie.

Op de langere termijn wil Dar de liquiditeit verbeteren mede door het project ‘Toekomstige financiële contouren Dar’ (zie volgende pagina).

2.1 Actuele ontwikkelingen

Investeringen in relatie tot begroting en duurzame bedrijfsvoering

De investeringen in 2024 bedragen € 3,0 miljoen en liggen op begroting, waarbij de belangrijkste investering € 1,8 miljoen in voertuigen betreft. Daarnaast is € 0,3 miljoen geïnvesteerd in de huisvestingsplannen. De grotere geplande investeringen in huisvesting zijn circa vier maanden vertraagd, mede vanwege het aantreffen van leidingen onder de parkeerplaats en gewijzigde plannen als gevolg hiervan.

Toekomstige financiële contouren Dar

Dar heeft een nieuw project opgestart genaamd ‘Toekomstige financiële contouren Dar’. Dit project bestaat uit twee sporen. Het eerste spoor is met name intern gericht en betreft het voormalige project ‘resultaatgericht sturen’. Het tweede spoor binnen het project ‘Toekomstige financiële contouren Dar’ is meer extern gericht en betreft het financiële beleid.

Afgelopen jaar heeft Dar middels het project ‘resultaatgericht sturen’ meer inzicht gekregen in de resultaten van geleverde diensten. In de resterende maanden van 2024 wordt een nieuwe tariefstructuur opgezet op basis van een nieuwe methode voor kostenallocatie. Hiermee wordt meer inzicht verkregen in het rendement op de activiteiten per gemeente en per geleverde dienst. Dit wordt in eerste instantie voor inzameling ingericht en in 2025 ook voor de IBOR-activiteiten. Met een meer transparante systematiek wordt een inzichtelijke prijs voor de dienstverlening van Dar voor de verschillende gemeenten neergezet, waarmee de dienstverlening financieel meer duurzaam/ toekomstgericht wordt gerealiseerd. Naar verwachting is eind november 2024 duidelijk wat de consequenties zijn van het nieuwe tarievenmodel en welke implementatiestrategie gekozen wordt. De organisatie is hierover actief in overleg met zowel de RvC als de aandeelhouders.

Wij hebben met de organisatie afgesproken dat wij, zodra de tariefstructuur en onderliggende allocatie gereed is, de documenten beoordelen en wij onze aandachtspunten meegeven ter overweging.

In spoor twee wordt in nauw overleg met de aandeelhouders opnieuw gekeken naar de wensen omtrent rendement, risico’s en het dividendbeleid.

Inmiddels hebben vijf bijeenkomsten plaatsgevonden met de aandeelhouders, waarbij hierover is gesproken en waarbij door Dar de relatie is toegelicht tussen de aankomende (omvangrijke) investeringen en de wens de financiële positie te verbeteren. Vanwege de lage financiële marges de afgelopen jaren is versterking van de financiële positie van belang, met name met betrekking tot de liquiditeit om de toekomstige investeringen te kunnen financieren. Hierbij wordt gedacht aan het verhogen van de tarieven. Naar verwachting zal een definitief voorstel en besluitvorming hierover niet meer in 2024 gerealiseerd worden, waarmee de impact op de jaarrekening van 2024 beperkt zal zijn. Wij zullen daarom ten tijde van de eindejaarscontrole kennis nemen van de stand van zaken op dat moment en hierover rapporteren in het accountantsverslag.

2.1 Actuele ontwikkelingen

Informatiebeveiliging en Network and Information Security Directive (NIS2)

Informatiebeveiliging en cybersecurity

Vanuit onze natuurlijke adviesrol attenderen wij u graag op een aantal ontwikkelingen op het gebied van IT. Afgelopen jaren is meer aandacht voor cybersecurity risico's ontstaan, mede door verhoogde (media)aandacht voor cybersecurity incidenten. Deze toegenomen aandacht voor cybersecurity risico's leeft bij zowel management, toezichthouders als ook het maatschappelijk verkeer. Organisaties zijn in sterke en toenemende mate afhankelijk van de continuïteit van IT-systemen. Zelfs zodanig dat bij het uitvallen of gijzeling (via ransomware) van de IT-systemen de bedrijfscontinuïteit geraakt kan worden. Dit kan daarmee ook een continuïteitsrisico in het kader van de jaarrekening met zich meebrengen. Als gevolg van de snelheid waarmee het digitale (cyber)domein zich ontwikkelt is het van belang continu en grondig te evalueren of cybersecurity risico's nog passend (juist en volledig) worden geadresseerd. Dit kunt u doen door veranderingen in dreigingen of kwetsbaarheden te identificeren en de effectiviteit van getroffen maatregelen periodiek te toetsen.

Wij zien verbeteringsmogelijkheden op het gebied van IT en bijbehorende interne beheersing en hebben hierover ook in eerdere jaren gerapporteerd aan het management. Dar is actief bezig om de IT-organisatie verder te verbeteren en te professionaliseren. Wij zien een positieve ontwikkeling en onderschrijven het belang van het doorvoeren van de voorgenomen verbeteringen op dit gebied. Verbeteringen zijn op dit moment met name benodigd op gebied van strategie- en beleidsvorming en IT General Controls. In paragraaf 3.4 hebben wij onze bevindingen opgenomen omtrent de IT-beheersing.

