Beoordeling van assurance-rapporten zoals de 3402-verklaring

Inleiding
Als zorgaanbieder maak je gebruik van software in de vorm van een EPD/ZIS en ondersteunende tooling zoals daily auditing tools van bijvoorbeeld ValueCare of Notiz. Als je wilt steunen op de diensten van deze aanbieders, door de tooling op te nemen in het control framework als zorgaanbieder, heb je vaak een assurance-rapport zoals een 3402-verklaring nodig. Met zo'n assurance-rapport verkrijg je als zorgaanbieder en zorgverzekeraar zekerheid dat de software betrouwbaar heeft gewerkt/is ingericht.

De softwareleverancier (hieronder service organisatie genoemd) maakt zelf afspraken met een accountant of EDP-auditor over een dergelijke assurance-opdracht en de wijze van rapportage. Als zorgaanbieder wil je wel weten of de werkzaamheden die door de accountant of EDP-auditor worden uitgevoerd alle relevante risico's afdekken. Dit betekent dat je als zorgaanbieder ook werkzaamheden zal moeten verrichten ter beoordeling van een dergelijke assurance-rapportage. Zowel bij de start van een kalenderjaar (vaststellen werkzaamheden accountant/EDP auditor) als na het afgeven van de assurance-rapportage. De belangrijkste onderdelen van deze werkzaamheden worden hieronder toegelicht.

Daarnaast is het belangrijk om te weten dat het assurance-rapport niet alle risico's afdekt. Een voorbeeld is dat een zorgaanbieder doorgaans zelf verantwoordelijk is voor het aanleveren van de codes van haar klinische afdelingen aan de softwareleverancier, voor de data-analyse op de verpleegdagen. Het assurance-rapport doet dan geen uitspraken over de juistheid en volledigheid van de door de zorgaanbieder aangeleverde afdelingscodes, waarin de data-analyse mee gewerkt wordt.

Assurance-rapport
Ondanks de uitbesteding blijft de zorgaanbieder verantwoordelijk voor de processen die worden uitgevoerd door de service organisatie. Om te kunnen steunen op de diensten, processen en beheersing van de service organisaties, kan zekerheid worden verkregen via een assurance-rapport. Een assurance-rapport zal, zoals aangegeven wel eerst beoordeeld moeten worden op bruikbaarheid voor het afdekken van de risico's in het eigen control framework van de zorgaanbieder. In deze bijlage wordt nader ingegaan op enkele onderwerpen die bij deze beoordeling van belang zijn en tracht daarmee een handvat te bieden aan zorgaanbieders.

Te beoordelen aspecten
Om te bepalen of het assurance-rapport geschikt is om zekerheid te bieden over de diensten van de service organisatie, en daarmee de beheersing die wordt uitgevoerd door de service organisatie t.b.v. het eigen control framework, zijn de volgende thema's van belang:

1. Geschiktheid auditor
2. Geschiktheid type assurance-rapport
3. Scope van het assurance-rapport
4. Toereikendheid periode assurance-rapport
5. Uitgevoerde controlewerkzaamheden
6. Oordeel en bevindingen in het assurance-rapport
7. Voldoen aan 'end-user considerations' door de gebruiker van de dienst (de zorgaanbieder)

Hieronder wordt nader ingegaan op deze aspecten.

1. *Geschiktheid auditor*
   In hoeverre is de auditor van de service organisatie deskundig en onafhankelijk van de service organisatie? Deskundigheid zal veelal blijken uit een RA of RE titel. Voor de onafhankelijkheid is het onder andere van belang dat de auditor niet werkzaam is voor de service organisatie, maar bijvoorbeeld bij een accountantskantoor.

2. *Geschiktheid type assurance-rapport*
   Er zijn verschillende standaarden die gebruikt kunnen worden voor een assurance-rapport, voorbeelden zijn de COS3000 en de ISAE3402. In die standaarden wordt onderscheid gemaakt tussen type 1 en type 2 rapporten. Type 1 geeft een oordeel (met een redelijke mate van zekerheid) over opzet en bestaan van de beschreven beheersmaatregelen op een bepaald moment. Type 2 geeft een oordeel (met een redelijke mate van zekerheid) over opzet, bestaan én werking over een bepaalde periode. Wil het assurance-rapport bruikbaar zijn voor de zorgaanbieder, dan zal het rapport zowel opzet, bestaan als werking van de beheersmaatregelen van de service organisatie moeten bevatten.

