13 MAART 2026

MANAGEMENT LETTER 2025

Stichting Nederlands Fonds voor Podiumkunsten

Aan:

Aan: Stichting Nederlands Fonds voor Podiumkunsten

T.a.v. de directeur-bestuurder en de raad van toezicht
Koningin Julianaplein 10
2595 AA Den Haag

Den Haag, 13 maart 2026

Kenmerk: IB/SN/AA20260318

Geachte directeur-bestuurder en leden van de raad van toezicht,

U heeft ons gevraagd de jaarrekening 2025 van Stichting Nederlands Fonds voor Podiumkunsten (hierna: 'Fonds Podiumkunsten') te controleren. Naar aanleiding van onze interim-controle brengen wij met deze management letter verslag uit over onze bevindingen.

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

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

Het vervolg van onze werkzaamheden voor de controle van de jaarrekening staat gepland in december, januari en februari 2026. Hier zijn met de controller afspraken over gemaakt.

Op basis van Nederlands recht en overige beroepsregels, zoals de 'Verordening inzake de onafhankelijkheid van accountants bij assuranceopdrachten' (ViO), is vereist dat wij onafhankelijk zijn ten opzichte van onze controle-cliënten. Wij zijn van mening dat door ons is voldaan aan deze eisen. Wij hebben de overige dienstverlening naast de controle van de jaarrekening beoordeeld aan de hand van onze beroepsregels en hebben geconcludeerd dat het type dienstverlening en de vergoeding onze onafhankelijkheid niet beïnvloeden.

Wij vertrouwen erop u met dit verslag van dienst te zijn. Vanzelfsprekend zijn wij graag bereid om een nadere toelichting op de inhoud te geven.

Hoogachtend/Met vriendelijke groet,

BDO Audit & Assurance B.V.
namens deze,

Digitaal ondertekend door:

Ilona Bothoff - Van Hoff
13 maart 2026 12:46 +01:00

L.C (Ilona) Bothoff- van Hoff MSc RA
Partner en extern accountant Fonds Podiumkunsten

Inhoudsopgave

1. Ontwikkelingen & Aandachtspunten

1.1 Interne ontwikkelingen

Voor Fonds Podiumkunsten zien we op dit moment de volgende belangrijke interne ontwikkelingen:

Vertrek controller

De huidige controller gaat in september 2025 met pensioen na een langdurig dienstverband. Ter voorbereiding op zijn vertrek is per januari 2025 een interim-controller aangesteld. Het is van belang om de opgebouwde kennis en ervaring zorgvuldig te documenteren en over te dragen. De interim-controller is aangetrokken om de organisatie actief te ondersteunen en te adviseren bij het vormgeven van de toekomstige invulling van de functie van controller. Hierbij wordt ook rekening gehouden met de aanstaande wijzigingen in de organisatiestructuur. U bent momenteel bezig met de herinrichting van uw organisatie. Ook de nieuwe functiebeschrijvingen voor de junior controller en business controller zullen worden uitgewerkt.

Nieuwe subsidieronde 2025-2028

Fonds Podiumkunsten is gestart met een nieuwe subsidieronde voor de periode 2025-2028. Tijdens onze controle hebben wij het handboek verantwoording cultuursubsidies 2025-2028 en het concept accountantsprotocol cultuursubsidies 2025-2028 beoordeeld. De wijzigingen in het handboek zijn beperkt en hebben geen gevolgen voor de jaarrekening of onze controlewerkzaamheden. In het accountantsprotocol is een relevante wijziging doorgevoerd: de toegestane maximale afwijking, en daarmee onze materialiteit, ten aanzien van de financiële rechtmatigheid in het financieel verslag is verhoogd naar 3% van de totale baten, waar dit in voorgaande jaren 2% betrof. Ook voor de projectsubsidies is de materialiteit verhoogd naar 3%. Deze wijziging heeft beperkte impact op onze controlewerkzaamheden, omdat wij voornamelijk systeemgerichte werkzaamheden uitvoeren. De afgelopen subsidieronde hebben wij de materialiteit bepaald op basis van de toekenningen van de meerjarige subsidies per jaarlaag in plaats van het jaar van toekenning (en daarmee de baten in de jaarrekening). Deze methodiek is in het verleden door het Ministerie van Onderwijs, Cultuur en Wetenschap goedgekeurd. Voor het nieuwe accountantsprotocol hebben wij u verzocht eveneens goedkeuring te vragen voor de toepassing van deze methodiek. Wij vragen u af te stemmen of dit geformaliseerd kan worden in het nieuwe accountantsprotocol.

Huisvesting

Vanaf 1 januari 2026 wordt het huidige kantoor gerenoveerd. Hierdoor was het Fonds genoodzaakt om op zoek te gaan naar nieuwe huisvesting. Naar verwachting zal de organisatie eind 2025 verhuizen naar het nieuw pand. In het nieuwe contract is een huurincentive opgenomen met een looptijd van 20 maanden. Wij adviseren u om bij het opstellen van de jaarrekening specifiek aandacht te besteden aan de juiste verwerking hiervan, conform de geldende verslaggevingsregels.

