International Standard on Assurance Engagements Report (ISAE) 3402

Type II

Voor het onderhoud en beheer van de Easyflex Software

Periode:	1 januari 2024 tot en met 31 december 2024
Ref:	R2503-02
Rapport datum:	6 maart 2025

Inhoudsopgave

I. Geheimhoudingsverklaring

Dit International Standard on Assurance Engagement (ISAE) 3402 type II rapport van Easyflex bevat vertrouwelijke informatie.

Dit rapport blijft eigendom van Easyflex en zal alleen door haar klanten aan wie deze rapportage rechtstreeks door Easyflex beschikbaar is gesteld en haar externe auditors worden gebruikt voor het beoordelen van de opzet, het bestaan en de werking van de interne beheersing van Easyflex.

Het is de gebruikersorganisatie en haar externe auditor verboden om vertrouwelijke informatie uit dit rapport te kopiëren, te reproduceren, te verkopen, over te dragen of op andere wijze van de hand te doen, dan wel op andere wijze aan een persoon, instelling of onderneming ter beschikking te stellen.

Gaat u niet akkoord met deze geheimhoudingsverklaring, dan verzoeken wij u het rapport terug te zenden aan Easyflex en geen kopie te bewaren.

Easyflex
Europark 3
4904 SX Oosterhout

II. Voorwoord

Hierbij bieden wij u het ISAE type II rapport aan dat is opgesteld voor de klanten die gebruik maken van de Easyflex software.

Als directie van Easyflex zijn wij ervoor verantwoordelijk dat de dienstverlening aan onze klanten van goede kwaliteit is.

Dit ISAE3402 type II rapport is als volgt opgebouwd:

1: **Managementverklaring** van het management van Easyflex, waarin zij vanuit de eigen verantwoordelijkheid aangeeft dat de beheersingsomgeving in het algemeen en de in het rapport genoemde specifieke beheersingsmaatregelen in het bijzonder, adequaat zijn opgezet en hebben gewerkt gedurende de verslagperiode.

2: **Assurance-rapport van de onafhankelijke IT-auditor**, waarin DNV haar oordeel geeft over het onderzoek dat zij heeft uitgevoerd naar de beschrijving van Easyflex, het behalen van de beheersingsdoelstellingen en de opzet en werking van de interne beheersingsmaatregelen.

3: **Beschrijving van de organisatie en interne beheersing**. In dit hoofdstuk zijn tevens het beheersingssysteem van Easyflex, de -doelstellingen en -maatregelen en de door de gebruikersorganisatie in overweging te nemen beheersingsmaatregelen opgenomen.

4: **Beschrijving van de beheersingsmaatregelen, testwerkzaamheden en -resultaten** van de onafhankelijke auditor. In dit hoofdstuk is het beheersingskader beschreven met daarbij de toelichting van DNV op de uitgevoerde testwerkzaamheden en haar conclusies.

1. Managementverklaring

Voor u ligt het ISAE 3402 type II rapport van Easyflex over de periode van 1 januari 2024 tot en met 31 december 2024.

De bijgaande beschrijving van het systeem van interne beheersing is opgesteld voor opdrachtgevers die gebruik hebben gemaakt van de Easyflex software (hierna de dienstverlening), hun auditors en de externe accountants. Het uitgangspunt hierbij is dat zij voldoende inzicht hebben om de beschrijving, samen met overige informatie waaronder informatie over interne beheersingsmaatregelen die door de opdrachtgevers zelf worden uitgevoerd, te beschouwen wanneer zij de risico's van afwijkingen van materieel belang van de financiële overzichten en operationele processen van de opdrachtgevers inschatten.

De directie van Easyflex bevestigt naar beste weten dat:

a. De beschrijving in hoofdstukken 3 en 4 van de processen, de bijbehorende beheersingsdoelstellingen en beheersingsmaatregelen betreffende de dienstverlening voor de opdrachtgevers van Easyflex, over de periode van 1 januari 2024 tot en met 31 december 2024 getrouw zijn weergegeven.

   De criteria waarvan gebruik wordt gemaakt bij het doen van deze bewering hielden in dat de bijgaande beschrijving:

   1. Weergeeft op welke wijze het systeem van interne beheersing is opgezet en geïmplementeerd, met inbegrip van:
      a. De soorten diensten die verleend zijn, met inbegrip van, in voorkomende gevallen de verwerkte transactiestromen;
      b. De procedures, binnen zowel informatietechnologie als handmatige systemen, waardoor de transacties werden geïnitieerd, vastgelegd, verwerkt, gecorrigeerd voor zover noodzakelijk en overgebracht naar de rapportages die voor opdrachtgevers zijn opgesteld;
      c. De verbonden administratie, de ondersteunende informatie en specifieke informatie waarvan gebruik is gemaakt om transacties te initiëren, te verwerken en vast te leggen; dit houdt onder meer het corrigeren van incorrecte informatie in en de wijze waarop informatie is overgedragen naar rapportages die voor opdrachtgevers zijn opgesteld;
      d. De wijze waarop de dienstverlening van Easyflex de significante gebeurtenissen en omstandigheden, buiten de transacties, heeft behandeld;
      e. Het proces waarvan gebruik werd gemaakt bij het opstellen van rapportages voor opdrachtgevers;
      f. Relevante interne beheersingsdoelstellingen en interne beheersingsmaatregelen die zijn opgezet om die doelstellingen te bereiken;
      g. Interne beheersingsmaatregelen waarvan wij, bij de opzet van het systeem, aannamen dat zij door gebruikende entiteiten zouden worden geïmplementeerd

en die, indien noodzakelijk om de interne beheersingsdoelstellingen die in de bijgaande beschrijving staan vermeld te bereiken, samen met de specifieke interne beheersingsdoelstellingen die niet alleen door onszelf kunnen worden bereikt, zijn onderkend;

h. Overige aspecten van onze beheersingsomgeving, het risico-inschattingsproces, het informatiesysteem (met inbegrip van het verbonden bedrijfsproces) en communicatie, beheersactiviteiten en interne beheersingsmaatregelen in het kader van het monitoren die relevant zijn voor het verwerken en het rapporteren van de transacties van de opdrachtgevers.

2. Relevante details bevat van wijzigingen in het systeem van de serviceorganisatie gedurende de verslagperiode van 1 januari 2024 tot en met 31 december 2024.

3. Geen informatie weglaat of verkeerd voorstelt die relevant is voor de reikwijdte van de dienstverlening van Easyflex die is beschreven terwijl erkend wordt dat de beschrijving is opgesteld om te voldoen aan de algemene behoeften van de gebruikers en daarom niet ieder aspect van de dienstverlening van Easyflex kan bevatten dat iedere individuele opdrachtgever in diens bijzondere omgeving belangrijk kan achten.

b. De interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de bijgaande beschrijving staan vermeld, met uitzondering van de aangelegenheden die staan beschreven in hoofdstuk 2, paragraaf "Basis voor een oordeel met beperking", op afdoende wijze zijn opgezet en hebben effectief gewerkt gedurende de periode van 1 januari 2024 tot en met 31 december 2024. De criteria waarvan bij het maken van deze bewering gebruik werd gemaakt hielden in dat:

1. De risico's die het bereiken van de interne beheersingsdoelstellingen die in de beschrijving staan vermeld in gevaar brengen, werden onderkend;

2. De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen;

3. De interne beheersingsmaatregelen consistent hebben gewerkt conform hun ontwerp en handmatige beheersingsmaatregelen zijn uitgevoerd door individuen met geschikte competenties en autoriteit gedurende de periode van 1 januari 2024 tot en met 31 december 2024.

Oosterhout, 6 maart 2025

M.Remie
COO

2. Assurancerapport van de onafhankelijke IT-auditor

Aan: De directie van Easyflex

Assurance-rapport van de onafhankelijke IT-auditor van de serviceorganisatie over de opzet en werking van de interne beheersingsmaatregelen.

2.1. Reikwijdte

Wij hebben opdracht gekregen om te rapporteren over de systeembeschrijving van Easyflex zoals opgenomen in de hoofdstukken 3 en 4 inzake de dienstverlening en over de opzet (de beschrijving) en werking van interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving staan vermeld over de periode van 1 januari 2024 tot en met 31 december 2024.