NIS2 - digitale weerbaarheid verankerd in wet- en regelgeving vanuit de EU

Om de digitale weerbaarheid van organisaties te verhogen is de NIS2 (Network and Information Security 2) richtlijn vanuit de EU vastgesteld. De NIS2 richtlijn is een update van de in 2016 ingevoerde NIS-richtlijn. In Nederland ook wel bekend als NIB2 (Netwerk- en informatiebeveiligingsrichtlijn) en/of de Wbni (Wet Beveiliging Netwerk- en Informatiesystemen).

Medio 2025 zal naar verwachting de NIS2 naar Nederlandse wetgeving worden vertaald en nadien van kracht zijn onder de noemer 'Cyberbeveiligingswet'. Dar kwalificeert als onderneming in de categorie 'Afvalstoffenbeheer' en is uit dien hoofde ook gebonden aan deze richtlijn.

De volgende verplichtingen vallen onder NIS2:

- **Zorgplicht**: organisaties dienen een risicobeoordeling uit te voeren en op basis daarvan passende maatregelen te nemen om hun diensten te beveiligen.
- **Opleidingsplicht**: bestuursorganen dienen opgeleid te zijn, en optioneel ook werknemers, om cyberrisico's te identificeren, impact te bepalen en beveiligingsmaatregelen te selecteren.
- **Meldplicht**: cyberincidenten dienen binnen 24 uur bij de toezichthouder te worden gemeld. Tevens dient een cyberincident ook bij een sectorspecifiek Computer Security Incident Response Team (CSIRT) te worden gemeld, wat eventueel hulp en bijstand kan verlenen.
- **Toezicht**: een onafhankelijk toezichthouder zal naleving van de verplichtingen uit de richtlijn borgen.

Op basis van onze werkzaamheden hebben wij geconstateerd dat Dar zich bewust is van de veranderingen die de NIS2 met zich meebrengt. Belangrijk is dat NIS2 aanvullende eisen stelt, die niet volledig door de huidige vereisten worden afgedekt. Dit betekent dat in de komende periode additionele maatregelen moeten worden getroffen ten einde aan NIS2 te voldoen.
DAR zal korte termijn een GAP-analyse laten uitvoeren waarin inzichtelijk wordt gemaakt welke acties ondernomen moeten worden om te voldoen aan de NIS2.

2.1 Actuele ontwikkelingen

Corporate Sustainability Reporting Directive (CSRD) en rapportage over ESG

Met ingang van boekjaar 2023 heeft een wetswijziging plaatsgevonden met betrekking tot het groottecriteria van bedrijven. Hierdoor valt Dar niet langer in de categorie ‘grote vennootschappen’, maar blijft Dar middelgroot. Deze wijziging brengt met zich mee dat Dar, zolang zij middelgroot blijft, niet vanaf boekjaar 2025 verplicht over duurzaamheid hoeft te rapporteren. Ondanks dat Dar op dit moment nog niet verplicht is vanaf boekjaar 2025 te rapporteren, adviseren wij wel in gesprek te blijven met de brancheorganisatie omtrent dit onderwerp en ons te blijven informeren over de analyses die gedaan worden om de belangrijkste thema’s te definiëren. Wij hebben begrepen dat Dar verder gaat met het uitwerken van het beleid omtrent ESG en de rapportage hierover en daarbij de ontwikkelingen vanuit de branche nauwlettend volgt.

Kwalificatie van arbeidsrelaties

Het aantal zelfstandigen zonder personeel (zzp) is de afgelopen jaren flink gestegen. Een deel van deze groep kwalificeert als schijnzelfstandige. Dit betekent dat op basis van wet- en regelgeving eigenlijk sprake is van een arbeidsovereenkomst. Het kabinet vindt deze situatie onwenselijk, omdat de beschermende werking van het arbeidsrecht wordt ontlopen en het sociale stelsel onder druk komt te staan. Daarom zet het kabinet de komende jaren in op het aanscherpen van regels en handhaving.

Sinds de introductie van de Wet DBA in 2016 is sprake van een handhavings-moratorium. Dit betekent dat de Belastingdienst niet controleert en handhaaft op het bestaan van een dienstbetrekking, tenzij sprake is van kwaadwillendheid. Vanaf 1 januari 2025 komt het handhavingsmoratorium naar verwachting te vervallen en gaat de Belastingdienst weer volledig handhaven. Hierdoor kunnen naheffingsrisico’s ontstaan.

Daarnaast werkt het kabinet aan nieuwe wetgeving voor de beoordeling van arbeidsrelaties. In het Hoofdlijnenakkoord is te lezen dat de behandeling van deze wetgeving door het nieuwe kabinet zal worden voortgezet. Kort gezegd zal de nieuwe wetgeving meer nadruk leggen op de vraag of het werk en de werkende organisatorisch zijn ingebed in de organisatie van de werkverschaffer. Daarmee wordt bedoeld of het werk een kernactiviteit van de organisatie vormt en zij aan zij met werknemers wordt verricht. In dat geval zal eerder sprake zijn van een arbeidsovereenkomst. De nieuwe wetgeving zal naar verwachting niet eerder ingaan dan 1 januari 2026.

Organisaties die werken met zelfstandigen die eigenlijk werknemer zijn lopen financiële risico’s. Zo is vanaf 1 januari 2025 sprake van een naheffingsrisico vanuit de Belastingdienst. Ook kunnen zelfstandigen die eigenlijk werknemer zijn vorderingen instellen op grond van arbeidsrechtelijke verplichtingen en kunnen verplichte pensioenregelingen leiden tot pensioenvorderingen. Om dergelijke risico’s te voorkomen is het voor organisaties die zelfstandigen inhuren van belang om de huidige inhuur van zelfstandigen en het inhuurproces onder de loep te nemen.