Nieuw systeem

Vanaf 1 januari 2025 maakt het Fonds gebruik van Microsoft Business Central als nieuw ERP pakket. Zowel de financiële administratie als de factuurautorisatie zitten nu in Microsoft Business Central. Wij hebben vastgesteld dat de beginbalans van het nieuwe systeem aansluit met de definitieve jaarrekening van 2024. Verder heeft IT-audit hier diverse controles op verricht om te beoordelen of de implementatie en het gebruik van Microsoft Business Central conform de gestelde eisen en richtlijnen verlopen. Hierbij is gekeken naar aspecten als gegevensbeveiliging, betrouwbaarheid van de financiële processen en de mate waarin het systeem voldoet aan de organisatorische behoeften. Zie hoofdstuk 2.4 voor de bevindingen.

1.2 Externe ontwikkelingen

Voor Fonds Podiumkunsten zien we op dit moment de volgende belangrijke externe ontwikkelingen:

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

De NIS2 (Network and Information Security 2) richtlijn is een update van de in 2016 ingevoerde NIS-richtlijn. In Nederland ook wel bekend als NIB2 (Netwerk- en informatiebeveiligingsrichtlijn) en/of de Wbni (Wet Beveiliging Netwerk- en Informatiesystemen). De NIS2 is vastgesteld door de Europese Unie en is bedoeld om de cyberveiligheid en de cyberweerbaarheid van essentiële diensten in EU-lidstaten te verhogen. Met deze nieuwe richtlijn worden organisaties die van vitaal belang zijn voor de samenleving binnen de EU, verplicht de NIS2-maatregelen te implementeren. Zo dienen organisaties extra cybersecuritymaatregelen te implementeren, hun digitale systemen te beschermen tegen geavanceerde cyberdreigingen en te kunnen aantonen dat zij voldoen aan deze aangescherpte regelgeving.

Niet in actie komen verhoogt de kans op disruptieve verstoring van bedrijfs-activiteiten, financiële verliezen, reputatieschade, en blootstelling van intellectueel eigendom en persoonsgegevens van uw personeel en cliënten. Het is van cruciaal belang dat Stichting Nederlands Fonds voor Podiumkunsten, als Zelfstandig Bestuursorgaan (ZBO) proactief actie onderneemt, doeltreffende maatregelen treft en bovenal veerkrachtige beveiligingsprocessen ontwikkelt en onderhoudt. De complexiteit van digitale infrastructuren, de noodzaak van samenwerking met toeleveringsketenpartners en de groeiende afhankelijkheid van digitale processen vergroten deze uitdagingen. In onze visie zijn proactieve investeringen in digitale beveiliging niet alleen wettelijk verplicht maar versterken deze ook de veerkracht en reputatie van organisaties, en ultimo de samenleving, op lange termijn.

In de kern wordt NIS2 in Q3 2025 naar Nederlandse wetgeving vertaald en nadien van kracht onder de noemer ‘Cyberbeveiligingswet’.

Belangrijk is dat NIS2 aanvullende eisen stelt, die niet volledig door de huidige ISO270001- of een andere sectorspecifieke beveiligingscertificering worden afgedekt, wat betekent dat in de komende periode additionele maatregelen moeten worden getroffen ten einde aan NIS2 te voldoen.

De volgende verplichtingen vallen onder NIS2:

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

Organisaties vallen direct onder de NIS2-richtlijn en daarmee de Cyberbeveiligings-wet, als zij actief zijn in aangewezen sectoren en gekenmerkt worden als ‘essentiële’ of ‘belangrijke’ entiteit. Direct wil zeggen dat bovengenoemde verplichtingen voor deze organisaties direct gaan gelden zodra de wet in werking treedt.

Stichting Nederlands Fonds voor Podiumkunsten heeft onderzocht in hoeverre zij NIS2 plichtig zijn. Hier heeft zij invulling aan gegeven door maatregelen te treffen op het gebied van informatiebeveiliging. Het is van belang dat Stichting Nederlands Fonds voor Podiumkunsten proactief onderzoekt of en in hoeverre er wordt voldaan aan de toekomstige Cyberbeveiligingswet en daarop te acteren.

1.2 Externe ontwikkelingen

Informatiebeveiliging
Fonds Podiumkunsten beschikt over een actueel overzicht van het IT-landschap waarin onderscheid wordt gemaakt tussen de applicatiearchitectuur en de netwerkstructuur. De kernapplicatie Aims is hierin als kritieke applicatie (kroonjuweel) aangemerkt. Deze inventarisatie vormt een belangrijke basis voor risicobeheersing en sluit aan bij de zorgplicht zoals voorgeschreven in de NIS2-richtlijn.

In 2025 is een nieuw informatiebeveiligingsbeleid opgesteld, waarin het streven naar een veilige en betrouwbare informatieomgeving centraal staat. Dit beleid is gedeeld binnen de organisatie, maar het is en blijft van belang dat periodieke herziening structureel wordt geborgd. De rol van Chief Information Security Officer (CISO) wordt momenteel vervuld door de teamleider ICT. Hiermee is formeel invulling gegeven aan de verantwoordelijkheid voor informatiebeveiliging.

Op het gebied van bewustwording en training is sprake van een positieve ontwikkeling. Via de Phished Academy worden medewerkers getraind in het herkennen van cyberdreigingen en het correct omgaan met informatie. Dit draagt bij aan de weerbaarheid van de organisatie, een kernprincipe binnen de NIS2-richtlijn.