Easyflex maakt gebruik van serviceorganisaties Interconnect voor housing services en Proximus NXT voor de Managed. Easyflex maakt voor haar beschrijving gebruik van de uitsluitingsmethode (‘carve-out method’). De beschrijving van de serviceorganisatie van haar systeem sluit daarmee de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersingsmaatregelen van de sub-serviceorganisatie uit. Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersingsmaatregelen van de sub-serviceorganisatie.

2.2. Verantwoordelijkheden van Easyflex

Easyflex is verantwoordelijk voor: het opstellen van de beschrijving en bijgaande vermelding in hoofdstuk 1, met inbegrip van de volledigheid, nauwkeurigheid en methode van presentatie van de beschrijving en de bewering; het verlenen van diensten die door de beschrijving worden omvat; het vermelden van de interne beheersingsdoelstellingen; het opzetten, implementeren en effectief laten werken van interne beheersingsmaatregelen om de vermelde interne beheersingsdoelstellingen te bereiken.

2.3. Verantwoordelijkheden van de IT-auditor van de serviceorganisatie

Onze verantwoordelijkheid is, op basis van onze werkzaamheden, het geven van een oordeel over de beschrijving van Easyflex en over de opzet en werking van interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving staan vermeld. We hebben onze opdracht uitgevoerd overeenkomstig Nederlands recht, waaronder Richtlijn 3402 “Assurance-rapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie” vastgesteld door Nederlandse Orde van Register EDP-Auditors (NOREA). Dit vereist dat wij onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen over de vraag of de beschrijving getrouw is weergegeven en de interne beheersingsmaatregelen, in alle van materieel belang zijnde aspecten, op afdoende wijze zijn opgezet en effectief hebben gewerkt.

Een assurance-opdracht om te rapporteren over de beschrijving en opzet van interne beheersingsmaatregelen bij een serviceorganisatie omvat het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de toelichtingen in de beschrijving van de serviceorganisatie van haar systeem en de opzet van interne beheersingsmaatregelen. De geselecteerde werkzaamheden zijn afhankelijk van de door de (IT)-auditor van de serviceorganisatie toegepaste oordeelsvorming, met inbegrip van het inschatten van de

risico's dat de beschrijving niet getrouw is weergegeven en dat interne beheersingsmaatregelen niet op afdoende wijze zijn opgezet. Een assurance-opdracht van dit type omvat ook het evalueren van het algehele beeld van de beschrijving, de geschiktheid van de interne beheersingsdoelstellingen die daarin staan vermeld en de geschiktheid van de criteria die door de serviceorganisatie zijn gespecificeerd en die staan beschreven in dit rapport.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor ons oordeel te bieden.

2.4. Onafhankelijkheid en kwaliteitsbeheersing

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke zijn gebaseerd op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhouden wij een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en de procedures met betrekking tot de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving.

2.5. Beperkingen van interne beheersingsmaatregelen bij een serviceorganisatie

De beschrijving van Easyflex is opgezet om aan de algemene behoeftes van een brede groep van opdrachtgevers, hun accountants en auditors te voldoen en kan daarom niet ieder aspect van het systeem bevatten dat iedere individuele opdrachtgever in diens eigen bijzondere omgeving belangrijk kan achten. Bovendien kunnen interne beheersingsmaatregelen bij een serviceorganisatie, vanwege hun aard, niet alle fouten of omissies bij het verwerken of rapporteren van transacties voorkomen of ontdekken.

2.6 Basis voor een oordeel met beperking

De tabel hieronder geeft de beheersingsmaatregel weer die als niet effectief wordt beschouwd:

Ref	Beheersingsmaatregel	Bevinding
IC02	Incidenten worden: • vastgelegd in een ticketsysteem; • afgehandeld en teruggekoppeld aan de klant.	Niet voor alle incidenten is een terugkoppeling naar de klant aantoonbaar.

2.7 Oordeel met beperking

Ons oordeel is gevormd op basis van de aangelegenheden die in deze rapportage zijn uiteengezet. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die in dit rapport staan beschreven.

Naar ons oordeel, in alle van materieel belang zijnde aspecten, uitgezonderd de aangelegenheden die staan beschreven in de paragraaf 'Basis voor een oordeel met beperking':

a. Geeft de beschrijving de dienstverlening van Easyflex aan haar opdrachtgevers getrouw weer zoals deze gedurende de verslagperiode van 1 januari 2024 tot en met 31 december 2024 is opgezet en geïmplementeerd;

b. Zijn de interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving staan vermeld gedurende de verslagperiode van 1 januari 2024 tot en met 31 december 2024 op afdoende wijze opgezet; en

c. Werkten de getoetste interne beheersingsmaatregelen, die noodzakelijk waren om een redelijke mate van zekerheid te verschaffen dat de in de beschrijving vermelde interne beheersingsdoelstellingen waren bereikt, gedurende de verslagperiode van 1 januari 2024 tot en met 31 december 2024 effectief.

2.8 Beschrijving van getoetste interne beheersingsmaatregelen

De specifieke getoetste interne beheersingsmaatregelen, de aard, timing en resultaten van die toetsingen zijn opgenomen in hoofdstuk 4 van deze rapportage.

2.9 Beoogde gebruikers en doel

Deze ISAE rapportage is alleen voor opdrachtgevers die gebruik hebben gemaakt van de dienstverlening van Easyflex en hun accountants en auditors, die voldoende inzicht hebben om het in aanmerking te nemen bij het verwerven van inzicht in de informatiesystemen van opdrachtgevers die relevant zijn voor financiële verslaggeving tezamen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die door opdrachtgevers zelf worden uitgevoerd.

Barendrecht, 6 maart 2025

Jessica Goossens, RE MSc.
Business Unit Manager

DNV Business Assurance B.V.
Zwolseweg 1
2994 LB, Barendrecht

3. Organisatie en interne beheersing

Dit hoofdstuk beschrijft de organisatie, dienstverlening en reikwijdte van het ISAE 3402 type II rapport.

3.1. Over Easyflex

Easyflex ontwikkelt software(applicaties) voor de flexbranche zoals uitzendbureaus, arbeidsmigrantenbemiddelaars en payroll bedrijven. De software die Easyflex ontwikkelt, ondersteunt alle bedrijfsprocessen voor flexibele arbeid en personele dienstverlening. Deze ontwikkeling vindt in eigen beheer plaats. Enkele functionaliteiten van de huidige applicatie zijn bijvoorbeeld het plannen en verlonen van medewerkers, het koppelen van documenten en signalen ontvangen wanneer een dossier nog niet compleet is en tijdsregistratie. Inmiddels bestaat Easyflex meer dan 20 jaar. Momenteel heeft Easyflex meer dan 1 miljoen flexwerkers in de database staan, werken iedere dag zo'n 1.500 gebruikers met de applicatie en worden iedere week zo'n 40.000 salarissen verwerkt.

3.1.1. Scope dienstverlening

De scope van dit rapport is beperkt tot het onderhoud en beheer van Easyflex Software. De Easyflex software betreft software waarmee (onder andere) de verloning en facturatie uitgevoerd kunnen worden onderdeel van deze software is de mogelijkheid om een digitale handtekening te zetten en om documenten te beheren met document management. Flexwrapp is een mobiele applicatie bedoeld voor flexwerkers om (onder andere) hun uren in te vullen.

Gebruikersorganisaties en hun onafhankelijke auditors zijn verantwoordelijk om te bepalen of de diensten die hun door het bedrijf worden aangeboden binnen de reikwijdte van dit rapport vallen.

Easyflex opereert vanuit de overtuiging dat haar doelgroep uitzendbureaus behoefte heeft aan software waarmee ze hun dagelijkse administratieve werkprocessen zoveel mogelijk kunnen automatiseren. Daarmee beoogt Easyflex dat de klant zich kan richten op werven en selecteren van flexibel personeel.

3.1.2. Visie

Visie

Easyflex heeft de volgende visie geformuleerd:

"Wij willen het beste salaris platform van Nederland zijn en evolueren naar een all-in-one oplossing voor de flexbranche."