Gezien de mogelijke risico’s is het voor Dar van belang de ontwikkelingen en gevolgen van het zzp-dossier in beeld te brengen en te houden.

3. Onze bevindingen

3.1 Onze werkzaamheden 12

3.2 Overzicht van onze bevindingen (proces en IT general controls) 13

3.3 Overzicht van onze bevindingen inzake de processen 15

3.4 IT-beheersmaatregelen 16

3.5 Bevindingen IT-beheer | IT General Controls 17

3.6 Bevindingen IT-beheer | per applicatie 18

3.7 Overzicht van onze bevindingen inzake de IT General Controls 19

3.1 Onze werkzaamheden

Controleaanpak en doel van de interim-controle

Het doel van de jaarrekeningcontrole is een oordeel tot uitdrukking brengen over de financiële overzichten. De controle heeft onder meer betrekking op het overwegen van de interne beheersing die voor het opstellen van de financiële overzichten relevant is, teneinde controlewerkzaamheden op te zetten die in de gegeven omstandigheden passend zijn, maar niet met het doel een oordeel over de effectiviteit van de interne beheersing tot uitdrukking te brengen.

Op basis van onze bevindingen bij deze werkzaamheden, geven wij, in het kader van onze natuurlijke adviesfunctie, in deze management letter aanbevelingen over de opzet van de administratieve organisatie en berichten wij u over vast-gestelde tekortkomingen in de uitvoering daarvan en in hoeverre corrigerende maatregelen door management zijn genomen.

De aangelegenheden waarover wij rapporteren betreffen die tekortkomingen die tijdens de controle zijn geïdentificeerd en waarbij wij van mening zijn dat deze voldoende belangrijk zijn om verslag van te doen.

Wij hebben specifiek aandacht besteed aan de volgende processen:
- Het financiële rapporteringsproces
- Het opbrengstenproces
- Het inkoop- en betaalproces
- het personeelsproces
- het proces omtrent IT en automatisering

Toelichting rapportering bevindingen

In deze management letter rapporteren wij onze bevindingen bij de interim-controle. Wij hebben op pagina 13 een overzicht opgenomen waarin wij de risicogradatie van detailbevindingen in de processen hebben weergegeven op basis van de kans dat een risico zich voordoet en de mogelijke impact hiervan.

Vervolgens behandelen wij de bevindingen die wij hebben rondom de processen en vervolgens de ontwikkelingen rondom IT en de bevindingen vanuit onze IT audit.

Totaalbeeld

Uit de door ons uitgevoerde werkzaamheden blijkt dat de interne beheersing van Dar voldoende tot goed is ingericht voor de processen die relevant zijn voor de jaarrekeningcontrole. Wij hebben geconstateerd dat de interne beheersingsmaatregelen veelal in opzet aanwezig zijn. Met name de beheersing van de IT-omgeving zal op een aantal vlakken verbeterd moeten worden om te groeien naar een meer volwassen organisatie. Vanuit het samenvattend overzicht op pagina 16 en 17 komt het beeld naar voren dat op een aantal bevindingen nog onvoldoende voortgang is gerealiseerd. De nuance die wij hierbij aan willen brengen is dat deze bevindingen niet tot verhoogde risico’s leiden. Tevens is onze inschatting dat een deel van deze bevindingen relatief eenvoudig kunnen worden geadresseerd. Onze aanbevelingen tot verbetering zijn opgenomen in de uitwerking van de detailbevindingen in deze management letter vanaf pagina 18.

Vanuit het beeld dat wij nu hebben, met name door de bevindingen in de IT-omgeving, is de verwachting dat wij een gegevensgerichte controle-aanpak zullen hanteren.

3.1 Onze werkzaamheden

Onze inschatting van de risico's

In het kader van de controle van de jaarrekening 2024 en onze aanpak hebben wij een zogenaamde initiële risico-inschatting gemaakt. Wij zien het volgende significante risico in de controle van de jaarrekening van Dar:

- Frauderisico als gevolg van het door het management doorbreken van interne beheersingsmaatregelen; In onze controlestandaarden (NV COS) wordt expliciet het risico van management override (bewuste beïnvloeding door bestuur of management van de jaarcijfers) als belangrijk te onderkennen theoretisch risico benoemd. Als accountant moeten wij in onze werkzaamheden hier specifiek aandacht aan besteden. Wij zijn van mening dat binnen Dar de mogelijkheden, om buiten de getroffen interne beheersmaatregelen invloed uit te oefenen op de in de jaarrekening gepresenteerde uitkomsten, beperkt zijn. Om het resterende risico te beperken beoordelen wij schattingsprocessen en bijzondere journaalposten in detail.
- Frauderisico rondom het bestaan van de opbrengstenverantwoording;
- Fraude en non-compliance.

Controle met aandacht voor fraude en non-compliance

Bij de planning voor de jaarrekeningcontrole, houden wij rekening met het risico dat de jaarrekening als gevolg van fraude en onregelmatigheden afwijkingen van materieel belang zou kunnen bevatten. Onze beroepsorganisatie, de NBA, heeft een notitie uitgebracht 'best practice maatregelen fraude(risico)beheersing voor bestuurders en toezichthouders'. In deze notitie komt nadrukkelijk de rol van bestuurders en toezichthoudende organen, zoals het algemeen bestuur, bij het voorkomen en detecteren van fraude, aan de orde. Door de nadruk te leggen op het voorkomen van fraude, kunnen de gelegenheden die tot fraude leiden, afnemen. Het voorkomen en mitigeren van frauderisico's is primair de verantwoordelijkheid van het directie. Deze aspecten zijn in onze risicoanalyse uitdrukkelijk aan de orde geweest.

