

2.2 IT audit algemeen

Introductie

In het kader van de jaarrekeningcontrole hebben wij een IT-audit naar de opzet en het bestaan van de algemene IT-beheersmaatregelen uitgevoerd. Dit zijn de beheersmaatregelen die uw organisatie heeft getroffen om ervoor te zorgen dat de IT-systemen betrouwbaar en integer zijn. Ze leveren 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. We hebben deze maatregelen beoordeeld met betrekking tot de voor de jaarrekening belangrijkste applicaties, waaronder Jaamo, AFAS, Factuur+.

Daarnaast hebben wij ook een IT-audit uitgevoerd op de systemen Jaamo en AFAS met betrekking tot het omzetproces en urenverwerking. Daarbij hebben we ons inzicht en begrip van deze processen ondersteund door Jaamo en/of AFAS geactualiseerd en de geautomatiseerde beheersmaatregelen opnieuw geïdentificeerd en beoordeeld.

Onze IT-auditwerkzaamheden hebben niet als doel gehad om te komen tot een beoordeling van de IT-organisatie of IT-omgeving als geheel, maar zijn uitsluitend gericht geweest op het verkrijgen van voldoende zekerheid ten aanzien van de continue, betrouwbare werking van de IT-omgeving van Dak Kindercentra voor zover relevant in het kader van de controle van de beginbalans en jaarrekening.

Ons beeld bij uw IT-omgeving en beheersing van uw IT

Op basis van gesprekken met uw de IT-verantwoordelijken en betrokken medewerkers vanuit Klantadvies, HR en Finance hebben wij een goed algemeen beeld gekregen van de IT-omgeving en applicaties bij Dak Kindercentra.

Wij hebben vastgesteld dat Dak Kindercentra zich bewust is van het belang van IT voor de organisatie, maar ook van de afhankelijkheid en kwetsbaarheid daarvan. Daarom geeft Dak Kindercentra verschillende IT-beheersmaatregelen getroffen om haar IT-risico's te kunnen mitigeren. De invulling van de belangrijkste IT-beheersmaatregelen zijn onder andere gebaseerd het informatiebeveiligingsbeleid. De maatregelen zijn daarbij echter nog niet altijd geformaliseerd en gedocumenteerd en worden nog niet altijd op basis van monitoring gecontroleerd.

Jaamo en AFAS zijn belangrijke applicaties voor Dak Kindercentra. Deze applicaties zijn standaard softwareoplossingen en worden afgenomen op basis van 'Software as a Service'. Dit betekent dat Dak Kindercentra voor deze oplossingen grotendeels wordt ontzorgd met betrekking tot IT-beheersmaatregelen, waaronder ontwikkeling en uitrol van updates, back-up & recovery en beveiliging van deze onlineoplossingen. De functionaliteiten van deze softwareoplossingen bieden Dak Kindercentra ondersteuning van haar operationele en financiële processen en vullen een groot deel van de informatievoorziening in.

2.2 IT audit algemeen



Ons beeld bij uw IT-omgeving en beheersing van uw IT (vervolg)

Ook wij maken in onze auditaanpak gebruik van deze oplossingen. Met name met betrekking tot het primaire proces van contracteren tot en met facturatie, financiële verwerking en urenregistratie. De functionaliteiten van beide systemen in combinatie met de wijze waarop Dak Kindercentra deze systemen toepast geven ons een bepaalde mate van comfort met betrekking tot de financiële verwerking van de opvang en uren. Hierdoor steunen wij deels op de systemen in combinatie met aanvullende gegevensgerichte werkzaamheden.

Gezien de afhankelijkheid en kwetsbaarheid van deze systemen voor zowel Dak Kindercentra als onze auditaanpak adviseren wij Dak Kindercentra zelf de monitoring van deze oplossingen en bijbehorende diensten van de leveranciers aan te scherpen. Hiermee kan worden vastgesteld of de betreffende leverancier hun diensten met betrekking tot bijvoorbeeld ontwikkelen en uitrollen van hun oplossing, beveiliging, back-up ed. op orde hebben en of dit aansluit bij de risico's van Dak Kindercentra. Dit kan onder andere door het jaarlijks opvragen van derdenverklaringen (AFAS isae3402), uitoefenen van het recht op audit en/of het periodiek laten rapporteren over de diensten en prestaties (vb. SLR).

Veiligheid en continuïteit

Gezien het gebruik van de verschillende systemen ter ondersteuning van de Dak kindercentra dienstverlening en de daarin aanwezige (klant, kind data) is het van belang dat de systemen beschikbaar en veilig zijn. Dak Kindercentra en haar IT-leveranciers hebben hiervoor verschillende IT-beheersmaatregelen getroffen.

Echter als gevolg van ontwikkelingen bijvoorbeeld op het gebied van technologie en cyber is het van belang continue aandacht te houden voor deze IT-beheersmaatregelen en de (cyber)weerbaarheid op het gewenste niveau te houden. Vandaag de dag is vooral cybersecurity een aandachtspunt gezien de mate van digitalisering en het aantal pogingen dat hackers doet om omgevingen te raken.

Wij adviseren Dak Kindercentra haar (cyber)weerbaarheid te vergroten door periodiek een risicoanalyse uit te voeren en haar uitgangspunten en randvoorwaarden voor informatiebeveiliging vast te leggen in een informatiebeveiligingsbeleid. Deze twee tezamen vormen dan de basis (Plan) voor de IT-beheersmaatregelen die voor Dak Kindercentra een veilige en continue geautomatiseerde gegevensverwerking en dienstverlening moeten waarborgen. De IT-beheersmaatregelen zijn daarbij dus van groot belang (Do), daarom adviseren wij deze ook periodiek te controleren op een effectieve werking (Check) en te optimaliseren of te vernieuwen als de risico's daarom vragen of de uitvoering niet heeft gewerkt (Act). Ook als deze zijn verlegd naar IT-leveranciers. Om dit stelsel te laten werken adviseren wij dit ook onderdeel te laten zijn van een Plan-Do-Check-Act cyclus en de beheersmaatregelen te formaliseren en documenteren.