Hoewel er risicoanalyses worden uitgevoerd op applicatieniveau, ontbreekt een organisatiebrede, gestructureerde aanpak. Dit vormt een aandachtspunt, aangezien de NIS2-richtlijn vereist dat organisaties periodiek een integrale risicobeoordeling uitvoeren en op basis daarvan passende maatregelen treffen. Ook de dataclassificatie en de omgang met data/documenten is nog niet formeel vastgelegd, terwijl dit essentieel is voor het bepalen van beveiligingsniveaus en toegangsrechten. Toegangsbeheer is deels beschreven in OneNote en het informatiebeveiligingsbeleid, maar een formeel vastgestelde procedure ontbreekt.

Dit geldt eveneens voor het beleid rondom patchmanagement, dat momenteel in samenwerking met leverancier Yellow Arrow wordt uitgevoerd op basis van best practices van Microsoft. Hoewel dit in de praktijk functioneert, is het vanuit compliance-oogpunt noodzakelijk om dit proces te formaliseren.

De organisatie beschikt over een gesegmenteerde netwerkarchitectuur en maakt gebruik van Microsoft Defender voor antivirusbescherming. Logging en monitoring worden uitgevoerd via Phished en proxies, en incidenten worden geregistreerd in TopDesk, met opvolging door YellowArrow. Er is een incident responseplan aanwezig, maar het IT Continuïteitsplan wordt niet jaarlijks getest, wat een risico vormt voor de bedrijfscontinuïteit bij calamiteiten.

Tot slot worden er wel securityscans en penetratietests uitgevoerd, maar ook hier ontbreekt een formeel beleid en een vaste frequentie. Dit is een belangrijk aandachtspunt, aangezien de NIS2-richtlijn expliciet stelt dat organisaties hun beveiligingsmaatregelen moeten kunnen aantonen en onderbouwen.

2. Bevindingen interim-controle jaarrekening

2.1 Onze werkzaamheden

1/2

Controleaanpak en doel van de interim-controle

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

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

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

Onze inschatting van de risico's

In het kader van de controle van de jaarrekening 2025 en onze aanpak hebben wij een zogenaamde initiële risico-inschatting gemaakt. Wij zien de volgende potentiële risico's in de controle van de jaarrekening van Fonds Podiumkunsten:

- Management override. In onze controlestandaarden (NV COS) wordt expliciet het risico van management override (bewuste beïnvloeding door bestuur of management van de jaarcijfers) als belangrijk te onderkennen theoretisch risico benoemd. Als accountant moeten wij in onze werkzaamheden hier specifiek aandacht aan besteden. Bij Fonds Podiumkunsten is geen sprake van significante schattingsposten. Het risico op transacties buiten de normale bedrijfsvoering en memoriaalboekingen rondom jaarafsluiting is bij Fonds Podiumkunsten niet gerelateerd aan specifieke posten. Wij zijn van mening dat de mogelijkheden, om buiten de getroffen interne beheersmaatregelen invloed uit te oefenen op de in de jaarrekening gepresenteerde uitkomsten, beperkt zijn. Om het resterende risico te beperken beoordelen wij bijzondere journaalposten in detail.
- Onrechtmatig verleende subsidies door het niet voldoen aan de subsidievoorwaarden. In het controleprotocol wordt specifiek benoemd dat wij dienen te controleren of de subsidie rechtmatig besteed is. In het controleplan wordt onder de definitie van rechtmatigheid alleen gesproken over de toegekende subsidies. Indirect vallen de apparaatskosten ook onder de rechtmatigheid, omdat in de subsidietoekenning wordt vermeld dat de subsidie alleen besteed mag worden aan de activiteiten waarvoor deze verleend is. Gezien de aarde van de apparaatskosten en de spreiding over de verschillende kosten onderkennen wij ten aanzien van de apparaatskosten geen significant risico.
- Frauderisico opbrengsten subsidies OCW. In onze controlestandaarden (NV COS) wordt verondersteld dat er een frauderisico in de opbrengstverantwoording bestaat. Het veronderstelde frauderisico ten aanzien van de subsidies OCW die worden ontvangen vanuit het OCW is laag. Het frauderisico dat wij onderkennen ziet primair toe op de onrechtmatig verlenen van de subsidies (zie risico onrechtmatig verleende subsidies door het niet voldoen aan de subsidievoorwaarden). Het frauderisico dat wij onderkennen in de opbrengstverantwoording ten aanzien van de opbrengsten ziet daarom enkel toe op financiële verslaggevingsfraude door middel van memoriaalboekingen in de baten.
- Onrechtmatige inkopen overige bedrijfskosten: Omdat er onvoldoende functiescheiding is tussen het wijzigen van crediteurenstamgegevens en het autoriseren van inkoopfacturen bestaat het risico op onrechtmatige inkopen ten aanzien van de overige bedrijfskosten. De medewerker kan zowel de crediteur aanmaken/crediteurenstamgegevens wijzigen en zelfstandig facturen autoriseren.

2.1 Onze werkzaamheden

2/2 Aandacht voor fraude

Onze bevindingen

Bij de planning voor de jaarrekeningcontrole houden wij rekening met het risico dat de jaarrekening als gevolg van fraude en onregelmatigheden onjuistheden van materieel belang zou kunnen bevatten. Daarnaast hebben wij beoordeeld in hoeverre sprake kan zijn van een risico omtrent corruptie of een risico omtrent het niet-naleven van wet- en regelgeving.