Hierbij hebben wij frauderisicofactoren overwogen en de interne beheersing geëvalueerd. Tijdens deze besprekingen hebben wij gesproken over de mogelijke fraude- en non compliancerisico's en mogelijke situaties van onregelmatigheden. Dit hebben wij gedaan aan de hand van de door u opgestelde frauderisicoanalyse en de door u ingevulde compliance vragenlijst.

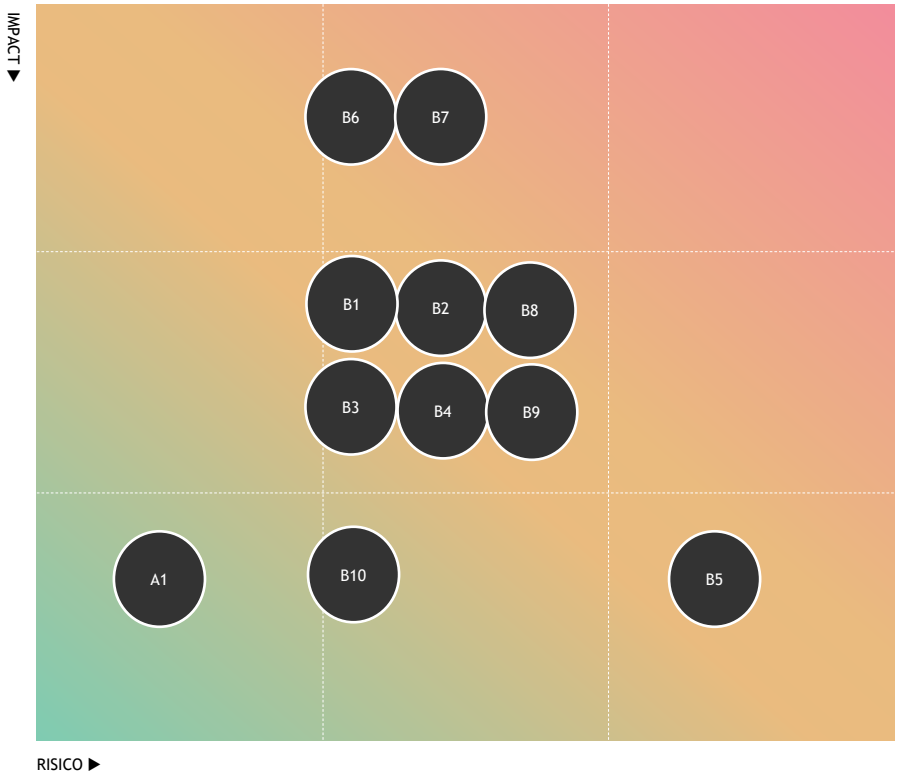
Onze observaties hierbij zijn als volgt:

- Uw frauderisicoanalyse is geformaliseerd;
- Dar kent een gedragscode, een klokkenluidersregeling en incidentenregistratie;
- Ten opzichte van vorig jaar zijn geen zaken gewijzigd in uw frauderisicobeleid;
- Vanwege het ontbreken van een incident-responsplan lijkt Dar nog onvoldoende voorbereid op een grootschalig/Dar-breed fraude-incident of bijvoorbeeld een cyber-aanval;

Wij hebben via de directie van Dar begrepen dat een tweetal incidenten heeft plaatsgevonden omtrent het door drie medewerkers illegaal meenemen van afval van bekenden. De directie heeft de betreffende personeelsleden ontslagen.

Wij hebben naast bovenstaande incidenten geen bevindingen aangetroffen omtrent frauderisico's. Wij hebben daarnaast aandacht besteed aan de compliance met de voor u van toepassing zijnde wet- en regelgeving en overige bepalingen voor zover wij die van belang achten in het kader van onze controle van de jaarrekening. Wij maken hierbij onderscheid tussen wet- en regelgeving die van directe invloed is op de bedragen en toelichtingen in de financiële overzichten en overige wet- en regelgeving die geen directe invloed heeft op de financiële overzichten zelf, maar waarvan naleving van fundamenteel belang kan zijn voor de operationele activiteiten. Deze werkzaamheden worden bij de eindejaarscontrole uitgevoerd.

3.2 Overzicht van onze procesbevindingen



Hierboven is een grafische weergave opgenomen van onze visie op de mate van risico en impact van de geconstateerde bevindingen in relatie tot de maatregelen van interne beheersing in de relevante processen. Verderop in deze management letter hebben wij de bevindingen nader toegelicht waarin wij ingaan op de bevinding, het risico voor Dar, mogelijke oplossingen ter adressering van de bevinding en de eventuele gevolgen voor onze accountantscontrole.