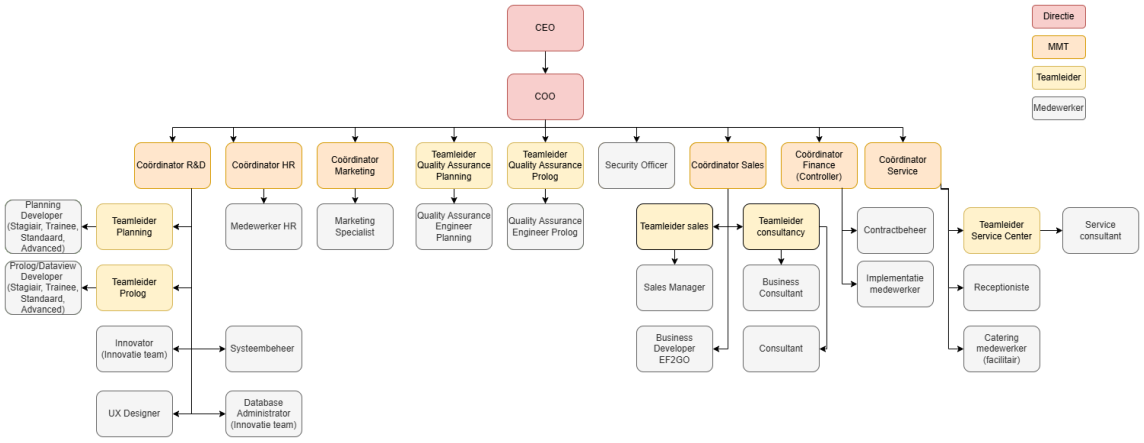
3.1.3. Doelstellingen van de onderneming

De hoofddoelstellingen van Easyflex luiden als volgt:

1. Waarborgen dat onze klanten gebruik kunnen blijven maken van onze dienstverlening, waarbij de relevante wetten en regelgeving correct is geïmplementeerd.
2. Voldoen aan onze contactuele verplichtingen en onze SLA.
3. De reputatie van Easyflex als betrouwbare partner waarborgen.
4. Bewust maken en houden van Easyflex personeel op het gebied van informatiebeveiliging.

3.2. Organisatiestructuur

De organisatie van Easyflex is weergegeven in onderstaand organogram.



Hieronder worden de functieprofielen kort toegelicht.

Functie	Verantwoordelijkheden
Business Consultant	Ondersteund klanten met implementaties en optimalisatie bedrijfsprocessen. Adviseert op medewerkers- en strategisch niveau.
Business Developer EF2GO	Monitoren, sturen en vast aanspreekpunt zijn voor (de voortgang van) projecten.
Catering medewerker (facilitair)	Het verzorgen en bereiden van de lunch. Zorg dragen voor het schoonhouden van de kantine, koffiezetapparaten en toiletten.
Consultant	Als consultant breng je de processen bij de klant in de praktijk op orde en help en adviseer je zowel bestaande als nieuwe klanten bij hun vraagstukken.

Contractbeheer	De Contractbeheerder is verantwoordelijk voor een correcte afhandeling van alle soorten contracten binnen Easyflex. Daarnaast is de Contractbeheerder verantwoordelijk voor: ALV en SLA, Invoeren en controleren van tarieven, Controleren en vastleggen features van klanten (bijv. ef2go, dataview), Vertrekkingen medewerkers vastleggen, Ondersteuning bieden aan facturatie, Opvolgen contractverlenging, Controleren opmaak contracten
Controller	Houdt toezicht op de financiële administratie, zorgt voor planning & control cyclus, maakt periodieke financiële rapportages, balansen, begroting/budgettering, jaarrekening, bewaakt de financiële positie en resultaten.
Chief Executive Officer	Eigenaar van EF. Vormt samen met de COO directie.
Chief Operating Officer	Geeft leiding aan de primaire processen binnen EF. Vormt samen met CEO directie. Neemt de dagelijkse leiding over van CEO. Uitrollen visie en strategie. Verbinden van afdelingen en mensen, geeft leiding aan MMT leden.
Coördinator • Beheer • Development • Sales • Service • Marketing en Communicatie	Verantwoordelijk voor het vertalen van strategie naar een afdeling. Stelt hier doelen, projecten, procedures en werkvormen op in. Speelt in op de markt. Geeft direct leiding aan een afdeling. Voert check-in en beoordelingsgesprekken, informeert MMT over voortgang.
Database Administrator (Innovatie team)	Structureren van informatie, het opslaan en toegankelijk maken met behulp van gespecialiseerde software.
Developer (Dataview, Planning, Prolog) • Advanced • Standaard • Trainee • Stagiair	Ontwikkelt, onderhoud en update software van EF, ontwerpt en ontwikkelt componenten op het software platform, stelt relevante documentatie op.
Human Resources	Interne communicatie tussen directie en personeel. Personeelsadministratie, verlonen, werven en selecteren, personeelsbeleid opstellen en deze voeren en opvolgen.

Innovator (Innovatie team)	Verbetert en vernieuwt de kernactiviteit van de applicatie. Identificeert ideeën en stimuleert om deze toe te passen in de organisatie.
Marketing Specialist	Uitvoeren van marketing doelstellingen, bedenken en uitrollen (innovatieve) salesacties, optimaliseren website, social media, mede organiseren evenementen, verzorgen promotiemateriaal, EF profileren in de markt, campagnes opzetten.
Quality Assurance Engineer	Waarborgen van kwaliteit van de applicatie en deliverables; stories, release notes, requirements, etc. Terugkoppelen testresultaten, opstellen requirements + inception deck, monitoren wet- en regelgeving, indienen wijzigingsvoorstellen wanneer wet-en regelgeving niet meer voldoet, deelnemen scrum teams.
Receptioniste	Zorgt voor een correcte, klantvriendelijk ontvangst van de klanten, correct doorverbinden binnenkomende telefoongesprekken, ondersteunen van diverse administratieve activiteiten.
Sales Manager	Verantwoordelijk voor commerciële doelen en acties, bezoekt en overtuigt prospects om klant te worden, speelt in op ontwikkelingen in de markt, informeert klanten over nieuwe functionaliteiten, meedenken marketing acties.
Implementatie Medewerker	Aanspreekpunt voor klanten tijdens de voorbereiding van de implementatie van onze software. Hieronder valt het maken van een planning, verzamelen van klantgegevens denk aan documentatie, bestaande systemen en processen.
Security Officer	Algemene zorg en uitvoering informatiebeveiligingsbeleid, bijstellen beleid informatievoorziening, coördineren risicobeoordeling en managementproces, vergroot beveiligingsbewustzijn EF mw, bewaakt voortgang, adviseert organisatie.
Service Consultant	Klanten ondersteuning bieden bij het gebruik van de Easyflex applicatie.
Systeembeheerder • Beheerder	Overziet en onderhoudt de ICT infrastructuur van de organisatie. Bij netwerkproblemen of andere technische complicaties handelend optreden om problemen op te lossen. Verzorgt alles omtrent de werkplekken.

Teamleider • Service • Planning • Prolog • Quality Assurance • Sales • Consultancy	Dagelijkse leiding over een afdeling. Je zorgt ervoor dat het team op een goede manier hun werk (kan) uitvoeren.
UX Designer	Als UX Designer onderzoek je de behoeften van gebruikers en vertaald dit naar ontwerpgerichte oplossingen om de bruikbaarheid en gebruikersvriendelijkheid te verbeteren.

3.2.1. Communicatiestructuur

Informatie en communicatie zijn noodzakelijk ter ondersteuning van de operationele processen en om beheersing mogelijk te maken. Easyflex werkt continu aan een betrouwbare en transparante informatievoorziening. Hieronder worden de verschillende communicatiestructuren besproken die hier invulling aan geven. Door aan de kwaliteit van informatie aandacht te besteden werkt Easyflex continu aan een betrouwbare informatievoorziening, die door de directie gezien wordt als een essentieel element bij het besturen en beheersen en de daarmee samenhangende (te nemen) beslissingen.