Eén van de door ons uitgevoerde maatregelen is het bespreken van de mogelijke frauderisico's en mogelijke fraudesituaties op verschillende niveaus binnen de organisatie. Hiertoe hebben wij de mogelijke frauderisico's en -situaties, besproken met de controller. Deze besprekingen en onze controlewerkzaamheden hebben geen indicaties voor materiële fraude opgeleverd. Wij hebben daarentegen wel vastgesteld dat u zelf nog geen frauderisicoanalyse heeft uitgevoerd. U heeft aangegeven dat dit onder handen is en naar verwachting eind 2025 gereed is. Wij zullen deze beoordelen als deze gereed is.

ONZE BEVINDINGEN			
Fraude	**2025**	**2024**	**Evaluatie**
Frauderisicoanalyse uitgevoerd	😑	—	Fonds Podiumkunsten is momenteel bezig met het uitvoeren van een frauderisicoanalyse. Het doel van deze analyse is het in kaart brengen van potentiële frauderisico's binnen de organisatie en het beoordelen van de bestaande beheersmaatregelen. Door deze risicoanalyse wordt inzicht verkregen in kwetsbaarheden, waardoor gerichte acties kunnen worden ondernomen om het risico op fraude te beperken en de interne beheersing te versterken. Naar verwachting is deze analyse eind 2025 gereed.
Gedragscode, klokkenluidersregeling en incidentenregistratie	🙂	🙂	Bij Fonds Podiumkunsten is een Code of Conduct (CoC) en klokkenluidersregeling aanwezig.
Frauderesponsplan	🙂	🙂	Fonds Podiumkunsten beschikt over een meldingsprocedure bij niet integer handelen.
Incidenten	🙂	🙂	Bij Fonds Podiumkunsten hebben gedurende 2025 geen incidenten plaatsgevonden.

2.2 Onze werkzaamheden bij de processen

Belangrijkste processen

Aan de navolgende processen hebben wij specifiek aandacht geschonken tijdens onze interim-controle:

- Subsidieproces
- Inkoopproces
- Betalingsorganisatie
- Personeelsproces
- Financiële verslaggevingsproces
- IT

Onze conclusie naar aanleiding van onze interim-controle is dat de interne beheersing toereikend is en dat de organisatie in control is. Met de implementatie van Business Central zijn een aantal eerder gerapporteerde tekortkomingen opgevolgd. Ten aanzien van de processen rondom het inkoopproces, financiële verslaggevingsproces en IT hebben wij nog beperkte aanbevelingen, waarmee het proces nog verder geoptimaliseerd kan worden. Voor een nadere toelichting per proces verwijzen wij naar de volgende paragrafen.

IT-audit algemeen

In het kader van de jaarrekeningcontrole is een IT-audit uitgevoerd. De IT-audit is primair gericht op de betrouwbaarheid van de gegevensverwerking ten behoeve van de totstandkoming van de jaarrekening. Dit betekent dat de IT-audit zich niet primair richt op het doen van uitspraken omtrent de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking als geheel of van onderdelen daarvan.

Het inzicht in de gebruikte IT-applicaties en ondersteunende IT-infrastructuur, vormen een onderdeel van het inzicht in de interne beheersing. Algemene IT-beheersingsmaatregelen (hierna: IT General Controls) rond de IT-processen leveren een belangrijke bijdrage aan het mitigeren van de risico's die voortkomen uit het gebruik van IT.

De bevindingen zoals gerapporteerd in deze management letter zijn gericht geweest op het beoordelen van de opzet en het vaststellen van het bestaan van IT General Controls voor zover relevant voor de jaarrekeningcontrole. De impact van de bevindingen met betrekking tot de IT General Controls zal bij de betreffende processen worden behandeld.

De organisatie heeft op het gebied van IT stappen gezet in 2025. De implementatie naar Business Central en de implementatie van MFA in AIMS zorgt ervoor de dat ITGC’s zijn verbeterd. De organisatie gaat actief aan de slag met de aanbevelingen op het gebied van IT. Een aandachtspunt hierbij is de vastlegging van de uitgevoerde procedures. Deze worden verder toegelicht in hoofdstuk 2.4.

2.3 Overzicht van onze bevindingen t.a.v. de processen

Subsidieproces

Proces

Het proces rondom het aanvragen en toekennen van subsidies is in opzet sterk. Of de aanvraag in behandeling genomen kan worden wordt gecontroleerd middels de checklist ‘toetsen aanvraag’. Middels de checklist ‘beoordelingsformulier’ worden relevante punten uit de regelingen getoetst, waardoor de rechtmatigheid van de aanvraag in voldoende mate gewaarborgd wordt. Tot slot vindt er nog een inhoudelijke beoordeling plaats door het subsidiebureau of de adviescommissie. Dit leidt tot een bureauvoorstel met daarin de scores per aanvraagronde. Deze wordt gecontroleerd en in AIMS geautoriseerd door meerdere functionarissen. Bij de subsidievaststelling volgt Fonds Podiumkunsten het Uniform Subsidiekader (USK). De verantwoording wordt beoordeeld in de checklist ‘vaststelling’ die voor iedere subsidie wordt ingevuld. Hierin wordt vastgelegd of de verkregen verantwoording voldoet aan de gestelde eisen. Wij hebben tijdens de interim-controle de werking van deze beheersingsmaatregelen vastgesteld.