3. *Scope van het assurance-rapport*
   Omvat de scope van het assurance-rapport de uitbestede beheersmaatregelen/het uitbestede deel van de beheersing uit het control framework van de zorgaanbieder? Van belang is hierbij om te beoordelen of de te verwachten beheersmaatregelen van de service organisatie, gezien de aard van de organisatie en het type dienst, aanwezig zijn in het beoordeelde control framework van de service organisatie. Zo

zal bij een softwareleverancier de verwachting zijn dat o.a. beheersmaatregelen aanwezig zijn op het gebied van het ontwikkelen, testen, accepteren en in productie brengen van software.

Een service organisatie is vrij om te bepalen welke processen en beheersmaatregelen zij opneemt in het assurance-rapport. Daarom is de kans aanwezig dat deze niet overeenkomen met de scope die de zorgaanbieder nodig heeft om de beheersdoelstellingen in het eigen control framework te behalen. Het is dus belangrijk als zorgaanbieder vooraf betrokken te zijn bij het vaststellen van de scope van het assurance-rapport van de service organisatie.

4. *Toereikendheid periode assurance-rapport*
   Het is van belang om vast te stellen dat het assurance-rapport betrekking heeft op dezelfde periode als waarover voor het eigen control framework van de zorgaanbieder werking dient te worden aangetoond.

5. *Uitgevoerde controlewerkzaamhedenwerkzaamheden*
   In het assurance-rapport dient bij het control framework van de service organisatie te zijn opgenomen welke controlewerkzaamheden door de auditor van de service organisatie zijn uitgevoerd. Geeft de informatie voldoende inzicht om een uitspraak te doen over de opzet, bestaan en werking van de beheersmaatregel?

6. *Oordeel en bevindingen in het assurance-rapport*
   Het assurance-rapport van de service organisatie kan bevindingen bevatten t.a.v. opzet, bestaan en/of werking van de door de service organisatie gepresenteerde beheersmaatregelen. Bevindingen worden opgenomen bij het normenkader in het assurance-rapport en door de auditor is een impactanalyse uitgevoerd in hoeverre de bevindingen al dan niet leiden tot een assuranceverklaring met beperking. De zorgaanbieder analyseert de impact van deze bevindingen op de beheersmaatregelen en – doelstellingen in het eigen control framework. Zijn er mogelijk mitigerende maatregelen te onderkennen in het framework van de service organisatie? Wat geeft deze hierover zelf aan in een eventuele managementreactie?

7. *Voldoen aan 'end-user considerations' door de gebruiker van de dienst (de zorgaanbieder)*
   Veelal worden in een assurance-rapport aanvullende interne beheersmaatregelen benoemd die de zorgaanbieder zelf moet uitvoeren om de interne beheersdoelstellingen van de service organisatie te behalen, de zogenaamde 'end-user considerations'. Bepaalde aspecten die samenhangen met de kwaliteit van de diensten van de service organisatie kunnen immers alleen door de afnemer van de diensten zelf geborgd worden. Voorbeelden hiervan zijn het testen van wijzigingen in software binnen de eigen omgeving van de gebruikersorganisatie. De zorgaanbieder moet beoordelen of aan deze voorwaarden, zoals genoemd in het rapport, ten aanzien van het zelf uitvoeren van bepaalde beheersmaatregelen is voldaan.

Impactanalyse
Uit de beoordeling van het assurance-rapport van de service organisatie kan blijken dat niet op alle aspecten voldoende zekerheid kan worden verkregen. Zo kan het bijvoorbeeld zijn dat de periode van het assurance-rapport niet de gehele periode afdekt waarover zekerheid verkregen moet worden, dat essentiële onderdelen niet zijn opgenomen in de scope van het assurance-rapport of dat er een oordeel met beperking is afgegeven. In deze gevallen zal een zorgaanbieder een impactanalyse moeten uitvoeren in hoeverre dit invloed heeft op het (niet) behalen van de beheersdoelstellingen van het eigen control framework. Afhankelijk van de impact kan het zijn dat er bijvoorbeeld aanvullende werkzaamheden moeten worden verricht in de eigen organisatie of bij de service organisatie.