Easyflex hanteert de volgende communicatievormen binnen haar organisatie in het kader van informatiebeveiliging:

Intern overleg	**Samenstelling en doelen overleg**
Documenten review	Jaarlijks reviewen van documenten met betrekking tot informatiebeveiliging op juistheid en actualiteit.
Securityoverleg	Twee wekelijks bespreken van de stand van zaken en voortgang op het gebied van informatiebeveiliging.
Intern overleg	**Samenstelling en doelen overleg**
Management review	Jaarlijks beoordelen van het huidig ingerichte ISMS op opzet, bestaan en werking. Op basis van deze directiebeoordeling worden de strategische aspecten voor de komende jaarcyclus vastgesteld.

Tussentijds worden verschillende managementrapportages opgesteld, zowel voor eigen (intern) gebruik als voor de opdrachtgevers (gebaseerd op de SLA met de opdrachtgever). Enkele voorbeelden en de frequentie van de meest belangrijke managementinformatie:

- Budget, realisatie (maandelijks);

- Service center: wachttijden, aantal meldingen (wekelijks);
- SLA-realisatie opdrachtgevers (conform afspraken met opdrachtgevers);
- Incidenten (maandelijks);
- Projecten (varieert van wekelijks tot maandelijks);
- Penetratietesten (jaarlijks).

Tevens zijn er structureel overleggen/vergaderingen met de volgende externe partijen:

Extern overleg	Samenstelling en doelen overleg
Commissie Softwareleveranciers met ABU en NBBU	Beleidsadviseurs ABU en NBBU, directie van diverse softwareleveranciers.
OSWO- congress	Softwareontwikkelaars van diverse verloningsapplicaties, belastingdienst, UWV.

3.3. Risicomanagement

Met de dienstverlening op het gebied van essentiële en vertrouwelijke bedrijfsinformatie is Easyflex blootgesteld aan risico's op strategisch, operationeel, financieel en compliance gebied. Voor het beheersen van deze risico's is een uniform beleid ontwikkeld. Risicomanagement is een integraal onderdeel van de bedrijfsvoering.
De filosofie achter het risicomanagementbeleid is:

- De directie, het management en de Security Officer zijn verantwoordelijk voor de opzet en het testen van de werking van systemen van risicobeheersing en interne controle. Deze systemen hebben tot doel significante risico's te identificeren, de realisatie van doelstellingen te bewaken en het naleven van relevante wet- en regelgeving te waarborgen;
- Adequate systemen van risicobeheersing en interne controle zullen de kans op fouten, het nemen van verkeerde beslissingen en verrassingen door onvoorziene omstandigheden reduceren;
- Het risicomanagement is geïntegreerd in de lijnmanagementactiviteiten en de planning- en control-cyclus;
- Het nemen van risico's is essentieel voor een gezonde onderneming. De directie is eindverantwoordelijk voor de bepaling van wat daarbij maximaal acceptabel is (de zogenoemde risicoacceptatie).

3.3.1. Proces van risicomanagement

Het management weet wat de risicobereidheid van de onderneming is en waar de grenzen liggen die bij het functioneren van de onderneming in acht moeten worden genomen. Deze zijn vastgelegd in het risicoanalyse document.

Proces risico's inventariseren en prioriteiten stellen
Het proces 'prioriteiten stellen' wordt minimaal eenmaal per jaar uitgevoerd in het eerste kwartaal van het jaar of indien zich ontwikkelingen of veranderingen voordoen die grote invloed hebben op het bedrijf.

Stappen
Het prioriteringsproces wordt (o.a.) ondersteund door het uitvoeren van een risicoanalyse waarin informatiebeveiligingsrisico's worden geïdentificeerd. De methodiek wordt beschreven in het document 'Procedure risicoanalyse'. De Security Officer bereidt de prioriteitstelling voor door actuele informatie te verzamelen en deze te verwerken in het bestaande risicoanalysedocument. Het geactualiseerde concept document wordt voorgelegd aan het management ter consultatie en aanvulling. Vervolgens wordt het document door de directie goedgekeurd. Uit de prioriteitstelling kan volgen dat het beleid dient te worden aangescherpt. Ook volgen er gerichte verbetermaatregelen uit de prioritering.

Bij het bepalen van en reageren op risico's staat de vraag centraal welke ongewenste gebeurtenissen en belemmeringen onderkend kunnen worden in relatie tot de doelstellingen.

Aan de risicoanalyse zullen ten minste de volgende medewerkers deelnemen:
- Leden MT;
- Security Officer;
- (Optioneel) Extern expert.

Ter voorbereiding op de risicoanalyse sessie zal de Security Officer de benodigde documenten, ten minste één week van tevoren, toesturen naar de deelnemers:
- De risicoanalyse procedure;
- De resultaten van de voorgaande risicoanalyse sessies;
- De risicoanalyse worksheet;
- De resultaten van het monitoring proces.

Gedurende de meeting zullen de volgende acties ondernomen worden:
- Vaststellen van de volledigheid;
- Vaststellen van de waarschijnlijkheid en de impact;
- Volledigheid m.b.t. waarschijnlijkheid, impact en kwetsbaarheid vaststellen;
- Gap analyse;
- Maken van een Risk Treatment plan.

De directie van Easyflex bepaalt in samenwerking met de Security Officer hoeveel risico men wil nemen bij de vastgelegde risico's. Indien het risico groter is dan het risico wat men bereid is te nemen zal hier actie op ondernomen moeten worden door het ISO-team. De prioriteit is hierbij afhankelijk van de grootte van het gecalculeerde risico.

Indien de geactualiseerde risicoanalyse en de hieruit voortvloeiende verbetermaatregelen definitief zijn goedgekeurd wordt het door de Security Officer opgenomen in het afwijking- en verbeterregister en eventueel de ISMS-documentatie en worden medewerkers van het bedrijf hiervan op de hoogte gesteld.

Output
De inhoudelijke resultaten van de risicoanalyse, de prioritering en de voorgenomen verbetermaatregelen zullen worden gebruikt om het bedrijf te verbeteren. Met inachtneming van de getroffen preventieve maatregelen zijn de risico's kwalitatief

samengevat in de risicoanalyse. Jaarlijks tijdens de directiebeoordeling, of indien nodig eerder, zal deze risico-inventarisatie worden beoordeeld op actualiteit.

De interne beheersing van Easyflex is risico gebaseerd ingericht. Op basis van een risicohouding beoordelen wij de relevante risico's op verschillende deelgebieden en richten daarvoor een passend systeem van interne beheersing in.

3.3.2. Beheersing van de compliance en integriteitsrisico's

De directie heeft een breed scala van (sociale) maatregelen getroffen die bijdragen aan de vorming en instandhouding van de door gewenste organisatiecultuur. Hieronder vermelden wij er enkele maatregelen.

Gedragscode en bedrijfswaarden
Easyflex heeft een arbeidsovereenkomst, personeelshandboek met een gedragscode waarin informatiebeveiliging een belangrijke plaats inneemt. Het Bedrijfsreglement bestaat uit huisregels en gedragsregels omtrent het gebruik van internet, netwerk en e-mail. De gedragscode voor informatiebeveiliging heeft tot doel om medewerkers en overige belanghebbenden te informeren over:

- De maatregelen die Easyflex heeft genomen op het gebied van informatiebeveiliging;
- De informatiebeveiligingsregels die onze organisatie stelt aan medewerkers en overige belanghebbenden.

Alle medewerkers hebben bij indiensttreding getekend voor de gedragsregels als onderdeel van hun arbeidsovereenkomst. Het onder de aandacht brengen van de gedragsregels is een onderdeel van het introductieprogramma voor nieuwe of tijdelijke medewerkers en de verantwoordelijkheid van de Security Officer. Hiermee beoogt de directie te bereiken dat gedragscode en bedrijfswaarden bij iedere medewerker bekend zijn. Naast informatie tijdens de introductieperiode wordt regelmatig aandacht gevraagd voor informatiebeveiliging en de gedragsregels.

Screening (i.v.m. informatiebeveiliging)
Easyflex heeft een screeningproces ingevoerd dat wordt toegepast bij het inhuren of aannemen van nieuwe medewerkers. Dit gebeurt in bijna alle gevallen in nauw overleg met de kandidaten die worden overwogen en die worden gescreend op betrouwbaarheid en deskundigheid. Easyflex vereist een VOG van medewerkers die in dienst treden. Ten behoeve van specifieke klanten kunnen aanvullende screeningseisen worden gesteld.