2.2 IT audit algemeen



Veiligheid en continuïteit

Hiervoor kan Dak Kindercentra de uitgangspunten of structuur van een normenkader gebruiken. Dit kan bijvoorbeeld de code voor informatiebeveiliging zijn (ISO27001). De overheid stimuleert ook steeds meer het bewustzijn en nemen van maatregelen met betrekking tot informatiebeveiliging. Of ze dwingt deze zelfs af met wet- en regelgeving. De NIS2 richtlijn is er daar een van. De exacte invulling van deze richtlijn voor Nederland moet nog definitief bepaald worden. Wel is bekend dat organisaties hierbij hun cyberbeveiligingsprocessen tot een volwassen niveau moeten brengen en voldoen aan rapportageverplichtingen. Of Dak Kindercentra binnen de scope valt is daarmee nog niet duidelijk. Wel dat haar maatregelen op een volwassen niveau zijn, maar nog gewerkt zal moeten worden aan o.a. de rapportageverplichtingen. Wij adviseren de ontwikkelingen te volgen en zodra de wetgeving voor Nederland bekend is te toetsen in welke mate eraan wordt voldaan en waar nodig eventuele acties nodig zijn.

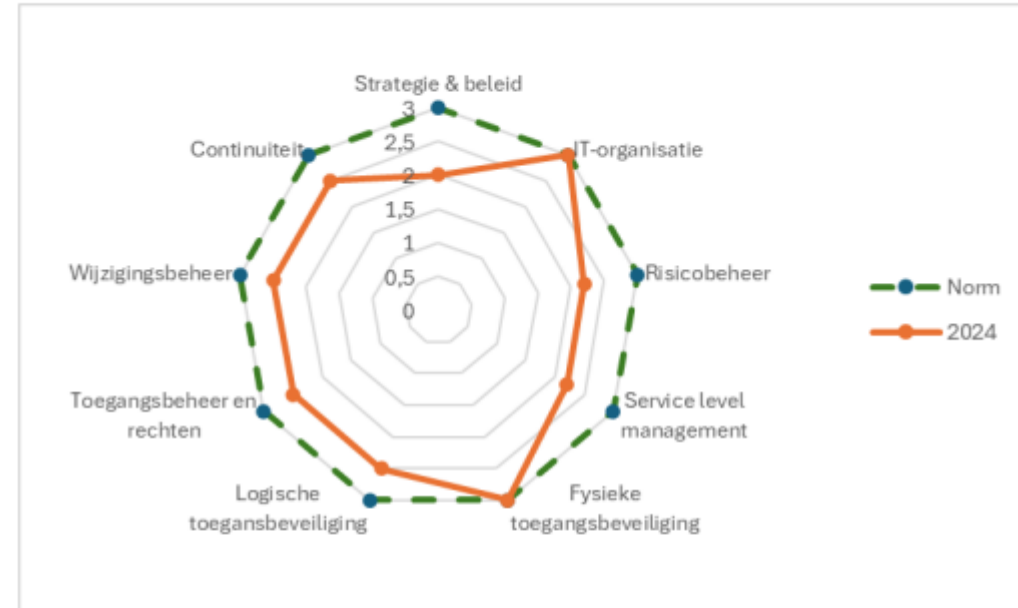
Daarnaast onderkennen wij een grote mate van afhankelijkheid van Jaamo. Jaamo betreft een relatief jonge en kleine organisatie met de daarbij behorende problematiek qua performance en professionaliteit. Wij achten het van belang dat Dak/Stichting Collectief Kindontwikkeling nagaat of Jaamo op de lange termijn de partner en oplossing is, die hun processen en informatievoorziening optimaal kan blijven ondersteunen.

2.2 IT audit algemeen

Hoe beoordelen wij het volwassenheidsniveau van de IT-beheersing?

Wij beoordelen de IT-omgeving van Dak Kindercentra aan de hand van een volwassenheidsmodel. Dit model heeft 5 niveaus, waarbij niveau 1 het laagste volwassenheidsniveau is en 5 het hoogste niveau.

Niveau 3 is de minimale norm voor meeste organisaties. Gezien de activiteiten i.c.m. het applicatielandschap bij Dak Kindercentra adviseren wij dat uw ambitieniveau op de norm van niveau 3 komt te liggen. Op dit moment liggen de IT-beheersmaatregelen tussen de niveaus 2 en 3 in. Dit is vergelijkbaar met 2023. Op de volgende pagina's zijn de belangrijkste bevindingen en adviezen opgenomen om te groeien naar het niveau 3.



2.3 IT – Samenvatting bevindingen

Proces	2024	2023	Korte toelichting	Referentie
IT Governance				
1. IT-strategie	●	●	Geen strategische IT-plannen, wat plausibel is gezien aard en omvang van de organisatie.	1
2. IT/Cyber risicoanalyse	●	●	Dak beschikt niet over een gestructureerde en geformaliseerde cyber/IT risicoanalyse	2
3. IT-monitoring	●	●	Dak voert geen structurele en eenduidige monitoring uit op haar IT-beheersmaatregelen of die van haar IT-partners.	3
Computer operations				
4. Calamiteitenplan	●	●	Dak beschikt niet over een calamiteitenplan of business recoveryplan dat periodiek wordt getest.	4
Informatiebeveiliging				
5. Vulnerability scans	●	●	Er wordt niet structureel periodiek een penetratietest of andere vulnerability scans uitgevoerd	5
Toegangsbeveiliging				
6. Super users	●	●	Operationele gebruikers hebben sterke rechten (o.a. super of administrator) in de applicaties AFAS, Jaamo en Factuur+.	6
7. Active directory	●	●	'Password never expires' actief voor verschillende accounts.	7
8. Entra ID	●	●	Voor pedagogisch medewerkers met alleen webmail MFA nog niet ingeregeld voor de Citrix omgeving.	8
9. Change management	●	●	Geen formele change management procedure waarmee (kritische) software en configuratiewijzingen op een eenduidige, aantoonbare en structurele wijze worden uitgevoerd.	9
AFAS				
10. AFAS boekingen	●	●	Boeking die vanuit Jaamo worden ingelezen in AFAS kunnen in AFAS nog onderhouden of verwijderd worden.	10

De details van deze bevindingen zijn als bijlage bij deze management letter opgenomen.