OVERZICHT DETAILBEVINDINGEN	
A	Detailbevindingen processen
A1	Bankrechten in bankapplicatie
B	Detailbevindingen IT General Controls
B1	Procedure autorisatiebeheer - Voor Exact Synergy, Exact Globe, BORVision en Clear is geen formele normpositie, goedgekeurd door het management, beschikbaar.
B2	Procedure autorisatiebeheer - Voor BORVision en Clear worden gebruikersaccounts niet ten alle tijden op of voor de uitdienstdatum geblokkeerd.
B3	Periodieke controle op juistheid ingerichte autorisaties - Een periodieke controle voor Exact Synergy, Exact Globe, BORvision en Clear wordt niet uitgevoerd.
B4	Identificatie van gebruikers voor toegang tot systemen en data - Voor Exact Globe zijn handelingen en transacties van generieke accounts niet herleidbaar naar een individuele gebruiker.
B5	Authenticatie - Binnen de Active Directory zijn enkele administrator accounts welke zijn uitgezonderd van het periodiek wijzigen van wachtwoorden.
B6	Administrator- en Superuser-accounts - In de Active Directory en Clear zijn beheerdersbevoegdheden belegd in de gebruikersorganisatie.
B7	Database autorisaties - In de database van BORVision zijn beheerdersbevoegdheden belegd binnen de gebruikersorganisatie.
B8	Wijzigingsbeheer - Voor Exact Synergy en Exact Globe wordt geen ISAE 3402 rapportage opgevraagd en beoordeeld.
B9	Gescheiden omgevingen – Binnen BORVision zijn autorisaties met betrekking tot ontwikkelen en doorvoeren van wijzigingen niet inzichtelijk
B10	Restore-test - Van de uitgevoerde restoretest zijn de uitkomsten niet gedocumenteerd

3.3 Overzicht van onze bevindingen inzake de processen

#	BEVINDING - INCL. RISICO	AANBEVELING	REACTIE MANAGEMENT
A1	Gedurende onze werkzaamheden hebben wij geconstateerd dat vertrekkend personeel met rechten in de bankapplicatie niet tijdig worden gedeactiveerd, waardoor deze nog actief zijn op het moment dat zij niet meer werkzaam zijn bij Dar. Op basis van onze waarnemingen tijdens de controle van de wijzigingen in de bankrechten hebben wij gezien dat vorige bedrijfscontroller nog rechten heeft in de bankapplicatie per september 2024, terwijl hij niet meer werkzaam is bij Dar sinds juli 2024. Hoewel een vier-ogen principe is ingeregeld in de bankapplicatie voor wijzigingen die gemaakt worden op dit niveau, brengt dit niet direct een risico op onrechtmatige handelingen met zich mee, maar wel op ongeautoriseerde toegang. Gezien de personeelswisselingen op dit niveau in 2024 adviseren wij aandacht te besteden aan de activatie en de-activatie van de bankrechten.	Als gevolg van het feit dat bankrechten niet tijdig worden ingetrokken bestaat het risico dat gebruikers (nog tijdelijk) toegang houden tot de applicatie, waardoor sprake is van ongeautoriseerde toegang tot de bankapplicatie. Wij adviseren daarom de bankrechten mee te nemen als onderdeel van de stappen die de betreffende afdeling middels de loopbrief bij uitdiensttreding moet uitvoeren. Hierdoor wordt gewaarborgd dat de bankrechten tijdig worden ingetrokken. Op deze manier kan ongeautoriseerde toegang worden voorkomen.	Bij de nieuw ontvangen overzicht van de gebruikers in de bankapplicatie op 14 oktober is de bedrijfscontroller die uit dienst is gegaan niet langer actief in de bankapplicatie. Hiermee zijn zijn rechten dus ingetrokken.

3.4 IT-beheersmaatregelen

IT-audit algemeen

In het kader van de jaarrekeningcontrole is een IT-audit uitgevoerd. De IT-audit is primair gericht op de betrouwbaarheid van de gegevensverwerking ten behoeve van de totstandkoming van de jaarrekening. Dit betekent dat de uitkomsten van de IT-audit geïnterpreteerd moeten worden met de uitkomsten van de andere werkzaamheden van de accountant en de IT-audit zich niet primair richt op het doen van uitspraken omtrent de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking als geheel of van onderdelen daarvan. Het inzicht in de betrouwbare werking van ICT-systemen en applicaties en het gebruik daarvan door Dar, vormen een onderdeel van de kwaliteit van de interne beheersing en de administratieve organisatie. Algemene IT-beheersmaatregelen (hierna: IT General Controls) rond uw kritieke systemen leveren daarnaast onder meer een belangrijke bijdrage aan het mitigeren van de risico's op onbeheerste wijzigingen, ongeautoriseerde handelingen en het optreden van verstoringen en het beperken van de 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 voor zover relevant voor de jaarrekeningcontrole. Wij hebben deze maatregelen beoordeeld om de impact van de risico's vanuit IT te kunnen vaststellen voor die systemen en applicaties die gekoppeld zijn aan de voor ons relevante processen en posten. Wij hebben bij deze beoordeling de bevindingen vanuit 2023 meegenomen, opnieuw de situatie omtrent IT-beheersing in kaart gebracht en de actuele situatie en bevindingen vanaf pagina 16 opgenomen in deze management letter.

Op het moment dat de intern getroffen IT General Controls rondom de applicaties in scope niet (bewijsbaar) voldoende aanwezig zijn, dan heeft dit mogelijk invloed op interne beheersingsmaatregelen in de applicaties en rapportages vanuit de applicaties.

Toelichting status IT General Controls

Het hierna opgenomen schema bevat een weergave van de status van de opzet en het bestaan van de door ons in het kader van de jaarrekeningcontrole onderzochte IT General Controls in het huidig jaar en in voorgaand jaar binnen de onderzochte systemen, zijnde Exact Synergy, Exact Global, BORvision, Clear. Onze relevante bevindingen met betrekking tot de IT General Controls en overige IT-gerelateerde bevindingen treft u hierna aan.

Op de volgende pagina's zijn vervolgens onze bevindingen met betrekking tot de IT General Controls tekstueel nader toegelicht per item, verdeeld naar logische toegangsbeveiliging en change management voor de applicaties en operating system gerelateerd aan de IT-omgeving. Tenslotte zijn onze overige IT-gerelateerde bevindingen uiteengezet. De scope van relevante IT General Controls wordt jaarlijks beoordeeld en kan hierdoor afwijken van de scope van voorgaande jaren.