Functie- en taakbeschrijvingen (verdeling van de verantwoordelijk- en bevoegdheden)
De verdeling van de Taken, Verantwoordelijkheden en Bevoegdheden over de sleutelfunctionarissen binnen Easyflex is beschreven in het document 'Taken, bevoegdheden en verantwoordelijkheden'.

Functionerings- en beoordelingsgesprekken
Easyflex heeft voornamelijk medewerkers in vaste dienst, daarnaast wordt beperkt gebruik gemaakt van (zoveel mogelijk dezelfde) inleenkrachten. Die laatste worden veelal via onze detacheringsorganisatie ingeleend. Daardoor wordt gewerkt met krachten die bekend zijn binnen de organisatie. Er worden binnen Easyflex zowel functionerings- als beoordelingsgesprekken gevoerd met vaste intervallen.

Opleiding en trainen
Easyflex is zich ervan bewust dat (nieuwe) medewerkers optimaal inzetbaar zijn voor de aan hen opgedragen taken na een gedegen inwerkperiode en training. Om de verschillen tussen de gewenste en noodzakelijke kennis en vaardigheden op te heffen wordt er gewerkt met formele en informele trainingen coaching. De hiervoor benodigde middelen worden dan vastgesteld en ingepland in overleg met de medewerker.

3.4. Beheerprocessen en deelprocessen

Het operationele risicomanagement richt zich op het beheersen van de kwaliteit van de bedrijfsprocessen, zodanig dat de aan de diensten gestelde kwaliteitseisen worden gehaald. Deze operationele doelstellingen worden gerealiseerd door de uitvoering van de primaire processen en ondersteunende processen.

Change management development
Binnen Easyflex wordt er op een iteratieve manier ontwikkeld door alle ontwikkelteams. Binnen iedere iteratie worden de volgende stappen doorlopen:
- Prioriteren;
- Implementeren;
- Testen;
- Deployment.

Het change managementproces van development kent een tweetal soorten RFC's (request for change):
- Bugs: fouten in bestaande broncode;
- Features: requests voor verbeteringen en nog niet bestaande functionaliteiten.

RFC's kunnen vastgelegd worden door alle medewerkers van Easyflex. Een RFC bevat initieel altijd de volgende informatie:
- Volgnummer;
- Project;
- Aanleiding tot de wijziging;
- Omschrijving van de wijziging;
- Prioriteit;
- Impact risico;
- Of er sprake is van een security issue.

Change managementdatabasewijzigingen
Het change managementproces voor databasewijzigingen kent een tweetal types RFC’s:
- Database actie met order;
- Database actie zonder order.

Een verzoek om een database actie komt binnen. Als hier akkoord op wordt gegeven wordt bepaald of een order aangemaakt en ondertekend moet worden. Als er een order aan wordt gemaakt wordt de database actie niet uitgevoerd tot dat de order ondertekend terug is. Hierna wordt de actie uitgevoerd, de output wordt geregistreerd en de change wordt afgesloten.

Change management beheer
De afdelingen Beheer en Interne automatisering werken niet op dezelfde manier als de ontwikkelafdeling, zij volgen dan ook een apart change managementproces.
Eerst wordt de RFC aangemaakt. Deze wordt vervolgens beoordeeld, ingepland en gecoördineerd. Als laatste wordt de change geëvalueerd en afgesloten.

Logische Toegangsbeveiliging
Middels toegangsbeveiliging wordt gewaarborgd dat onbevoegde toegang tot informatiesystemen voorkomen wordt. Hiervoor worden de volgende middelen ingezet:
- Registratie van gebruikers;
- Beheer van speciale bevoegdheden;
- Beoordeling van toegangsrechten van gebruikers;
- Verantwoordelijkheden van gebruikers;
- Beheer van gebruikerswachtwoorden;
- Clean desk & clear screen.

Netwerkbeveiliging
De netwerkbeveiliging van Easyflex wordt op diverse manieren gewaarborgd:
- Toegangsbeheersing voor netwerken;
- Bescherming logische toegang tot poorten en configuraties;
- Scheiding van netwerken;
- Beheersingsmaatregelen voor netwerkverbindingen;
- Telewerken;
- Toegangsbeveiliging voor besturingssystemen;
- Toegangsbeveiliging voor toepassingen en informatie.

Fysieke toegangsbeveiliging
Het kantoorpand van Easyflex zijn fysiek beveiligd. In en om het pand van Easyflex zijn de onderstaande maatregelen geïmplementeerd:
- Alarm in het pand met pincodes;
- Alarmcentrale;
- Toegangstijden;
- Registratie van bezoekers;
- Authenticatiemiddelen (druppel en pincode);
- Stoppers om ramen te blokkeren;
- Sloten op kasten;
- Sloten op apparatuur;
- Extra beveiligde zones;
- Beveiligingsbedrijf op bedrijventerrein;
- ISO 27001 gecertificeerd datacenter.

Logging en monitoring
Om te zorgen dat onverhoopte onbevoegde informatieverwerkingsactiviteiten ontdekt worden, wordt het proces omtrent verslaglegging en monitoring gevolgd. In dit proces zijn de volgende zaken omschreven:
- Registratie van verstoring;
- Synchronisatie van systeemklokken;
- Bescherming van informatie inlogbestanden;

- Monitoring beschikbaarheid en capaciteit van de Easyflex systemen;
- Aanpassingen broncode.

Incident management
Er zijn binnen Easyflex meerdere manieren waarop een incident tot stand kan komen. Een aantal van deze manieren zijn:

Klantmeldingen
De klantmeldingen betreffen de meldingen die door de klanten telefonisch of per e-mail aan ons door worden gegeven. Deze meldingen worden verder door het service center, al dan niet samen met andere afdelingen, afgehandeld.

Hardware
Een hardware incident betreft een probleem van een medewerker van Easyflex met de hardware zoals bijvoorbeeld een niet werkende headset. Deze meldingen worden door de afdeling 'Beheer' afgehandeld.

Security
Een voorbeeld van een security incident is het kwijtraken van een USB-stick met daarop een export van klantdata. Zodra het incident gemeld is, treed de procedure 'Correctieve acties' in werking.

Facilitair
Een voorbeeld van een facilitair incident is 'de vaatwasser is kapot'. Deze incidenten worden afgehandeld door de administratie.

Software
Een voorbeeld van een software incident is 'Kleur van productieschema in Easyflex is roze, waardoor klanten kunnen denken dat we gehackt zijn'. Software incidenten kunnen zowel intern als extern gemeld worden. Afhankelijk van hun bron, worden ze of door het service center, of door development verder afgehandeld.

Issues
Grotere issues die meerdere klanten beslaan, die zowel intern als extern gemeld kunnen worden, worden behandeld binnen het issue overleg. In dit issue overleg is een afvaardiging van Easyflex aanwezig, zodat besproken kan worden wie het issue af moet handelen.

Leveranciersmanagement
Iedere potentiële leverancier moet vooraf worden geïnformeerd over het vereiste niveau van informatiebeveiliging. Ten einde, in voldoende mate, te garanderen dat onze eisen ten aanzien van informatiebeveiliging worden nagekomen, moeten deze expliciet gecommuniceerd worden.

Het is een expliciete wens van Easyflex dat leveranciers een geldig ISO27001:2013 certificaat hebben. Easyflex realiseert zich dat dit niet in alle gevallen mogelijk of noodzakelijk is. Daarom wordt bij leveranciers jaarlijks een risicoprofiel bepaald.

Leveranciers (met een risicoprofiel van hoog en midden) worden (minimaal) eens per jaar beoordeeld waarin wordt opgenomen wie de leverancier is, welke dienst zij leveren, wat hun risicoprofiel is, wat hen beoordeling is en het beoordelingsformulier waarmee de leverancier beoordeeld is.

Backup en recovery
Binnen Easyflex maken we gebruik van veel verschillende soorten informatiesystemen, elk voor hun eigen doeleinde. De manier en frequentie van backups zijn afhankelijk van werking van de informatiesysteem en bijbehorende data.