OVERZICHT EN EVALUATIE VAN INTERNE BEHEERSMAATREGELEN			
Beheersmaatregelen in het proces	**2025**	**2024**	**Impact IT**
• Functiescheiding tussen medewerkers die betrokken zijn bij verdeling subsidiegelden	🙂	🙂	✓
• Functiescheiding tussen opboeking financiële verplichting en medewerkers die betrokken zijn bij verdeling subsidiegelden	🙂	🙂	–
• Controle op subsidievoorwaarden	🙂	🙂	–

Conclusie
We kunnen steunen op de interne beheersingsmaatregelen in het proces. Dit leidt tot een combinatie van systeem- en gegevensgerichte aanpak.

2.3 Overzicht van onze bevindingen t.a.v. de processen

Inkoop- en betaalproces

Proces

Binnen het inkoopproces bestaat in opzet voldoende functiescheiding tussen het registreren van inkoopfacturen (medewerkers FA) en het controleren en autoriseren van inkoopfacturen (controller, budgethouder, directeur/voorzitter RvB). Voor het registeren en autoriseren van inkoopfacturen en het klaarzetten van betalingen wordt gebruik gemaakt van MIcrosoft Business Central. Binnen het betaalproces bestaat voldoende functiescheiding tussen het aanmaken van betalingen (medewerkers FA), het controleren (bureaumedewerker) en autoriseren van betalingen (hoofd subsidieondersteuning). Vanaf 2025 maakt u ook gebruik van de BNG bank. Wij hebben vastgesteld dat de ingeregelde autorisaties en beheerrechten juist zijn. Ten aanzien van de rechten in de ABN Amro en het wijizgen van crediteurenstamgegevens hebben wij enkele bevindingen.

Bevindingen

Binnen het betaalproces hebben wij enkele bevindingen geconstateerd. Dit ziet toe op de controle op de bankrekeningnummers en de iDeal betaalrekeningen. Voor de subsidiegerelateerde uitgaande betalingen wordt gebruikgemaakt van Surepay om het bankrekeningnummer van de aanvrager te verifiëren. Dit is een toereikende stap in de controle om eventuele fraude te voorkomen en het bankrekeningnummer van de aanvrager te controleren. Voor de reguliere inkoopfacturen is er sprake van een toereikende factuurautorisatie. De controle van de betaalbatches vindt steekproefsgewijs plaats aan de hand van de achterliggende factuur. Wij bevelen u aan om ook de crediteur na te bellen bij het aanmaken/wijzigen van bankrekeningnummers. Daarnaast hebben wij vastgesteld dat twee medewerkers gemachtigd zijn om iDEAL-betalingen uit te voeren. Aangezien het maximale overboekingsbedrag is beperkt tot €1.000, achten wij het risico beperkt.

Ten aanzien van de crediteurenstamgegevens hebben wij vastgesteld dat nagenoeg alle medewerkers die toegang hebben tot Business Central de rechten hebben om crediteurenstamgegevens te wijzigen. Wij bevelen u aan om deze rechten enkel toe te kennen aan medewerkers die niet betrokken zijn bij het proces rondom factuurautorisatie en het betaalproces. Wij hebben ook inzicht verkregen in de ingeregelde autorisatieflows in Business Central. Hieruit blijkt in een van de autorisatieflows enkel autorisatie nodig is van de junior controller. Aangezien deze medewerker ook crediteurenstamgegevens kan wijzigen ontstaat hierdoor mogelijk een risico op onrechtmatige wijzigingen in de crediteurenstamgegevens en betalingen. Wij hebben echter vastgesteld dat er tot en met heden alle facturen door twee of meer medewerkers zijn geautoriseerd. Hiermee hebben we vastgesteld dat dit risico zich niet heeft voorgedaan. Wij bevelen u echter wel aan goed te kijken naar de inrichting van de autorisatieflows en ervoor te zorgen dat minimaal twee medewerkers hierbij betrokken zijn.

2.3 Overzicht van onze bevindingen t.a.v. de processen

Inkoop- en betaalproces

OVERZICHT EN EVALUATIE VAN INTERNE BEHEERSMAATREGELEN			
Beheersmaatregelen in het proces	**2025**	**2024**	**Impact IT**
• Functiescheiding tussen het registreren en autoriseren van facturen			✓
• Functiescheiding tussen de beheerrechten BC en gebruikers die facturen autoriseren			✓
• Toereikende controle op de juistheid van de kosten			–
• Toereikende controle op mutaties crediteurenstamgegevens			–
• Functiescheiding tussen het klaarzetten, controleren en autoriseren van betalingen			✓
• Functiescheiding tussen de beheerrechten en de gebruikersorganisatie binnen de bankapplicatie			✓

Conclusie
We kunnen deels steunen op de interne beheersingsmaatregelen in het proces. Dit leidt tot mix van systeem- en gegevensgerichte aanpak.