- Bevinding met lage prio
- Bevinding met middel prio
- Bevinding met hoge prio
- Niet van toepassing

2.2 IT – reactie management



Bevindingen die we oppakken (korte termijn):

- **Autorisatierechten en toegangsbeveiliging:**
Er wordt een project gestart om sterke rechten (zoals administrator-rechten) te herstructureren. Alleen functioneel beheerders krijgen toegang tot kritieke rollen, en MFA wordt verplicht gesteld voor alle gebruikers, inclusief pedagogisch medewerkers met webmailtoegang.
- **Herstelplan:**
We zijn begonnen met de voorbereidingen op het opstellen van een incident respons en herstelplan in samenwerking met onze IT-partners. Naar verwachting zal dit nog voor het einde van 2024 zijn opgesteld. Workshop business impact analyse vindt waarschijnlijk eind november, doch begin december plaats.

Bevindingen die we nog niet direct oppakken:

- **Periodieke vulnerability scans:**
We zullen in gesprek gaan met een partij die ons periodiek kan ondersteunen bij dit onderwerp. We onderzoeken de mogelijkheden om dit structureel op te nemen in de IT-kalender vanaf Q2-3 | 2025
- **Formaliseren change management:**
Dit staat op onze roadmap, maar gezien de huidige omvang en complexiteit van wijzigingen achten we dit momenteel minder urgent. De focus ligt eerst op toegangsbeveiliging en monitoring.

Bijlage bij 2.3 - IT bevindingen

#	Bevinding / risico	Aanbeveling	Impact op controle
1	<p>Dak beschikt niet over een geformaliseerde IT-strategie. Keuzes en invullingen worden gemaakt o.b.v. een aantal algemene uitgangspunten.</p> <p>Hiermee loopt Dak de kans dat de keuzes, invulling en borging van IT niet aansluit bij haar ambities en verwachtingen en processen, informatievoorziening etc niet maximaal ondersteund.</p>	<p>Wij adviseren op basis van de ambities en doelstellingen van Dak een IT-beleid op te zetten waarin de richting, randvoorwaarden en uitgangspunten voor IT zijn gedefinieerd ter ondersteuning van de bedrijfsvoering en doelstellingen. Dit als basis voor de invulling van IT en toekomstige keuzes.</p>	<p>Geen directe impact gegeven de gegevensgerichte controle-aanpak.</p>
2	<p>Dak beschikt niet over een gestructureerde en geformaliseerde cyber/IT risicoanalyse waarmee haar risico's, afhankelijkheden en kwetsbaarheden m.b.t. bijvoorbeeld informatiebeveiliging, cyber en continuïteit inzichtelijk zijn gemaakt.</p> <p>De getroffen beheersmaatregelen kunnen hierdoor mogelijk niet in lijn zijn met de behoeften of verwachtingen van Dak en daarmee onder of over presteren.</p>	<p>Wij adviseren periodiek een IT/cyber risicoanalyse uit te voeren en deze op te nemen in een Plan-Do-Check-Act cyclus waarin risico's en maatregelen worden benoemd, gemonitord en opgevolgd. Op basis van deze risicoanalyse ook de afhankelijkheden en kwetsbaarheden m.b.t. IT vast te stellen. Dit, samen met het informatiebeveiligingsbeleid, als basis voor de getroffen of nog te treffen beheersmaatregelen.</p>	<p>Geen directe impact gegeven de gegevensgerichte controle-aanpak.</p>
3	<p>Dak voert geen structurele en eenduidige monitoring uit op haar IT-beheersmaatregelen of die van haar IT-partners.</p> <p>Hierdoor loopt Dak de kans dat risico's niet adequaat worden gemitigeerd en/of de omgeving niet werkt of beschikbaar is conform haar verwachtingen of behoeften.</p>	<p>Wij adviseren om de (kritische) IT-beheersmaatregelen periodiek te monitoren/testen en daarmee vast te stellen of deze adequaat werken. Wij adviseren deze ook onderdeel te laten zijn van de Plan-Do-Check-Act cyclus.</p>	<p>Geen directe impact gegeven de gegevensgerichte controle-aanpak.</p>

Bijlage bij 2.3 - IT bevindingen

#	Bevinding / risico	Aanbeveling	Impact op controle
4	Dak beschikt niet over een calamiteitenplan of business recoveryplan dat periodiek wordt getest. Hierdoor loopt Dak de kans in geval van een calamiteit niet (tijdig) te kunnen herstellen.	Wij adviseren in samenwerking met de IT-partners een calamiteitenplan op te zetten. Met daarin o.a. aandacht voor communicatie, taken en verantwoordelijkheden en de technische maatregelen.	Geen directe impact gegeven de gegevensgerichte controle-aanpak.
5	Er wordt niet structureel periodiek een penetratietest of andere vulnerability scans uitgevoerd. Hierbij loopt Dak mogelijk veiligheidsrisico's.	Wij adviseren om samen met de IT-partners na te gaan welke periodieke scans op de omgeving van Dak of haar partners uitgevoerd zou kunnen worden.	Geen directe impact gegeven de gegevensgerichte controle-aanpak.
6	Operationele gebruikers (van vb. afdeling boekhouding, HR of klantadvies) hebben sterke rechten (o.a. super of administrator) in de applicaties AFAS, Jaamo en Factuur+. Hiermee loopt Dak het risico op functievermenging/-doorbreking.	Wij bevelen aan om de sterke rechten zoals de administrator rol alleen te beleggen bij de functioneel beheerder. Bij voorkeur is dat binnen de IT-functie. Hiermee kan je functiescheiding realiseren tussen initiëren en uitvoeren van wijzigen met betrekking tot rollen en rechten maar ook instellingen etc. Indien dit niet mogelijk is, adviseren wij de administrator rechten te beperken tot een of twee operationele gebruikers, maar kritische transacties of wijzigingen te monitoren.	Geen directe impact gegeven de gegevensgerichte controle-aanpak. Betreft wel een belemmering voor een systeemgerichte aanpak van de inkopen en betalingen.
7	'Password never expires' actief voor verschillende accounts. Dit zijn met name locaties, serviceaccounts etc. En verouderde besturingssoftware actief op systemen. Hiermee loopt Dak risico's m.b.t. (logische) toegangsbeveiliging.	Wij adviseren het AD periodiek te controleren en op te schonen. Daarbij adviseren wij om 'password never expires' niet toe te passen op kritische accounts en verouderde systemen te updaten of uit het netwerk te halen.	Geen directe impact gegeven de gegevensgerichte controle-aanpak. Betreft wel een belemmering voor een systeemgerichte aanpak van de inkopen en betalingen.