Geautomatiseerde gegevensverwerking

De accountant dient op basis van artikel 2:393, lid 4 BW aandacht te besteden aan de bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

Wij hebben de automatiseringsorganisatie uitsluitend in het kader van de jaarrekeningcontrole beoordeeld. Voor een verdere uitwerking van de bevindingen over de continuïteit en betrouwbaarheid van de geautomatiseerde gegevensverwerking verwijzen wij naar de volgende pagina's.

3.5 Bevindingen IT-beheer | IT General Controls

Algemene IT-beheersing

Wij hebben in onderstaande tabel onze bevindingen opgenomen rondom de algemene IT-beheersing, waarbij wij voor deze onderzochte gebieden op hoofdlijnen onze bevindingen hebben opgenomen. Wij constateren dat de beheersing op een aantal onderdelen nog niet toereikend is ingericht. Het gaat dan om bevindingen met betrekking tot de Active Directory/ operating system of waar sprake is van bevindingen die voor alle applicaties van Dar gelden. Op de volgende pagina hebben wij vervolgens per applicatie opgenomen welke aanvullende bevindingen wij hebben. Vanaf pagina 18 hebben wij de bevindingen in detail uitgewerkt.

PROCES	KORTE OMSCHRIJVING BEVINDINGEN
Logische toegangsbeveiliging	
1. Procedure autorisatiebeheer	Geen normposities uitgewerkt voor autorisaties (B1)
2. Periodieke controle op toegang en juistheid ingerichte autorisaties	Periodieke controles vinden niet plaats op ingerichte autorisaties (B3)
3. Identificatie	Geen significante bevindingen voor de algemene IT-beheersing
4. Authenticatie	Wij hebben vastgesteld dat persoonlijke gebruikersaccounts zijn uitgezonderd van het periodiek wijzigen van wachtwoorden (operating system) (B5)
5. Administrator- en superuser-accounts	In de Active Directory (operating system) en Clear zijn beheerdersbevoegdheden belegd in de gebruikersorganisatie (B6)
6. Database toegang	Geen significante bevindingen voor de algemene IT-beheersing
Change management	
7. Wijzigingsbeheer applicaties	Geen significante bevindingen voor de algemene IT-beheersing
8. Gescheiden IT-omgevingen	Geen significante bevindingen voor de algemene IT-beheersing
Continuïteit	
9. Back-up maatregelen	Geen significante bevindingen voor de algemene IT-beheersing
10. Restoretest	Van de uitgevoerde restoretest zijn de uitkomsten niet gedocumenteerd (B10)

3.6 Bevindingen IT-beheer | per applicatie

Per applicatie

PROCES	Exact Synergy	Exact Globe	Borvision	Clear
Logische toegangsbeveiliging				
1. Procedure autorisatiebeheer (B2)	●	●	●	●
2. Identificatie van gebruikers voor toegang tot applicaties (B4)	●	●	●	●
3. Administrator- en superuser-accounts (B6)	●	●	●	●
4. Database toegang (B7)*	○	○	●	●
Change management				
5. Wijzigingsbeheer applicaties (B8)**	●	●	○	○
6. Gescheiden IT-omgevingen (B9)	●	●	●	○

* *Voor Exact Synergy en Exact Globe is de database toegang niet onderzocht, omdat sprake is van SaaS-oplossingen*

** *De ISAE3402 verklaringen voor Exact Synergy en Exact Globe zijn nog niet opgevraagd, deze zullen per jaareinde beschikbaar zijn en beoordeeld worden.*

● onvoldoende ● verbeterpunten ● voldoende ● geen waarneming ○ niet onderzocht

3.7 Overzicht van onze bevindingen inzake de IT General Controls

#	BEVINDING - INCL. RISICO	AANBEVELING	REACTIE MANAGEMENT
B1	Autorisaties worden toegekend naar inzicht van de applicatiebeheerder. Autorisaties worden niet toegekend op basis van een formele normpositie, die is goedgekeurd door het management van DAR. Hierdoor is het autorisatiebeheer nog niet toereikend. Als gevolg van tekortkomingen met betrekking tot autorisatiebeheer bestaat het risico dat de toekenning van rechten niet in lijn ligt met de organisatorische rollen en functies van medewerkers. Hierdoor kunnen zij beschikking krijgen over ruimere autorisaties dan noodzakelijk voor uitoefening van hun functie, dan wel kunnen zij beoogde functiescheiding doorbreken.	Wij adviseren een normpositie (SOLL-positie) op te stellen waarbij de voornaamste rechten en functiescheidingen in kaart worden gebracht en toegekend aan functies binnen de organisatie. Het startpunt voor het opstellen van deze positie ligt bij het identificeren van de vereisten inzake functiescheiding vanuit de operationele processen van DAR. Een normpositie beschrijft vervolgens de vereisten die DAR stelt aan functiescheiding, en vertaalt deze in de kritieke rollen in Exact Synergy, Exact Globe, BORVision en Clear per gebruikersgroep (functie). Wij adviseren deze te laten autoriseren door het management van DAR.	De autorisatiematrix wordt in 2024 opgeleverd door afdeling I&A. Daarnaast loopt het project 'in- door- en uitstroom' waarmee het indiensttredingsproces wordt geoptimaliseerd. Het gebruik en de controle van de autorisatiematrix zal in dit proces worden opgenomen.
B2	Specifiek voor de applicaties BORVision en Clear geldt dat een gebruikersaccount bij een uitdiensttreding niet te allen tijde op of vóór uitdienstdatum worden geblokkeerd. Een formeel uitdienst-proces is niet aanwezig en het verwijderen van gebruikers gebeurt op basis van een regelmatige controle door de functioneel beheerder. Als gevolg van het feit dat autorisaties mogelijk niet tijdig worden ingetrokken bestaat het risico dat gebruikers onterecht toegang behouden tot BORVision en Clear, waardoor het risico bestaat dat zij ongeautoriseerde handelingen uitvoeren of de beoogde functiescheiding doorbreken.	Wij adviseren een proces in te richten dat zorg draagt voor het tijdig blokkeren van gebruikersaccounts als medewerkers uit dienst treden.	HR gaat I&A maandelijks de lijst met uitdiensttreders sturen. Dit is een geautomatiseerd proces via 'connect'. I&A zal zorgdragen voor tijdige blokkering van de gebruikersaccounts als medewerkers uit dienst treden.