Binnen Easyflex wordt er onderscheid gemaakt in de volgende soorten data:

- Klantdata, dit is data die eigendom is van onze klanten, Easyflex verwerkt deze data voor haar klanten. Deze gegevens moeten op meerdere fysieke locaties worden veiliggesteld;
- Interne data. Dit is data die eigendom is van Easyflex, en gebruikt wordt om de dienstverlening van Easyflex te verzorgen/verbeteren. Ook hier moeten de contracten en financiële gegevens op meerdere fysieke locaties worden bewaard.

3.5. Beheerkader

In deze paragraaf zijn de beheersingsdoelstellingen van Easyflex benoemd gericht op de bescherming van (privacygevoelige) informatie. De onderstaande tabel bevat een samenvatting van de beheersprocessen inclusief beheersingsdoelstellingen. Een goede interne beheersing is voor Easyflex van zeer groot belang voor het behalen van de door de directie gestelde jaardoelen. Hoewel dit een belangrijk argument is, is het zeker niet het enige.

Easyflex werkt door het continu verbeteren en verder invoeren van haar beheerkader vooral ook aan het borgen van de kwaliteit van haar strategieën en de bedrijfsvoering. Enerzijds om de schaarse middelen zo goed mogelijk te besteden en anderzijds om de kwaliteit van de informatie te borgen waardoor het verlies van integriteit, vertrouwelijkheid en beschikbaarheid wordt voorkomen.

Voor de klanten van Easyflex is het essentieel dat de bedrijfsvoering van Easyflex en met name de ICT-dienstverlening goed en betrouwbaar verloopt. Een goede ICT-beheersing is daarbij een voorwaarde om te kunnen blijven beschikken over een ICT-infrastructuur die voldoet aan de kwaliteitseisen op het terrein van wet- en regelgeving, beschikbaarheid, vertrouwelijkheid, voldoende onderhoud en overdraagbaarheid. Om dit te bereiken maakt Easyflex gebruik van processen, procedures en vervolgens controles hierop.

Deze beheersprocessen en bijbehorende beheersingsdoelstellingen zijn door Easyflex gedefinieerd. Daarbij zijn voor ieder proces in scope de beheersingsdoelstellingen en de beheersingsmaatregelen beschreven. Deze vormen het interne controle raamwerk. Het informatiebeveiligingsbeleid biedt de kaders voor het interne controle raamwerk. De processen en procedures zijn opgesteld conform de kaders van het informatiebeveiligingsbeleid.

Proces	Deelproces	Beheersingsdoelstelling
Change management	Change management development	Het waarborgen dat wijzigingen in programmatuur op een gestructureerde en beheerste wijze worden uitgevoerd, getest en in productie genomen.
	Change management infrastructuur	Het waarborgen dat infrastructurele wijzigingen op een gestructureerde en beheerste wijze worden uitgevoerd, getest en in productie genomen.
	Change management database	Het waarborgen dat wijzigingen in databases op een gestructureerde en beheerste wijze worden uitgevoerd, getest en in productie genomen.
Toegangs-beveiliging	Logische Toegangsbeveiliging	Het waarborgen dat slechts geautoriseerde medewerkers toegang hebben tot gegevens en programmatuur.
	Netwerkbeveiliging	Het waarborgen dat onbevoegden van buiten de organisatie geen toegang verkrijgen tot netwerken, systemen en gegevens.
	Fysieke Toegangsbeveiliging	Het waarborgen dat locaties slechts toegankelijk zijn voor bevoegde personen
	Logging en monitoring	Het waarborgen dat de wijzigingen in de beschikbaarheid van systemen tijdig worden ontdekt en dat adequate maatregelen worden getroffen.
Incident- en problem management	Incident- en problem management	Het waarborgen dat incidenten tijdig worden opgelost.
	Leveranciersmanagement	Het waarborgen dat afspraken over de dienstverlening door leveranciers worden vastgelegd en gemonitord.
	Backup en recovery	Het waarborgen dat bij verlies van gegevens en programmatuur reservekopieën van beschikbaar zijn.

3.6. Sub-serviceorganisaties

De sub-serviceorganisaties die gebruikt worden door Easyflex zijn:

- Interconnect
  - Interconnect is de leverancier achter de datacenters in Den Bosch en Eindhoven waar Easyflex gebruik van maakt;
  - De dienstverlening van Interconnect is van kritiek belang voor Easyflex;
  - Interconnect beschikt over een ISO27001:2013 certificering, tevens wordt Interconnect jaarlijks beoordeeld door Easyflex en wordt er een bezoekersregistratie van de datacenters bijgehouden.
- Proximus NXT
  - Easyflex maakt gebruik van de managed services van Proximus NXT;
  - De dienstverlening van Proximus NXT is van kritiek belang voor Easyflex;
  - Proximus NXT beschikt over een ISO27001:2013 certificering, tevens wordt Proximus NXT jaarlijks beoordeeld door Easyflex en ontvangt Easyflex ieder kwartaal een Servicemanagement rapportage

Voor de bovenstaande sub-serviceorganisaties wordt gebruik gemaakt van de carve-out methode.

3.7. Overwegingen ten behoeve van de gebruiker

De beheersingsmaatregelen die door Easyflex worden uitgevoerd, vormen een beperkt deel van de totale beheersingsmaatregelen waar de opdrachtgever zelf voor verantwoordelijk is. Het beheer en onderhoud van de Easyflex software is ontworpen in de veronderstelling dat gebruikersorganisaties (klanten) zelf een reeks beheersingsmaatregelen implementeren. In bepaalde situaties is de toepassing van deze beheersingsmaatregelen aan de kant van de gebruikersorganisatie noodzakelijk om de genoemde beheerdoelstellingen in onze beschrijving van beheer en onderhoud van de Easyflex software te bereiken. Derhalve dient de gebruikersorganisatie deze beheersmaatregelen te beoordelen in samenhang met de beheersmaatregelen van Easyflex zoals genoemd in sectie III en sectie IV van dit rapport.

Hieronder noemen wij de beheersingsmaatregelen die de gebruikersorganisatie zou moeten overwegen als aanvulling op de door ons getroffen maatregelen. Het management van de gebruikersorganisatie dient samen met zijn auditor te evalueren of deze maatregelen in toereikende mate geïmplementeerd en operationeel zijn:

- Indien de ICT-middelen van de gebruikersorganisatie (ten dele) in beheer zijn ondergebracht bij een andere dienstverlener dan die van Easyflex, dan dient de gebruikersorganisatie te borgen dat deze omgeving voldoet aan de gestelde eisen;
- De gebruikersorganisatie dient een adequaat beveiligingsniveau te implementeren op haar ICT-middelen;
- De gebruikersorganisatie dient adequaat gebruikersbeheer te implementeren voor zover niet in beheer bij Easyflex;

- De gebruikersorganisatie dient alle wijzigingen op haar ICT-middelen voor implementatie goed te keuren en achteraf (functioneel) te testen;
- De gebruikersorganisatie dient de rapportages en berichtgevingen van Easyflex tijdig te monitoren en tijdig Easyflex op de hoogte te stellen van eventuele tekortkomingen;
- Easyflex vervult een rol als supply-organisatie. De gebruikersorganisatie dient een demand organisatie in te richten ten behoeve van de aansturing van Easyflex.

Deze maatregelen zijn niet limitatief; additionele maatregelen kunnen noodzakelijk zijn binnen de gebruikersorganisatie. De auditor van opdrachtgever van Easyflex dient te beoordelen of deze maatregelen zijn geïmplementeerd binnen de gebruiksorganisatie.

3.8. Wijzigingen gedurende verslagperiode

Gedurende verslagperiode van 1 januari 2024 tot en met 31 december 2024 zijn er geen wijzigingen geweest die impact (kunnen) hadden op het beheerkader.

4. Beheersingsmaatregelen, testwerkzaamheden en -resultaten

In dit hoofdstuk is het beheersingsraamwerk met de beheersingsdoelstellingen en de beheersingsmaatregelen beschreven met daarbij de toelichting van DNV op de uitgevoerde testwerkzaamheden en haar conclusies.