Bijlage bij 2.3 - IT bevindingen

#	Bevinding / risico	Aanbeveling	Impact op controle
8	<p>MFA is ingeregeld voor gebruikers van de Citrix omgeving en gebruikers met een Dak Kindercentra laptop. Voor pedagogisch medewerkers met alleen webmail is dit nog niet ingeregeld.</p> <p>Hiermee loopt Dak risico's m.b.t. (logische) toegangsbeveiliging.</p>	<p>Wij adviseren altijd sterke wachtwoorden i.c.m. MFA in te regelen om toegang tot de omgeving en systemen van Dak te krijgen.</p>	<p>Geen directe impact gegeven de gegevensgerichte controle-aanpak. Betreft wel een belemmering voor een systeemgerichte aanpak van de inkopen en betalingen.</p>
9	<p>Geen formele change management procedure waarmee (kritische) software en configuratiewijzigingen op een eenduidige, aantoonbare en structurele wijze worden uitgevoerd.</p> <p>Hiermee loopt Dak het risico dat niet goed werkende en/of niet goedgekeurde wijzigingen worden doorgevoerd.</p>	<p>Wij adviseren om een generieke change management procedure uit te werken die van toepassing is op alle applicaties voor zowel updates, eventuele maatwerkverzoeken als configuratiewijzigingen. Hierin dient rekening te worden gehouden dat wijzigingen worden aangevraagd, getest en goedgekeurd. Wij adviseren hierbij onderscheid te maken tussen complexe en niet complexe wijzigingen.</p>	<p>Geen directe impact gegeven de gegevensgerichte controle-aanpak.</p>
10	<p>Boeking die vanuit Jaamo worden ingelezen in AFAS kunnen in AFAS nog onderhouden of verwijderd worden.</p> <p>Hiermee loopt Dak het risico dat de aansluiting tussen Jaamo en AFAS niet gewaarborgd kan worden.</p>	<p>Wij adviseren na te gaan of automatische boekingen gegenereerd in Jaamo als niet te wijzigen boeking in AFAS kunnen worden ingelezen m.b.t. in ieder geval debiteur, bedrag, grootboekrekening.</p>	<p>Geen directe impact gegeven de gegevensgerichte controle-aanpak.</p>

ICT-strategie en organisatie DAK



Inleiding

In een snel veranderend digitaal landschap is het van cruciaal belang dat organisaties hun ICT-infrastructuur en beleid up-to-date houden. Bij DAK is echter gebleken dat de organisatie op dit gebied achterloopt. De ICT-zaken worden grotendeels intern georganiseerd, met een beperkt beroep op externe leveranciers voor essentiële infrastructuurdiensten. Deze aanpak heeft geleid tot een infrastructuur die niet volledig voldoet aan de dynamische vereisten van hedendaagse technologie en de groeiende behoeften van zowel personeel als klanten.

De interne organisatie van ICT-zaken is nog steeds sterk afhankelijk van traditionele methoden en is tot nu toe traag geweest met het adopteren van modernere systemen zoals Software as a Service (SaaS) werkplekken. Hoewel de eerste stappen richting een overgang naar deze moderne werkplekken zijn gezet, bevinden de implementatie en integratie ervan zich nog in een beginstadium. De aanpassing aan nieuwe technologieën is niet alleen een technische uitdaging, maar vereist ook een cultuuromslag binnen de organisatie.

Het beleid op het gebied van ICT binnen de organisatie is zwak gestructureerd, met aanzienlijke lacunes in zowel de uitvoering als de documentatie. Dit gebrek aan structuur en documentatie vergroot de kans op inconsistenties, inefficiënties en beveiligingsrisico's. Om deze problematiek het hoofd te bieden, is het van belang om beleid en procedures te standaardiseren en een duidelijke documentatiestructuur te creëren, wat een gestroomlijnde overgang naar SaaS-oplossingen zal ondersteunen en de algehele operationele effectiviteit zal verbeteren.

De kernwoorden die echt aandacht nodig hebben binnen de ICT organisatie zijn met name: **datazekerheid** en **security**.

Constateringen DAK



Kernvragen

Onderstaande tabel presenteert kernvragen met bijbehorende uitgewerkte antwoorden en evaluaties om een grondig begrip te verkrijgen van onze bevindingen en conclusies.

