

Pagina 1/2

steller

J. Melissant / L. van Kesteren

Leiden
24 april 2025

onderwerp

- Oplegnotitie ISAE3402 type II Assurance rapportage 2024

Inleiding

De BSGR heeft AuditNexus auditing (voorheen: Audit Connect) voor het tweede jaar opdracht gegeven om te rapporteren over het systeem van interne beheersingsmaatregelen met betrekking tot de geleverde diensten (Sectie 3) voor het verwerken van transacties van deelnemers, gedurende de verslagperiode van 1 januari 2024 tot en met 31 december 2024.

De beheersingsmaatregelen zijn opgenomen in een beheersingsraamwerk. Jaarlijks vindt er een evaluatie plaats op dit beheersingsraamwerk. De evaluatie in 2024 heeft onder andere geleid tot een aantal tekstuele aanscherpingen in bestaande beheersingsmaatregelen. Tevens zijn er een klein aantal beheersingsmaatregelen toegevoegd in het beheersingsraamwerk of samengevoegd in andere beheersingsmaatregelen.

Op basis van de uitgevoerde audit heeft AuditNexus een ISAE3402 verklaring afgegeven slechts met één enkele beperking. Deze beperking is gebaseerd op het niet effectief werken van beheersingsmaatregelen rondom informatiesystemen op het gebied van een back-up systeem, waarover de leverancier conform de doelstelling periodiek dient te rapporteren.

De bevinding luidt als volgt:

Ref	Sub proces	Beheersmaatregel	Uitzondering
ITGC-Continuity		BSGR heeft binnen het proces van waarborging van de continuïteit van de door BSGR gebruikte informatiesystemen en de daarbinnen als kritisch aangemerkte applicaties en data, een goed uitgewerkt en betrouwbaar back-up systeem ingericht. BSGR maakt in dit verband gebruik van de diensten en faciliteiten van de IT provider.	
7.02	ITGC-Continuity	Per kwartaal rapporteert KPN over de realisatie van de genomen maatregelen rondom back-ups, beschikbaarheid en incidenten. De ICT-coördinator beoordeelt deze rapportage en geeft er indien noodzakelijk opvolging aan.	KPN rapporteert niet over de realisatie t.a.v. de genomen maatregelen rondom back-ups en beschikbaarheid. De beoordeling van de service level rapportage door de ICT coördinator is niet aantoonbaar gemaakt.

Naar aanleiding van bovenstaande bevinding zal de BSGR met de betreffende leverancier aanvullende afspraken maken om de betreffende informatie tijdig, juist en volledig te ontvangen.

Ontwikkeling 2024 ten opzichte van 2023

De algemene conclusie vanuit de BSGR over het jaar 2023 was dat de migratie naar KPN uitdagend was, maar dat in het kader van risicobeheersing geen additionele risico's naar voren zijn gekomen. Tevens was dit het eerste jaar van de IT-auditor.

Op basis van de door Audit Connect uitgevoerde werkzaamheden zijn zij in 2023 tot een oordeel met beperking gekomen. De basis van de beperking is voortgekomen uit de conclusie dat een aantal beheersmaatregelen in 2023 volgens Audit Connect niet effectief hebben gewerkt. Deze bevindingen richten zich met name op de IT omgeving.

Naar aanleiding van deze bevindingen heeft de BSGR een aantal actiepunten geformuleerd die in 2024 zijn opgepakt en uitgevoerd. Dit heeft uiteindelijk geleid tot een significante verbetering in de ISAE3402 rapportage over 2024, waarin uiteindelijk slechts één beperking is opgenomen. Dit is een significante verbetering ten opzichte van de rapportage over 2023 waarin 11 beperkingen waren opgenomen.

Eind januari 2025 is de BSGR, ondersteund door een extern bureau, een onderzoek gestart naar een fraudegeval. In de jaarrekening 2024 is hierop een nadere toelichting gegeven. Door BSGR is hiervan aangifte gedaan bij de politie. De omvang van dit fraudegeval bedraagt circa € 70K en is grotendeels al teruggestort naar de BSGR.

Naar aanleiding van dit voorval zullen door de BSGR in 2025 op zowel organisatorisch als op procedureel vlak aanpassingen worden doorgevoerd in de beheeromgeving, en worden vastgelegd in beheersmaatregelen in zowel de ISAE als de VIC, om zodoende het risico op herhaling zoveel mogelijk te beperken voor de toekomst. Er is geen sprake van een continuïteitsrisico. Alle beheersmaatregelen in de ISAE hebben naar behoren gefunctioneerd. De geconstateerde fraude kan naar zijn aard echter nimmer geheel door beheersmaatregelen worden ondervangen. Als aanvullende beheersmaatregelen in de ISAE gaan de gedachten uit naar een intensivering van de kascontrole en het oninbaar verklaren van alle vorderingen op basis van het meer-ogenprincipe. Daarnaast wordt nog nagedacht over het versturen van een brief naar de debiteur van wie de vordering(en) oninbaar word(en)t verklaard. Bezien wordt nog in hoeverre dit past binnen de wet- en regelgeving.

Advies

Het Algemeen bestuur wordt gevraagd:

- In te stemmen met de rapportage ISAE 3402 type II.

Besluit

Besloten conform advies	
De voorzitter	
De secretaris	