2.3 Overzicht van onze bevindingen t.a.v. de processen

Personeelsproces

Proces

Er is voldoende functiescheiding binnen het proces van aanname en ontslag van personeel waarbij de beschikkende (directeur), registrerende (medewerker FA) en controlerende (juridisch medewerker en controller) handelingen zijn belegd bij verschillende functionarissen. Tevens bestaat voldoende functiescheiding tussen het doorgeven van salarismutaties (medewerker PZ), het invoeren van de mutaties (medewerker FA), het controleren van de verwerking van de mutaties (medewerker PZ/controller) en de salarisbetaling (hoofd subsidieondersteuning). Wij hebben de salarisadministratie niet meegenomen in de scope van onze werkzaamheden, omdat een gegevensgerichte controle efficiënter is. Een onjuiste salarismutatie als gevolg van ontoereikende ITGC's in de salarisadministratie zal ondervangen worden door de maandelijkse zichtbare controle op het standenregister.

OVERZICHT EN EVALUATIE VAN INTERNE BEHEERSMAATREGELEN			
Beheersmaatregelen in het proces	**2025**	**2024**	**Impact IT**
• Functiescheiding tussen aanname en registratie nieuw personeel	🙂	🙂	—
• Functiescheiding tussen het doorgeven en het invoeren van salarismutaties.	🙂	🙂	—
• Maandelijkse zichtbare controle op het standenregister	🙂	🙂	—
• Functiescheiding tussen het klaarzetten, controleren en autoriseren van betalingen	🙂	🙂	✓

Conclusie

We kunnen steunen op de interne beheersingsmaatregelen in het proces. Vanwege efficiencyoverwegingen zullen wij echter een gegevensgerichte controle aanpak hanteren.

2.3 Overzicht van onze bevindingen t.a.v. de processen

Financiële verslaggevingsproces

Proces

Binnen het proces rondom de financiële rapportages en de jaarafsluiting bestaat in opzet voldoende functiescheiding tussen het opstellen van de begroting en het autoriseren van de begroting. Het opstellen van de tussentijdse rapportages en jaarrekening gebeurt door de junior controller. De financiële afdeling is momenteel bezig met het integreren van de controle op memoriaalboekingen in Microsoft Business Central. In afwachting van deze geautomatiseerde inrichting zijn de memoriaalboekingen over het eerste en tweede kwartaal handmatig gecontroleerd door de controller. Deze controle wordt vastgelegd in Excel. Wij bevelen u aan dit in te regelen in Microsoft Business Central. Met de integratie in Microsoft Business Central zal de workflow transparanter en beter inzichtelijk worden. De verwachting is dat deze automatisering in het derde of vierde kwartaal van 2025 gerealiseerd zal zijn. Wij hebben geen verdere leemtes gesignaleerd in de opzet van het proces die leiden tot significante risico's voor de jaarrekening. Zoals eerder aangegeven blijft het risico op management override als theoretisch risico wel bestaan.

OVERZICHT EN EVALUATIE VAN INTERNE BEHEERSMAATREGELEN			
Beheersmaatregelen in het proces	**2025**	**2024**	**Impact IT**
• Functiescheiding tussen opstellen begroting en goedkeuren van de begroting	🙂	🙂	—
• Functiescheiding tussen de aanmaken van memoriaalboekingen en controleren van memoriaalboekingen	🙂	😐	—

Conclusie

We kunnen steunen op de interne beheersingsmaatregelen in het proces. Vanwege efficiencyoverwegingen zullen wij echter een gegevensgerichte controle aanpak hanteren.

2.4 Overzicht van onze bevindingen t.a.v. de IT General Controls

Bevindingen IT General Controls

Hierna zijn de bevindingen opgenomen met betrekking tot de opzet en het bestaan van de door ons in het kader van de jaarrekeningcontrole onderzochte IT General Controls. Per bevinding is de status in het huidige jaar en in het voorgaande jaar aangegeven met betrekking tot de onderzochte IT-applicaties, zijnde Dynamics Business Central en Aims, en de hieraan gerelateerde IT-infrastructuur voor zover relevant voor de jaarrekeningcontrole. Onze relevante bevindingen en overige IT-gerelateerde bevindingen treft u op de volgende pagina's aan.

De scope van relevante IT General Controls wordt jaarlijks beoordeeld en kan hierdoor afwijken van de scope van voorgaande jaren.

Geautomatiseerde gegevensverwerking

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

Wij hebben de automatiseringsorganisatie uitsluitend in het kader van de jaarrekeningcontrole beoordeeld. De interim-controle heeft meerdere tekortkomingen in de continuïteit en betrouwbaarheid van de geautomatiseerde gegevensverwerking aan het licht gebracht. Voor een verdere uitwerking van de bevindingen over de continuïteit en betrouwbaarheid van de geautomatiseerde gegevensverwerking verwijzen wij naar de volgende pagina's.