Kernvraag	Antwoord en beoordeling
ICT-strategie en organisatie	
Op welke manier worden risico's geïdentificeerd, beoordeeld en gemitigeerd binnen de ICT-strategie?	De ICT-strategie van de organisatie vertoont een gebrek aan een samenhangend systeem voor het identificeren, beoordelen en verminderen van risico's. Het vertrouwen berust voornamelijk op de beloften in de SLA-overeenkomsten met leveranciers voor risicobeheer, zonder adequate ondersteuning van interne documentatie. Dit creëert een aanzienlijke kloof in het risicobeheerproces, waarbij systematische identificatie en documentatie van risico's ontbreken.
Zijn er specifieke doelstellingen geformuleerd voor de ICT-afdeling om bij te dragen aan het succes van de organisatie?	Er ontbreekt duidelijke documentatie met specifieke ICT-doelen die aantoonbaar bijdragen aan het succes van de organisatie. Hoewel de lopende veranderingen wijzen op een positieve verschuiving van een afhankelijkheid van leveranciers naar een meer moderne omgeving, is het essentieel dat de ICT-afdeling haar doelstellingen concreet definieert en documenteert. Dit is cruciaal voor een sterke strategische visie en versterkt de rol en het belang van ICT bij het realiseren van de organisatiedoelen.
Is er een duidelijk plan voor bedrijfscontinuïteit en disaster recovery?	Binnen de organisatie is geen specifiek bedrijfscontinuïteitsplan of herstelplan voor rampen geïdentificeerd. De afhankelijkheid lijkt voornamelijk te liggen bij de dienstverleningsovereenkomsten (Service Level Agreements, SLA's) met SaaS-providers. Daarnaast lijkt de interne ICT-organisatie nog niet zo ver ontwikkeld te zijn, waarbij de aanpak van dit soort situaties op ad-hocbasis wordt beoordeeld.
Hoe wordt er binnen de ICT-strategie omgegaan met innovatie en het toekomstbestendig maken van de technologische infrastructuur?	De aanpak van innovatie en het toekomstbestendig maken van de technologische infrastructuur binnen de ICT-strategie van de organisatie wordt bepaald door interne besluitvorming die gericht is op marktontwikkelingen. Het managementteam (MT) speelt hierbij een cruciale rol door strategische keuzes te maken die de richting bepalen voor de implementatie van nieuwe technologieën en systemen, waarmee de organisatie voorbereid dient te worden op toekomstige uitdagingen.
Is er een proces voor het evalueren en implementeren van nieuwe technologieën?	Aansluitend op de vorige vraag lijkt hier geen documentatie specifiek voor bedoeld. Uit het interview bleek ook dat hier geen gestructureerd proces voor aanwezig is.
Hoe flexibel is de huidige ICT-infrastructuur en in hoeverre kan deze meegroeien met veranderende behoeften van de organisatie?	Op dit moment draait DAK op een on-premise Citrix-omgeving die wordt beheerd door zowel interne medewerkers als de externe leverancier Eshgro. Hoewel er een transitie gaande is naar SaaS-oplossingen, is de huidige infrastructuur hier nog niet klaar voor. Het fundament voor deze vernieuwingen lijkt nog niet goed doordacht te zijn, waardoor de organisatie momenteel niet gereed is voor verdere innovaties.
Voldoet de huidige ICT-infrastructuur aan de relevante beveiligingsnormen en wet- en regelgeving?	Op basis van de huidige informatie en het gebrek aan aangeleverde documentatie blijkt dat de ICT-infrastructuur geen aantoonbare naleving heeft van relevante beveiligingsnormen en wet- en regelgeving. Het lijkt erop dat de veiligheidsmaatregelen voornamelijk worden bepaald door beste inzichten en leveranciersnotificaties, wat geen structurele compliance garandeert.

Constateringen DAK

Kernvraag	Antwoord en beoordeling
Stakeholders, gebruikers	
Hoe ervaren de medewerkers de huidige ICT-voorzieningen en in hoeverre dragen deze bij aan een efficiënte werkomgeving?	Er ontbreekt volledige documentatie om hier uitspraken over te doen. Tijdens het interview is aangegeven dat er geen documentatie of registratie beschikbaar is met betrekking tot dit onderwerp.
Zijn er evaluatiemethodes gebruikt om de ervaring van gebruikers te meten?	Hoewel dit momenteel niet van toepassing is, heeft een gebruiker altijd de mogelijkheid om op individueel niveau een probleem te melden bij een functioneel beheerder, met name als er problemen zijn bij het gebruik van een applicatie.
In hoeverre worden ICT-trainingen gefaciliteerd aan medewerkers? Zijn hiervoor budgetten?	Dit is niet van toepassing.
Wie zijn de externe stakeholders binnen de volledige IT omgeving en hoe is veiligheid en stabiliteit geborgd?	Er wordt gebruik gemaakt van een oudere Jaamo omgeving die als extern systeem geldt.
Hoe is de toegang tot systemen en data geregeld en wie heeft waar toegang toe?	Verschillende functiegroepen hebben verschillende rollen. De autorisatiematrix is op Citrix, fileserver en Exchange niveau goed aangesloten op de functieprofielen & rollen. Echter binnen Jaamo sluit de autorisatiematrix niet aan, dit heeft te maken met een beperking in Jaamo zelf. Er is dan ook geen SSO geregeld.
Software en licentiebeheer	
Zijn er integraties tussen verschillende softwareapplicaties en hoe zijn deze geconfigureerd en daarnaast geborgd op kwaliteit?	Er zijn verschillende integraties operationeel binnen de software-infrastructuur, maar binnen DAK ontbreken beschrijvingen of bewijsvoeringen hiervan. Het vertrouwen ligt bij externe partijen die verantwoordelijk zijn voor de ontwikkeling en het beheer ervan.
Hoe wordt omgegaan met softwarelicenties en hoe wordt dit beheerd? En hoe wordt omgegaan met de verlenging van de licenties?	Handmatige controle van de beheerders en men wordt op de hoogte gehouden vanuit de externe leveranciers.

Constateringen DAK

Kernvraag	Antwoord en beoordeling
Infrastructuur	
Hoe is het beheer van de infrastructuur geregeld en is er sprake van proactief onderhoud?	Het beheer van de infrastructuur is uitbesteed aan de partij Informatel. Hier ligt ook een SLA aan ten grondslag.
Worden er regelmatige audits of controles uitgevoerd op de systemen en infrastructuur?	Dit is niet van toepassing.
Zijn er maatregelen getroffen voor disaster recovery en bedrijfscontinuïteit?	Dit is niet van toepassing.
Hoe is de monitoring en alarmering geregeld voor de kritieke systemen en is deze beschikbaar voor iemand binnen de interne organisatie?	Er wordt minimaal gemonitord. Het enige wat er aan monitoring gebruikt wordt is PRTG voor de meest kritische onderdelen binnen de server infrastructuur.
Is er documentatie beschikbaar over de infrastructuur, randapparatuur en mobiele devices en wordt deze up-to-date gehouden?	Topdesk fungeert als facilitair systeem voor het beheer van apparatuur, maar er is geen specifiek onderhoudsplan beschikbaar. De belangrijkste infrastructuurapparatuur wordt up-to-date gehouden door interne ICT-beheerders en deels door externe leveranciers Informatel en Eshgro.
Zijn er redundante systemen of onderdelen om de continuïteit te waarborgen bij uitval?	De kernsystemen zijn redundant om de continuïteit te waarborgen, zoals blijkt uit het interview waarin werd vermeld dat er gebruik wordt gemaakt van een on-premise serveromgeving met ESX.