4.1. Definitie testwerkzaamheden

De testresultaten zijn tot stand gekomen door het verrichten van de volgende testactiviteiten:

Type test	Beschrijving
Interview	Het verkrijgen van informatie over de naleving van beheersingsmaatregelen door middel van gesprekken met management en medewerkers
Observatie	Het ter plaatse waarnemen van de uitvoering van beheersingsmaatregelen
Inspectie	Het inzien en controleren van (fysieke) bronnen waaronder documenten, rapporten, systeeminstellingen en andere gegevens
Hernieuwd uitvoeren	Toelichting en het opnieuw uitvoeren van eerder door management of medewerkers uitgevoerde beheersingsmaatregelen

Voor de steekproefomvang handhaven wij de volgende methodiek:

Steekproefomvang	ISAE 3402 type II
Dagelijkse proces controls	25 tot 40 (afhankelijk van het risico)
Wekelijkse processen	5 tot 12 (afhankelijk van het risico)
Maandelijkse processen	2 tot 4 (afhankelijk van het risico)
Driemaandelijkse processen	2
Jaarlijkse processen	1
Ad hoc	10% met een maximum van 40 (afhankelijk van het risico)
Geautomatiseerd	Minimaal 2 (indien er sprake is van applicatieve controls bijvoorbeeld om negatieve scenario's tijdens de lijncontroles uit te voeren)

4.2. Testresultaten

In deze paragraaf zijn de door Easyflex geïmplementeerde beheersingsdoelstellingen en -maatregelen, de door DNV uitgevoerde testwerkzaamheden en de conclusies hiervan beschreven.

ID	Beheersingsmaatregel	Uitgevoerde testwerkzaamheden	Conclusie
Change management development Het waarborgen dat wijzigingen in programmatuur op een gestructureerde en beheerste wijze worden uitgevoerd, getest en in productie genomen.			**Doelstelling Behaald**
CH01	De organisatie heeft een change management procedure en heeft deze beschikbaar gesteld aan de medewerkers.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat de organisatie beschikt over een change management procedure en deze beschikbaar heeft gesteld aan de medewerkers. *Geen bevindingen geconstateerd.*	Effectief
CH02	De organisatie heeft gescheiden ontwikkel-, test- en productieomgevingen ingericht.	Op basis van interviews met proceseigenaren en systeeminstellingen hebben wij vastgesteld dat de organisatie gescheiden ontwikkel-, test- en productieomgevingen heeft ingericht. *Geen bevindingen geconstateerd.*	Effectief
CH03	Development changes worden: • vastgelegd in een ticketsysteem; • door minimaal een andere ontwikkelaar gereviewd.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat development changes worden vastgelegd in een ticketsysteem en door minimaal een andere ontwikkelaar wordt gereviewd. *Geen bevindingen geconstateerd.*	Effectief
Change management infrastructuur Het waarborgen dat infrastructurele wijzigingen op een gestructureerde en beheerste wijze worden uitgevoerd, getest en in productie genomen.			**Doelstelling Behaald**
CH04	Infrastructurele changes worden: • vastgelegd in een ticketsysteem; • beoordeeld en goedgekeurd door een beheerder.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat infrastructurele changes worden vastgelegd in een ticketsysteem en worden beoordeeld en goedgekeurd door een beheerder. *Geen bevindingen geconstateerd.*	Effectief
CH05	Database changes worden: • vastgelegd in een ticketsysteem; • vooraf goedgekeurd door de klant.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat database changes worden vastgelegd in een ticketsysteem en vooraf worden goedgekeurd door de klant. *Geen bevindingen geconstateerd.*	Effectief

ID	Beheersingsmaatregel	Uitgevoerde testwerkzaamheden	Conclusie
CH06	Changes worden maandelijks gecontroleerd door de teamleider.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat changes maandelijks worden gecontroleerd door de teamleider. *Geen bevindingen geconstateerd.*	Effectief
CH07	Infrastructurele changes worden maandelijks gecontroleerd door de coördinator.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat infrastructurele changes maandelijks worden gecontroleerd door de coördinator. *Geen bevindingen geconstateerd.*	Effectief
Change managementdatabase Het waarborgen dat wijzigingen in databases op een gestructureerde en beheerste wijze worden uitgevoerd, getest en in productie genomen.			**Doelstelling Behaald**
CH08	Database changes worden maandelijks gecontroleerd door de teamleider.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat database changes maandelijks worden gecontroleerd door de teamleider. *Geen bevindingen geconstateerd.*	Effectief
CH09	Testgegevens zijn gepseudonimiseerd en worden geautomatiseerd gecontroleerd door middel van een script in Jenkins.	Op basis van interviews met proceseigenaren en registraties hebben wij vastgesteld dat testgegevens zijn gepseudonimiseerd en worden geautomatiseerd gecontroleerd door middel van een script in Jenkins. *Geen bevindingen geconstateerd.*	Effectief
Logische toegangsbeveiliging Het waarborgen dat slechts geautoriseerde medewerkers toegang hebben tot gegevens en programmatuur.			**Doelstelling Behaald**
LT01	De organisatie beschikt over een toegangsbeleid.	Op basis van interviews met proceseigenaren en inspectie van documentatie hebben wij vastgesteld dat de organisatie beschikt over een toegangsbeleid. *Geen bevindingen geconstateerd.*	Effectief
LT02	Rechten van medewerkers worden toegekend op basis van een rollen- en rechtenmatrix.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat rechten van medewerkers worden toegekend op basis van een rollen- en rechtenmatrix. *Geen bevindingen geconstateerd.*	Effectief
LT03	Tijdelijke toegangsrechten van medewerkers worden beoordeeld en uitgegeven door de teamleiders of coördinator.	Op basis van interviews met proceseigenaren, systeeminstellingen en registraties hebben wij vastgesteld dat tijdelijke toegangsrechten van medewerkers worden beoordeeld en uitgegeven door de teamleiders of coördinator.	Effectief

ID	Beheersingsmaatregel	Uitgevoerde testwerkzaamheden	Conclusie
		Geen bevindingen geconstateerd.	
LT04	Tijdelijke toegangsrechten van medewerkers worden automatisch ingetrokken.	Op basis van interviews met proceseigenaren, systeeminstellingen en registraties hebben wij vastgesteld dat tijdelijke toegangsrechten van medewerkers automatisch worden ingetrokken. *Geen bevindingen geconstateerd.*	Effectief
LT05	Toegangsrechten worden ingetrokken of aangepast wanneer medewerkers de organisatie verlaten.	Op basis van interviews met proceseigenaren, systeeminstellingen en registraties hebben wij vastgesteld dat toegangsrechten worden ingetrokken of aangepast wanneer medewerkers de organisatie verlaten. *Geen bevindingen geconstateerd.*	Effectief
LT06	Wijzigingen in de rollen- en rechtenmatrix worden uitgevoerd door het ISO-team	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat wijzigingen in de rollen- en rechtenmatrix worden uitgevoerd door het ISO-team *Geen bevindingen geconstateerd.*	Effectief
LT07	Uitgegeven toegangsrechten worden maandelijks gecontroleerd door de Security Officer.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat uitgegeven toegangsrechten maandelijks worden gecontroleerd door de Security Officer. *Geen bevindingen geconstateerd.*	Effectief
LT08	De organisatie heeft een wachtwoordbeleid geïmplementeerd.	Op basis van interviews met proceseigenaren en inspectie van documentatie, systeeminstellingen en registraties hebben wij vastgesteld dat de organisatie een wachtwoordbeleid heeft geïmplementeerd. *Geen bevindingen geconstateerd.*	Effectief
Netwerkbeveiliging Het waarborgen dat onbevoegden van buiten de organisatie geen toegang verkrijgen tot netwerken, systemen en gegevens.			**Doelstelling Behaald**
NB01	De organisatie heeft software om malware te detecteren geïnstalleerd op systemen van medewerkers.	Op basis van interviews met proceseigenaren en inspectie van documentatie, systeeminstellingen en registraties hebben wij vastgesteld dat de organisatie software om malware te detecteren heeft geïnstalleerd op systemen van medewerkers. *Geen bevindingen geconstateerd.*	Effectief
NB02	De organisatie maakt gebruik van beveiligde verbindingen en beschikt over een formeel	Op basis van interviews met proceseigenaren en inspectie van documentatie, systeeminstellingen en registraties hebben wij vastgesteld dat de	Effectief