3.7 Overzicht van onze bevindingen inzake de IT General Controls

#	BEVINDING - INCL. RISICO	AANBEVELING	REACTIE MANAGEMENT
B3	Voor Exact Synergy, Exact Globe, BORvision en Clear is geen zichtbare controle uitgevoerd op de actualiteit van gebruikers en juistheid van de toegewezen autorisaties. Doordat gedurende het boekjaar geen review is uitgevoerd op de ingerichte autorisaties, loopt DAR het risico dat medewerkers over ruimere autorisaties dan noodzakelijk voor uitoefening van hun functie beschikken, dan wel de beoogde functiescheiding kunnen doorbreken. Teven kan met de huidige werkwijze van controleren een fout in de autorisatietoekenning te laat of niet worden opgemerkt met mogelijke doorbreking van functiescheiding en ongewenste mutaties tot gevolg.	Wij adviseren DAR een periodieke review (bijv. halfjaarlijks, jaarlijks) uit te voeren waarin achteraf, tegen de normpositie, wordt nagegaan of gebruikers teveel/onjuiste rollen/rechten toegekend hebben gekregen en deze waar nodig te corrigeren.	Binnen I&A wordt maandelijks gecontroleerd op de gebruikers. Echter beschikken wij (nog) niet over een autorisatiematrix, deze is nog in ontwikkeling (zie ook B.1).
B4	Wij hebben vastgesteld dat in Exact Globe diverse generieke gebruikersaccounts aanwezig zijn, die door meerdere medewerkers actief worden gebruikt om toegang tot de applicatie te verkrijgen. Als gevolg zijn handelingen en transacties, die mogelijk zijn uitgevoerd met deze accounts, niet herleidbaar naar een individuele gebruiker. Het risico bestaat dat handelingen en transacties in het systeem niet herleidbaar zijn tot een individuele medewerker en dat mogelijk onrechtmatige transacties plaatsvinden dan wel dat functiescheidingen al dan niet opzettelijk worden doorbroken.	Wij adviseren het gebruik van niet-persoonsgebonden gebruikersaccounts en de hieraan gekoppelde autorisaties tot een minimum te beperken.	In verband met continuïteit (vakanties/ziekte) van de crediteuren processen (autorisatie) worden algemene folders in Synergy gebruikt. Risico is zeer beperkt aangezien hier alleen inkoopfacturen in terecht komen die gematcht moeten worden - er moet dus ook een inkooporder gegenereerd zijn. Met deze rechten kun je alleen in deze bak - geen andere rechten in Synergy.
B5	Op basis van de analyse van de Active Directory hebben we vastgesteld dat enkele administrator accounts zijn uitgezonderd van het periodiek wijzigen van wachtwoorden. Het risico bestaat dat voor de accounts waarvoor de periodieke wijziging van het wachtwoord is uitgeschakeld, het wachtwoord intern bekend raakt, waardoor deze gebruikersaccounts ongemerkt misbruikt kunnen worden. Daarbij beschikken deze accounts over hoge rechten. Hierdoor bestaat een verhoogd risico dat functiescheidingen worden doorbroken als met deze accounts door middel van de beheerrechten ongeautoriseerde aanpassingen in het systeem worden doorgevoerd.	Om de bevinding te adresseren adviseren wij u het periodiek wijzigen van het wachtwoord op gebruikersniveau niet uit te schakelen, zodat alle gebruikers met toegang tot de Active Directory aan het wachtwoordbeleid voldoen. Als deze instelling wordt aangepast, zullen alle gebruikers ten minste elke 180 dagen het wachtwoord wijzigen.	Per direct worden administrator accounts elke 180 dagen aangepast.