Constateringen DAK

Kernvraag	Antwoord en beoordeling
Security	
Hoe is de security awareness momenteel geregeld?	Er is niets geregeld.
Hoe is het geregeld met het algemene informatiebeveiligingsbeleid binnen de organisatie?	Er is niets geregeld.
Zijn er historische data beschikbaar over incidenten of storingen, en hoe zijn deze opgelost?	Er zijn meerdere beveiligingsincidenten geweest en deze zijn individueel behandeld.
Hoe is een incident respons plan geregeld en geborgd? Hoe loopt de lijn op dit moment voor de verwerking.	Het incidentresponsplan binnen de organisatie is momenteel niet adequaat geregeld en geborgd. Er is weinig tot geen structuur zichtbaar voor de aanpak van incidenten, en de procedures hiervoor lijken niet formeel vastgelegd te zijn. Tot op heden is er ook geen documentatie over dergelijke processen verstrekt, wat duidt op een ontbrekend of onvolledig incidentresponsprotocol.
Is er een cybercrisis management plan beschikbaar en hoe zit deze in elkaar en wie is daarbij betrokken?	Er ontbreekt momenteel een duidelijk omschreven plan voor het beheer van cybercrises binnen de organisatie. De details, structuur en betrokkenheid bij een dergelijk plan zijn niet bekendgemaakt, en er zijn geen documenten of procedures verstrekt. Dit suggereert dat er geen gestructureerd plan is om effectief om te gaan met cyberincidenten.
Leveranciers	
Hoe worden de prestaties en service levels van de leveranciers gemonitord en beoordeeld?	Op dit moment vindt er geen systematische monitoring en beoordeling plaats van de prestaties en service levels. Hoewel er communicatie is tussen DAK en de leverancier, met name mondeling, ontbreken concrete beoordelingen of gedocumenteerde evaluaties.
Hoe wordt omgegaan met eventuele geschillen of issues met leveranciers, en is hier een procedure voor vastgelegd?	Er lijkt geen officiële procedure te zijn voor het afhandelen van geschillen of problemen met leveranciers. Er is geen documentatie ontvangen die een dergelijk proces beschrijft, en er zijn geen bewijzen van bestaande protocollen voor dergelijke situaties. Bovendien werd tijdens het interview aangegeven dat er zelden tot nooit problemen zijn met leveranciers, wat suggereert dat er mogelijk weinig noodzaak is gevoeld om een formele procedure te ontwikkelen.

ICT leveranciers DAK



Overzicht van belangrijke ICT leveranciers

In de volgende tabel zien we de belangrijke ICT leveranciers, die echt invloed hebben op het dagdagelijkse handelen en proces.

Leverancier	Toelichting	SLA	Performance rapportage	Beoordeling
Informatel	Leverancier van netwerk equipment / beveiliging. Werkzaamheden worden samen met interne medewerkers met deze leverancier uitgevoerd. Leverancier stuurt notificatie als er updates zijn.	Aanwezig, bij ons niet bekend	Niet aanwezig.	Primaire leverancier Beoordeling niet mogelijk door ontbreken documentatie.
Eshgro / Avensus	Primaire leverancier t.b.v. on-premises ICT omgeving, o.a. Citrix / MS Exchange. Werkzaamheden worden samen met interne medewerkers met deze leverancier uitgevoerd. Leverancier stuurt notificatie als er updates zijn, hiervoor is ook een SLA bekend.	Aanwezig, bij ons niet bekend	Niet aanwezig.	Primaire leverancier Beoordeling niet mogelijk door ontbreken documentatie, echter er is wel een SLA aangeleverd voor ICT monitoring en notificaties – deze is niet getekend en onvolledig ingevuld – is deze dan echt wel actief?
Jaamo	Belangrijke leverancier van het integrale softwaresysteem Jaamo.	Aanwezig, bij ons niet bekend	Niet aanwezig.	Primaire leverancier Beoordeling niet mogelijk door ontbreken documentatie.
AFAS / Peopletrack	Leverancier van Profit voor HR en financiële software. Deze draait als een SaaS oplossing (RDP over internet) / Peopletrack is de consultant.	Software overeenkomst, bij ons niet bekend.	Niet aanwezig	Primaire leverancier Beoordeling niet mogelijk door ontbreken documentatie.
Onguard	Debiteurenbeheer software (on-premises)	Onbekend	Niet aanwezig	Beoordeling niet mogelijk door ontbreken documentatie.
Topdesk	Topdesk als SaaS voor facilitair beheer	Onbekend	Niet aanwezig	Deze facilitaire tool als SaaS oplossing is niet-kritiek en een strenge beoordeling is daarom niet noodzakelijk.

Systemen en infrastructuur DAK

Inleiding

Binnen DAK is het grootste deel van de infrastructuur in beheer vanuit eigen organisatie, met ondersteuning vanuit Eshgro en Informatel.

Clienthardware (werkplekken) Mobiele devices Overige randapparatuur	Server hardware	Netwerkapparatuur
De client hardware bestaat voornamelijk uit HP mini PC's en Microsoft Surface laptops.	Server hardware onpremises, met Vmware ESX als virtualisatieplatform. Citrix, Office software en Microsoft Exchange zijn nog actief	Firewalls aanwezig in hoofdlocatie alsook in de branche vestigingen (sublocaties)
In house ondersteuning en onderhoud met hulp van Eshgro	In house ondersteuning en onderhoud met hulp van Eshgro	In house ondersteuning en onderhoud met hulp van Informatel
<div>Niet vastgesteld</div> <div>Geen controles uitgevoerd</div> <div>Beoordeling is niet in te schatten</div>	<div>Niet vastgesteld</div> <div>Geen controles uitgevoerd</div> <div>Beoordeling is niet in te schatten</div>	<div>Niet vastgesteld</div> <div>Geen controles uitgevoerd</div> <div>Beoordeling is niet in te schatten</div>

Identificatie en strategie beperking potentiële Risico's DAK




In deze paragraaf hebben we de ICT-gerelateerde risico's zorgvuldig in kaart gebracht en strategieën ontwikkeld om deze te beperken. Door een systematische benadering te hanteren, zorgen we ervoor dat alle potentiële gevaren worden geïdentificeerd, beoordeeld en dat er passende maatregelen worden voorgesteld om de impact op de organisatie te minimaliseren.