ID	Beheersingsmaatregel	Uitgevoerde testwerkzaamheden	Conclusie
	certificaat lifecycle management procedure.	organisatie gebruik maakt van beveiligde verbindingen en beschikt over een formeel certificaat lifecycle management procedure. *Geen bevindingen geconstateerd.*	
NB03	De organisatie voert jaarlijks een pentest uit.	Op basis van interviews met proceseigenaren en inspectie van documentatie hebben wij vastgesteld dat de organisatie jaarlijks een pentest uitvoert. *Geen bevindingen geconstateerd.*	Effectief
Fysieke beveiliging Het waarborgen dat locaties slechts toegankelijk zijn voor bevoegde personen			**Doelstelling Behaald**
FB01	De organisatie heeft een toegangsbeleid gedefinieerd en geïmplementeerd.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat de organisatie een toegangsbeleid heeft gedefinieerd en geïmplementeerd. *Geen bevindingen geconstateerd.*	Effectief
FB02	Beveiligde zones zijn gedefinieerd om ongeautoriseerd toegang te voorkomen.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat beveiligde zones zijn gedefinieerd om ongeautoriseerd toegang te voorkomen. *Geen bevindingen geconstateerd.*	Effectief
FB03	Bezoekers worden aangemeld en geregistreerd.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat bezoekers worden aangemeld en geregistreerd. *Geen bevindingen geconstateerd.*	Effectief
FB04	Druppels worden uitgegeven en ingenomen bij in- en uitdiensttreding.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat druppels worden uitgegeven en ingenomen bij in- en uitdiensttreding. *Geen bevindingen geconstateerd.*	Effectief
FB05	Buiten kantoortijden is het pand toegankelijk met een 24-uurs code.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat het pand buiten kantoortijden toegankelijk is met een 24-uurs code. *Geen bevindingen geconstateerd.*	Effectief
FB06	Dagdruppels worden uitgegeven en ingenomen. Dat wordt geregistreerd in Confluence.	Op basis van interviews met proceseigenaren en registraties hebben wij vastgesteld dat dagdruppels worden uitgegeven en ingenomen en geregistreerd in Confluence.	Effectief

ID	Beheersingsmaatregel	Uitgevoerde testwerkzaamheden	Conclusie
		Geen bevindingen geconstateerd.	
FB07	Laptops zijn beveiligd met een Bitlocker.	Op basis van interviews met proceseigenaren en inspectie van documentatie, systeeminstellingen en registraties hebben wij vastgesteld dat Laptops beveiligd zijn met een Bitlocker. *Geen bevindingen geconstateerd.*	Effectief
FB08	De organisatie heeft een clear desk beleid gedefinieerd en geïmplementeerd.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat de organisatie een clear desk beleid heeft gedefinieerd en geïmplementeerd. *Geen bevindingen geconstateerd.*	Effectief
Logging en monitoring Het waarborgen dat de wijzigingen in de beschikbaarheid van systemen tijdig worden ontdekt en dat adequate maatregelen worden getroffen.			**Doelstelling Behaald**
LM01	Capaciteit, performance en beschikbaarheid van systemen wordt gemonitord met geautomatiseerde hulpmiddelen.	Op basis van interviews met proceseigenaren en inspectie van documentatie, systeeminstellingen en registraties hebben wij vastgesteld dat capaciteit, performance en beschikbaarheid van systemen wordt gemonitord met geautomatiseerde hulpmiddelen. *Geen bevindingen geconstateerd.*	Effectief
LM02	Dagelijks is een beheerder verantwoordelijk voor het monitoren van de systemen en opvolgen van events.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat dagelijks een beheerder verantwoordelijk is voor het monitoren van de systemen en opvolgen van events. *Geen bevindingen geconstateerd.*	Effectief
LM03	Logregels worden weggeschreven naar een beveiligde server die slechts toegankelijk is voor bevoegde medewerkers.	Op basis van interviews met proceseigenaren en inspectie van documentatie, systeeminstellingen en registraties hebben wij vastgesteld dat logregels worden weggeschreven naar een beveiligde server die slechts toegankelijk is voor bevoegde medewerkers. *Geen bevindingen geconstateerd.*	Effectief
Incident en problem management Het waarborgen dat incidenten tijdig worden opgelost.			**Doelstelling Behaald**
IC01	De organisatie heeft een incident management procedure en heeft deze beschikbaar gesteld aan de medewerkers.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat de organisatie een incident managementprocedure heeft ingericht en beschikbaar gesteld aan de medewerkers. *Geen bevindingen geconstateerd.*	Effectief

ID	Beheersingsmaatregel	Uitgevoerde testwerkzaamheden	Conclusie
IC02	Incidenten worden: • vastgelegd in een ticketsysteem; • afgehandeld en teruggekoppeld aan de klant.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat niet voor alle incidenten de terugkoppeling aan de klant aantoonbaar is. *Bevinding geconstateerd: Niet voor alle incidenten is een terugkoppeling naar de klant aantoonbaar.*	Niet effectief
IC03	Informatiebeveiligingsincidenten worden: • vastgelegd in een ticketsysteem; • beoordeeld door de Security Officer; • geëvalueerd en opgelost.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat informatiebeveiligingsincidenten worden vastgelegd in een ticketsysteem, beoordeeld worden door de Security Officer en worden geëvalueerd en opgelost. *Geen bevindingen geconstateerd.*	Effectief
IC04	Tweewekelijks vinden er ISO-overleggen plaats om openstaande incidenten te bespreken.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat er tweewekelijks ISO-overleggen plaatsvinden om openstaande incidenten te bespreken. *Geen bevindingen geconstateerd.*	Effectief
IC05	Problems worden twee maandelijks in een issue overleg besproken en afgehandeld.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat problems twee maandelijks in een issue overleg worden besproken en afgehandeld. *Geen bevindingen geconstateerd.*	Effectief
Leveranciersmanagement Het waarborgen dat afspraken over de dienstverlening door leveranciers worden vastgelegd en gemonitord.			**Doelstelling Behaald**
LE01	Afspraken met leveranciers worden vastgelegd in een overeenkomst en SLA.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat afspraken met leveranciers worden vastgelegd in een overeenkomst en SLA. *Geen bevindingen geconstateerd.*	Effectief
LE02	Jaarlijks wordt er een leveranciersbeoordeling uitgevoerd.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld dat er jaarlijks een leveranciersbeoordeling wordt uitgevoerd. *Geen bevindingen geconstateerd.*	Effectief

ID	Beheersingsmaatregel	Uitgevoerde testwerkzaamheden	Conclusie
LE03	De organisatie wordt op de hoogte gehouden van verstoringen van diensten die invloed kunnen hebben op de dienstverlening.	Op basis van interviews met proceseigenaren en registraties hebben wij vastgesteld dat de organisatie op de hoogte wordt gehouden van verstoringen van diensten die invloed kunnen hebben op de dienstverlening. *Geen bevindingen geconstateerd.*	Effectief
Backup en recovery Het waarborgen dat bij verlies van gegevens en programmatuur reservekopieën van beschikbaar zijn.			**Doelstelling Behaald**
BR01	De organisatie beschikt over een backup beleid.	Op basis van interviews met proceseigenaren en inspectie van documentatie hebben wij vastgesteld dat de organisatie beschikt over een backup beleid. *Geen bevindingen geconstateerd.*	Effectief
BR02	Backups worden uitgevoerd conform SLA.	Op basis van interviews met proceseigenaren en inspectie van documentatie en registraties hebben wij vastgesteld backups worden uitgevoerd conform SLA. *Geen bevinding geconstateerd.*	Effectief
BR03	Dagelijks wordt een restore uitgevoerd naar de supportomgeving.	Op basis van interviews met proceseigenaren en inspectie van documentatie, systeeminstellingen en registraties hebben wij vastgesteld dat dagelijks een restore wordt uitgevoerd naar de supportomgeving. *Geen bevindingen geconstateerd.*	Effectief