2.4 Overzicht van onze bevindingen t.a.v. de IT General Controls

1/2 - Per applicatie

OVERZICHT EN EVALUATIE VAN ITCG - PER APPLICATIE	Aims		Business Central	
Logische toegangsbeveiliging	**2025**	**2024**	**2025***	**2024**
LT.1 - Procedure autorisatiebeheer	😒	😒	—**	N/A
LT.2 - Periodieke controle op toegang en juistheid ingerichte autorisaties	🙂	🙂	—**	N/A
LT.3 - Identificatie van gebruikers voor toegang tot applicaties	🙂	🙂	🙂	N/A
LT.4 - Authenticatie	🙂	😒	🙂	N/A
LT.5 - Administrator- en superuser-accounts	🙂****	🙂	🙂	N/A
Wijzigingsbeheer				
CM.1 - Wijzigingsbeheer applicaties	🙂	🙂	🙂	N/A
CM.2 - Gescheiden IT-omgevingen	🙂	🙂	🙂	N/A
Continuïteit				
CON.1 - Back-up maatregelen	🙂	🙂	🙂	N/A
CON.2 - Restoretests	—***	😒	🙂	N/A

* Business Central is sinds 2025 in gebruik genomen en derhalve is deze applicatie in 2025 voor de eerste keer getoetst, binnen de controle.
** Voor het proces rondom autorisatiebeheer geldt, dat er vanwege de recente livegang van Business Central, nog geen mutaties zijn doorgevoerd in de gebruikers en derhalve het proces voor het toekennen en intrekken van rechten zich nog niet heeft voorgedaan. Derhalve hebben wij dit proces niet kunnen waarnemen.
*** In 2025 heeft er een migratie plaatsgevonden. Uit de data voor de migratie en de data na de migratie blijkt dat deze succesvol is geweest. De controle op deze migratie is echter niet zichtbaar vastgelegd, derhalve hebben wij deze niet kunnen waarnemen.
**** Onze bevindingen zijn na de bespreking van de managementletter opgevolgd.

De impact van deze bevindingen ten aanzien van de applicaties op de processen zijn meegenomen in hoofdstuk 2.3.

— Geen waarneming **N/A** Niet van toepassing ☹ Proces ontoereikend 😒 Proces enigszins ontoereikend 🙂 Proces enigszins toereikend ☺ Proces toereikend

2.4 Overzicht van onze bevindingen t.a.v. de IT General Controls

2/2 – Per applicatie

BEVINDINGEN			
Prioriteit	**Bevinding - incl. risico**	**Aanbeveling**	**Reactie management**
LT.1 - Procedure autorisatiebeheer (Indiensttreding) (Aims)			
Midden	Voor het proces rondom het toekennen van rechten wordt een generiek proces gevolgd voor alle applicaties in scope. Er vindt minimale vastlegging plaats van dit proces, middels een ticket, waardoor wij de juistheid van toe te kennen rechten niet kunnen vaststellen aan de hand van de aanvraag. Daarnaast ontbreekt een overzicht uit Aims, op basis waarvan is vast te stellen of de juiste rechten (confom de aanvraag) zijn toegekend. Als gevolg van de tekortkomingen met betrekking tot autorisatiebeheer bestaat het risico dat de toekenning van rechten niet in lijn is met de organisatorische rollen en functies van medewerkers waarmee zij beschikking kunnen krijgen over ruimere autorisaties dan noodzakelijk voor uitoefening van hun functie, dan wel beoogde functiescheiding kunnen doorbreken.	Wij adviseren om gebruik te maken van een formulier voor het toekennen, wijzigen en intrekken van autorisaties. Hierbij dient minimaal de functie en de afdeling van de nieuwe medewerker, en de goedkeuring door een geautoriseerd persoon te worden vastgelegd.	Wanneer een medewerker een functie krijgt waarbij toegang tot AIMS noodzakelijk is, wordt vanuit de ICT-afdeling of de leidinggevende een TOPdesk-ticket aangemaakt. Op basis van deze aanvraag wordt de betreffende gebruiker in AIMS gekoppeld aan de juiste rol(len) via de beheerinterface. Dit is zichtbaar in het tabblad "Assignments", waarin per rol exact staat weergegeven welke personen eraan gekoppeld zijn.

2.4 Overzicht van onze bevindingen t.a.v. de IT General Controls

2/2 – Per applicatie

BEVINDINGEN			
Prioriteit	**Bevinding - incl. risico**	**Aanbeveling**	**Reactie management**
LT.2 - Periodieke controle op toegang en juistheid ingerichte autorisaties (Aims en Business Central)			
Midden	Wij hebben vastgesteld dat een periodieke review voor de applicatie Aims is uitgevoerd. Hierbij is alleen een controle uitgevoerd op de actualiteit van gebruikers in de applicatie Aims. Er is geen review uitgevoerd op de juistheid van (de toekenning van) autorisaties in de applicatie Aims. Voor Business Central hebben wij vernomen dat vanwege de recente livegang en het beperkte aantal gebruikers in de applicatie, geen review op toegekende autorisaties is uitgevoerd. Het risico bestaat dat toegekende autorisaties binnen de geautomatiseerde gegevensverwerkende systemen niet in lijn liggen met de eisen die het management aan functiescheiding stelt. Hierdoor kunnen medewerkers (mogelijk) over toegangsrechten beschikken, waartoe zij uit hoofde van hun functie geen toegang toe zouden moeten hebben. Hierdoor bestaat het risico dat medewerkers ongeautoriseerde handelingen in systemen verrichten, door het (onbewust) toekennen van te ruime rechten of het cumuleren van rechten na verloop van tijd.	Wij adviseren Fonds Podiumkunsten om de periodieke controle op de actualiteit van de gebruikers uit te breiden met een controle op de juistheid van de aan de toegekende autorisaties.	Er is een periodieke review uitgevoerd, waarbij de actuele lijst van gebruikers in AIMS is gecontroleerd op juistheid en volledigheid. Rollen zijn gebaseerd op functieprofielen en bevatten enkel de toegangsrechten die nodig zijn voor die functie (least privilege-principe). De reden dat in de review geen aparte analyse is gedaan van de juistheid van de toegekende autorisaties per gebruiker, is dat het autorisatieontwerp in AIMS functiebepaald en statisch is. Een gebruiker kan slechts één rol hebben, en deze rol bevat uitsluitend de rechten die passen bij de functie. Dit betekent dat bij de review van actieve gebruikers indirect ook de autorisaties worden gevalideerd, omdat: De roltoewijzing is direct gekoppeld aan het functieprofiel. Afwijkende of te ruime rechten niet zelfstandig door de gebruiker of beheerder kunnen worden toegevoegd buiten het formele proces om. Wij erkennen dat een aanvullende check op “juistheid van roltoewijzing” explicieter kan worden uitgevoerd en vastgelegd in de reviewdocumentatie. Indien mogelijk wordt hiervoor vanaf de volgende reviewperiode een kolom toegevoegd waarin expliciet wordt bevestigd dat de huidige rol per gebruiker nog in lijn is met de actuele functie.