Risico	Toelichting	Strategie voor risicobeperking
Gebrek aan systematische risico-beheerprocessen Hoog risico ●	De huidige ICT-strategie van de organisatie vertoont aanzienlijke tekortkomingen in het systematisch identificeren, beoordelen en verminderen van risico's. Er ontbreekt interne documentatie en de expertise om beheersprocessen op te zetten, waardoor de organisatie kwetsbaar is voor onvoorzienbare bedreigingen.	<ul style="list-style-type: none">• Implementeer een intern risicobeheersysteem dat SLA's aanvult met eigen risicoanalyses.• Ontwikkel een gedocumenteerd proces voor risico-evaluatie en mitigatie.• Versterk risicobewustzijn en -management door personeel te trainen, waardoor eigenaarschap en kennis worden vergroot.
Onvoldoende disaster recovery planning intern Hoog risico ●	Het bedrijf beschikt niet over een formeel bedrijfscontinuïteitsplan (BCP) of disaster recovery plan (DRP), wat potentieel aanzienlijke verstoringen kan veroorzaken bij onvoorziene gebeurtenissen. De huidige afhankelijkheid van eigen on-premises hardware biedt geen afdoende garantie voor snelle hersteltijden en kan de bedrijfsvoering negatief beïnvloeden bij ernstige incidenten.	Ontwikkel en implementeer een gedetailleerd Bedrijfscontinuïteitsplan (BCP) en Disaster Recovery Plan (DRP), inclusief organisatie-specifieke herstelstrategieën en regelmatige prestatie-evaluaties. Zorg ervoor dat deze plannen periodiek worden getest en bijgewerkt om de veerkracht te waarborgen.
Gebruikersautorisatie niet op orde Hoog risico ●	De autorisatie op de clientsystemen, vooral op externe locaties, is niet op orde. Gebruikers loggen in met een gedeeld locatieaccount in plaats van een gepersonaliseerd account. De logininformatie komt overeen met de logins voor de Microsoft Exchange-accounts van de locatie, wat toegang biedt tot e-mail en agenda's. Dit creëert aanzienlijke risico's voor ongeautoriseerde toegang.	<ul style="list-style-type: none">• Implementeer persoonlijke gebruikersaccounts in combinatie met Multi-Factor Authenticatie (MFA).• Stel autorisatiebeheer in, inclusief Single Sign-On (SSO).
Back-up systeem is niet immuun Hoog risico ●	Ondanks de aanwezigheid van een NAS-back-up en een online back-up naar de Microsoft cloud bij DAK, biedt dit geen voldoende garantie tegen dataverlies. Risico's zoals lokale calamiteiten, cyberaanvallen of technische storingen kunnen nog steeds de integriteit en beschikbaarheid van gegevens in gevaar brengen. Het is belangrijk om aanvullende maatregelen te overwegen om een robuustere bescherming tegen deze risico's te waarborgen.	<p>Aanbevelingen voor de back-upstrategie:</p> <ul style="list-style-type: none">• Wisselende opslagmedia: Implementeer een roterend systeem van externe harde schijven die regelmatig worden gewisseld. Zorg ervoor dat deze schijven buiten het primaire bedrijfsnetwerk worden opgeslagen om extra redundantie te bieden in geval van calamiteiten.• Clouddienst voor immutable backup: Overweeg het gebruik van clouddiensten die immutable backups aanbieden. Deze diensten zorgen ervoor dat de back-ups niet kunnen worden gewijzigd, waardoor bijvoorbeeld een ransomware-aanval geen dataverlies met zich meebrengt. Dit voegt een extra laag van bescherming toe tegen cyberdreigingen.