3.7 Overzicht van onze bevindingen inzake de IT General Controls

#	BEVINDING - INCL. RISICO	AANBEVELING	REACTIE MANAGEMENT
B6	In de Active Directory en Clear zijn hoge bevoegdheden toebedeeld aan gebruikers, die formeel werkzaam zijn vanuit de lijnorganisatie. Hierdoor is de gewenste functiescheiding niet gewaarborgd. Gebruikersaccounts met hoge bevoegdheden beschikken over alle rechten en kunnen hiermee de gewenste functiescheiding doorbreken en eventueel ongeautoriseerde wijzigingen doorvoeren. Dit is een inherent risico van accounts met hoge bevoegdheden, dat aanzienlijk wordt verhoogd door deze accounts te beleggen in de lijnorganisatie	Wij adviseren DAR het gebruik van verhoogde rechten alleen beschikbaar te stellen voor gebruikers die deze rechten uit hoofde van hun functie nodig hebben en die geen onderdeel zijn van de lijnorganisatie. In lijn hiermee adviseren wij de toedeling van hoge bevoegdheden onderdeel te maken van autorisatiematrices en periodiek te controleren op juiste toekenning en noodzaak van de toekenning.	Binnen Clear is één gebruiker (Pdrunen@dar.nl) die teveel rechten (applicatiebeheerder) zou hebben. Hij wordt onderdeel van de gebruikersgroep DARDAT. De gebruiker (sengels@dar.nl) is reeds uit dienst.
B7	In de database van BORVision zijn kritieke database autorisaties belegd binnen de gebruikersorganisatie, waardoor gewenste functiescheiding niet wordt gewaarborgd. Gebruikersaccounts met hoge bevoegdheden beschikken over alle rechten en kunnen hiermee de gewenste functiescheiding doorbreken en eventueel ongeautoriseerde wijzigingen doorvoeren. Dit is een inherent risico van accounts met hoge bevoegdheden, dat aanzienlijk wordt verhoogd door deze accounts te beleggen in de lijnorganisatie	Wij adviseren een grondige analyse uit te voeren op de huidige autorisaties in de database van BORVision en deze te herzien waar nodig. Hierbij kan worden gekeken naar functieverantwoordelijkheden van gebruikers en of zij daadwerkelijk de benodigde autorisaties nodig hebben.	Zie punt B1. Qua planning wordt dit in Q1 2025 aangepast.
B8	DAR heeft geen procedure voor wijzigingsbeheer opgesteld. Exact Synergy en Exact Globe zijn SaaS-applicaties. Beheersmaatregelen rondom wijzigingsbeheer en continuïteit liggen daarmee gedeeltelijk bij de leverancier. Hiertoe kan beoordeling van verstrekte ISAE3402 bijdragen aan het inzichtelijk maken van de beheersmaatregelen die door de leverancier zijn getroffen en of deze toereikend zijn dan wel dat Dar zelf nog aanvullende maatregelen zou moeten treffen. Tot nu toe is een dergelijke rapportage niet opgevraagd en beoordeeld. Het risico van het niet uitvoeren van adequate veranderingsbeheer-procedures is dat ongeautoriseerde of ongecontroleerde wijzigingen in de productieomgeving kunnen worden geïntroduceerd. Dit kan onverwachte nadelige effecten hebben op gegevens (bijv. corruptie, verwijdering, integriteit) en/of IT-systeemprestaties of beschikbaarheid (bijv. uitval, prestatiedegradatie).	Wij adviseren een beoordeling op de inhoud van de ISAE 3402 assurance rapportage uit te voeren om de impact op het dagelijks gebruik van de applicaties Exact Synergy en Exact Globe in te schatten. Naar wij hebben begrepen zal deze beoordeling bij de jaarrekeningcontrole uitgevoerd worden. Daarbij adviseren wij het uitvoeren van deze beoordeling te documenteren, zodat deze beoordeling achteraf aantoonbaar is. Als de inhoud van de rapportage daar aanleiding toe geeft, adviseren wij maatregelen te treffen om de impact op de organisatie te beperken. Naar wij hebben begrepen zal deze beoordeling bij de jaarrekeningcontrole uitgevoerd worden.	Wij voeren geen wijzigingen uit op genoemde applicaties. Dat doet Business Expert namens ons. Gegevens zijn opgevraagd bij Business Expert, zij beschikken niet over een ISAE3402 rapportage. Exact en Global-E data center beschikken beide wel over een ISAE3402 verklaring.

3.7 Overzicht van onze bevindingen inzake de IT General Controls

#	BEVINDING - INCL. RISICO	AANBEVELING	REACTIE MANAGEMENT
B9	Binnen BORVision bestaat de mogelijkheid om in de applicatie zelf wijzigingen te ontwikkelen en door te voeren. Wij hebben echter geen inzage kunnen krijgen in de autorisaties met betrekking tot het ontwikkelen en doorvoeren van wijzigingen. Het ontbreken van duidelijke autorisaties voor het ontwikkelen en doorvoeren van wijzigingen kan resulteren in ongeautoriseerde wijzigingen en onvoldoende controle over de wijzigingen. Dit kan leiden tot fouten, onjuiste gegevens of beveiligingsproblemen en kan het moeilijk maken om de verantwoordelijkheid te achterhalen bij problemen.	Wij adviseren het proces van wijzigingsbeheer inzichtelijk te documenteren en, indien nodig, daarbij functiescheiding in te voeren. Daarmee kunnen verstoringen in actieve bedrijfsprocessen, als gevolg van ongeautoriseerde of onvoldoende geteste aanpassingen in de productieomgeving, worden voorkomen.	Wijzigingen in programmatuur worden in de praktijk niet door Dar doorgevoerd, maar door een externe partij. Wij achten derhalve het benoemde risico beperkt aanwezig.
B10	Van de uitgevoerde restoretest zijn de uitkomsten niet gedocumenteerd. Het niet vastleggen van de uitkomsten van een uitgevoerde restoretest kan leiden tot een gebrek aan inzicht in de effectiviteit van het back-up en herstelproces en het vermogen om eventuele problemen op te lossen.	Wij adviseren alle uitgevoerde restoretest te rapporteren waarbij de conclusies gestructureerd worden opgeslagen.	Een restoretest wordt nog in 2024 uitgevoerd. Bevindingen kunnen worden gedeeld. Daarna zal een restoretest jaarlijks plaatsvinden.