2.4 Overzicht van onze bevindingen t.a.v. de IT General Controls

2/2 – Per applicatie

BEVINDINGEN			
Prioriteit	**Bevinding - incl. risico**	**Aanbeveling**	**Reactie management**
LT.5 - Administrator- en superuser-accounts (Aims)			
Hoog	Wij hebben op basis van inzichten in de gebruikersgroepen in Aims vastgesteld dat gebruikers met een rol binnen de gebruikersorganisatie over verhoogde rechten beschikken. Als gevolg hiervan is op 16 september 2025 een verzoek gedaan om deze gebruikergroep te legen.	Wij adviseren Fonds Podiumkunsten het gebruik van verhoogde rechten alleen beschikbaar te stellen voor gebruikers die deze rechten uit hoofde van hun functie nodig hebben en geen onderdeel zijn van de lijnorganisatie. In lijn hiermee adviseren wij om toedeling van hoge bevoegdheden onderdeel te maken van autorisatiesmatrices en periodiek te controleren op juiste toekenning.	Wij hebben de betreffende medewerkers laten verwijderen uit de functiegroep administrator. Ook zijn de betreffende medewerkers uit de functiegroep superuser gezet. Die laatste functiegroep was bedoeld als lichte administrator rechten in de tussenfase waarin er nog maar 1 applicatiebeheerder was. Dat is nu niet meer aan de orde, dus deze groep met rechten is overbodig.

2.4 Overzicht van onze bevindingen t.a.v. de IT General Controls

2/2 – Per applicatie

BEVINDINGEN			
Prioriteit	**Bevinding - incl. risico**	**Aanbeveling**	**Reactie management**
CON.2 - Restoretests (Aims)			
Midden	Voor Aims hebben wij begrepen dat er gedurende boekjaar 2025 een restoretest is uitgevoerd, als onderdeel van de migratie naar de Cloud, door de lokale omgeving in de Cloud omgeving te importeren. Deze overgang is door de organisatie als akkoord bevonden. Echter hebben wij niet kunnen vaststellen dat er een controle is uitgevoerd op de volledigheid en juistheid van de data die is overgezet en daarmee het succesvolle verloop van deze restore, omdat onderliggende vastlegging ontbreekt.	Wij adviseren Fonds Podiumkunsten om voor Aims minimaal jaarlijks een full restore- (en failover)test in te richten waarmee de geautomatiseerde gegevensverwerking in het geval van een calamiteit binnen de gestelde downtime en met een aanvaardbare hoeveelheid gegevensverlies hervat kan worden. Resultaat van uitvoering en evaluatie ten aanzien van RTO/RPO-vereisten dient te worden gedocumenteerd en indien mogelijk buiten de IT-omgeving te worden bewaard. Daarnaast adviseren wij om bij het uitvoeren van een restoretest, de uitgevoerde stappen, resultaten en het verloop hiervan vast te leggen.	Op dit moment is er nog geen periodieke full restore- of failover-test ingericht voor de gehoste AIMS-omgeving bij Quest, maar dit is wel voorzien. In het document NFPK-QSS135849-Upgrade_to_AIMS_500-Hosted-v0.1 is vastgelegd dat het Disaster Recovery Plan (DRP) zal worden uitgebreid met formele RTO- en RPO-vereisten. De inrichting, uitvoering en documentatie van deze testen staat gepland voor begin 2026, in samenwerking met Quest. Hiermee wordt het continuïteitsbeheer structureel geborgd en voldoen we aan de aanbevelingen. Historisch (in de on-premises omgeving) zijn restore-tests reeds uitgevoerd en succesvol afgerond, zoals vastgelegd in het runbook van de AIMS 5.0 migratie.

2.4 Overzicht van onze bevindingen t.a.v. de IT General Controls

Operating system (Entra ID)

OVERZICHT EN EVALUATIE VAN ITGC		
Beheersmaatregelen in het proces	**2025**	**2024**
OS.2 - Authenticatie	☺	☺
OS.3 - Toegang met hoge privileges	☺	☺