Identificatie en strategie beperking potentiële Risico's DAK



Risico	Toelichting	Strategie voor risicobeperking
Stabiliteit en robuustheid Medium risico 	Op dit moment wordt er voornamelijk gebruikgemaakt van een on-premises serveromgeving met Citrix-implementatie. Hoewel dit op zichzelf niet noodzakelijkerwijs een stabiliteitsprobleem met zich meebrengt, is er wel een duidelijke indicatie dat er aandacht is besteed aan aspecten zoals disaster recovery, het rapporteren van prestatieproblemen, en soortgelijke zaken. Om een robuuste werkwijze te garanderen, is het cruciaal om te beschikken over gedocumenteerde procedures. Hierdoor kan op overtuigende wijze worden aangetoond dat het systeem stabiel is, met minimale risico's op storingen, zowel op server- als netwerkniveau. Deze documentatie is van essentieel belang, vooral met het oog op potentiële netwerkstoringen en de ernstiger dreiging van cyberinbraken.	<ul style="list-style-type: none">• Opstelling van een uitgebreid disaster recovery plan: Ontwikkel een gedetailleerd plan voor noodherstel, inclusief regelmatige testscenario's om de effectiviteit van de herstelprocedures te waarborgen. Zorg voor helder gedocumenteerde stappen voor failover en herstel, zowel op het niveau van servers als netwerkinfrastructuur. Deze procedures zijn van cruciaal belang omdat ze in noodsituaties moeten worden toegepast, en het is geruststellend als alle stappen stap voor stap bekend zijn.• Versterking van cybersecurity: Implementeer een meerlagige aanpak voor beveiliging, inclusief regelmatige penetratietests, continu netwerkmonitoring, en aanscherping van toegangscontroles om de weerbaarheid tegen cyberdreigingen te vergroten.
Gebrek aan (log)monitoring identificeren van incidenten. Medium risico 	Naast het gebruik van PRTG wordt er nauwelijks gebruikgemaakt van monitoring. Incidentele reactieve respons op incidenten kan een risico vormen en is niet voldoende om proactief potentiële problemen te identificeren en aan te pakken.	<ul style="list-style-type: none">• Overweeg de implementatie van uitgebreidere monitoringtools, zoals een Security Information and Event Management (SIEM) systeem, om een breder scala aan activiteiten te bewaken.• Transformeer bestaande processen zoveel mogelijk van reactieve naar proactieve benaderingen om potentiële problemen te anticiperen en aan te pakken voordat ze kritiek worden.
Personeelsonboarding ICT omgeving niet geautomatiseerd. Laag risico 	De procedure voor het onboarden van personeel is niet geautomatiseerd, wat het risico met zich meebrengt dat er tijdens de onboarding ergens een verkeerde autorisatie wordt ingesteld of een onjuiste configuratie wordt uitgevoerd. Dit kan schade veroorzaken, met name op het gebied van beveiliging, waar privacygevoelige gegevens mogelijk worden blootgesteld.	<ul style="list-style-type: none">• Standaardisatie van onboardingprocedures: Maak gedetailleerde checklists en protocollen voor elke stap van de onboardingprocedure om de consistentie te waarborgen en fouten te minimaliseren. Regel bijvoorbeeld autorisatie (gedeeltelijk) via de Active Directory (AD).• Periodieke toegangsreviews: Implementeer regelmatige audits op gebruikersrechten en configuraties om onregelmatigheden en ongeautoriseerde toegang te identificeren, corrigeren en rapporteren.
Personeelstrainingen blijven uit Laag risico 	Het ontbreken van personeelstrainingen verhoogt het risico op onvoldoende vaardigheden en kennis, wat kan leiden tot verminderde prestaties en verhoogde foutmarges. Bovendien kan het resulteren in een minder tevreden werkhouding en een verminderd interessegebied in het correct indienen van belangrijke informatie.	<ul style="list-style-type: none">• Implementeer een verplicht trainingsprogramma met regelmatige intervallen om kennis en vaardigheden actueel te houden. Dit hoeft geen high-level training te zijn; eventuele E-learning-filmpjes of online bewustwordingstrainingen kunnen voldoende zijn.• Koppel prestatiebeoordelingen aan trainingsdeelname om het belang van continue professionele ontwikkeling te benadrukken. Dit geeft ook extra motivatie om het goed te (blijven) doen.

Algemene Bevindingen DAK



- Er wordt **verondersteld** dat er binnen de organisatie overeenkomsten/contracten bekend zijn bij verschillende ICT-leveranciers (in de vorm van een SLA); echter deze lijken niet compleet.

Het onderzoek naar de huidige ICT-status geeft aan dat er ruimte is voor significante verbeteringen. Hoewel er toekomstige plannen zijn, moeten we ons focussen op de huidige situatie, die enkele kritische gebieden belicht die onmiddellijke aandacht behoeven. Het gebrek aan gedocumenteerde informatie op ICT vlak beperkt ons vermogen om de betrouwbaarheid van de verstrekte informatie volledig te beoordelen en te valideren.

Om een robuuste basis voor toekomstige ontwikkelingen te leggen, raden we dringend aan om documentatie te formaliseren en te structureren.

- De organisatie beschikt over **onvoldoende** kennis op het gebied van **privacy, wetgeving, en beveiliging**, wat resulteert in een niet georganiseerd systeem.
- In het verleden hebben zich beveiligingsincidenten voorgedaan, maar er lijkt nog geen aanzienlijke waarde gehecht te worden aan een **gestructureerd registratiesysteem voor dergelijke incidenten**.
- De organisatie vertrouwt sterk op externe leveranciers, ook voor notificaties met betrekking tot updates en mogelijke kwetsbaarheden. Er wordt echter niet voldoende nadruk gelegd op **kwaliteits- en prestatiebeoordelingen** van deze leveranciers, en er bestaat onzekerheid over de betrouwbaarheid van externe bronnen, aangezien ook leveranciers fouten kunnen maken.

ICT-strategie en organisatie DAK



Conclusie en samenvatting

Vanwege het ontbreken van aangeleverde documentatie met betrekking tot de ICT van DAK is het lastig om een beoordeling van de huidige stand van zaken op te stellen. Alle punten die eerder genoemd zijn en hieronder nog behandeld worden zijn opgesteld op basis van het interview dat is gehouden met de verantwoordelijke medewerkers.

De huidige ICT-strategie en organisatie vertonen aanzienlijke tekortkomingen, vooral met betrekking tot risicobeheer, doelstellingen, bedrijfscontinuïteit, en innovatie. Er ontbreekt een samenhangend systeem voor het identificeren, beoordelen en verminderen van risico's, waarbij het vertrouwen voornamelijk op externe SLA's berust. Duidelijke doelstellingen voor de ICT-afdeling ontbreken, en er is geen specifiek plan voor bedrijfscontinuïteit en disaster recovery. De aanpak van innovatie is afhankelijk van interne besluitvorming gericht op marktontwikkelingen, waarbij een structurele aanpak ontbreekt.

De ICT-infrastructuur staat momenteel niet klaar voor verdere innovaties. Autorisatie op clientsystemen en back-upsystemen vormen aanzienlijke veiligheidsrisico's, en monitoring, zowel proactief als reactief, is ontoereikend. Het ontbreken van geautomatiseerde onboardingprocedures en personeelstrainingen vergroot het risico op beveiligingsinbreuken en prestatieproblemen.

Het risico op gebrek aan systematische risicobeheerprocessen, onvoldoende disaster recovery planning, ongeautoriseerde toegang, en het ontbreken van (log)monitoring kan worden beperkt door het implementeren van interne risicobeheersystemen, gedetailleerde BCP/DRP-plannen, geavanceerde autorisatie- en back-upstrategieën, en uitgebreide monitoringtools. Verbeteringen in personeelstraining en onboardingprocedures zijn essentieel om het personeel bekwaam en bewust te houden. Het benadrukken van continue professionele ontwikkeling kan de algemene prestaties en betrokkenheid verbeteren.