User control considerations voor ISAE3402-assurancerapportages

Ruimte en noodzaak voor verbetering

Drs. J.J. van Beek RE RA
is als partner werkzaam bij KPMG IT Advisory.
vanbeek.jaap@kpmg.nl

Ir. R.P.A.C. van Vught
is als senior consultant werkzaam bij KPMG IT Advisory.
vanvught.rolijn@kpmg.nl

Steeds meer organisaties en hun accountants krijgen te maken met uitbesteding. Niet enkel de uitbesteding van IT-applicaties; hele processen worden ondergebracht bij zogeheten serviceorganisaties. Hoe houden gebruikersorganisaties en hun accountants grip op deze uitbestede diensten? Het antwoord hierop is vaak door het ontvangen van een assurancerapportage over de uitbestede dienstverlening. Het assurancelandschap is echter aan het veranderen, en de focus zal daar de komende jaren verschuiven. User control considerations zullen een belangrijkere rol gaan spelen in de assurancerapportage, en gezien de huidige ontwikkelingen in de markt is er een noodzaak om organisaties bewuster te maken op het gebied van user control considerations. Dit artikel gaat in op de user control considerations en wat deze in de praktijk voor uitwerking hebben, zowel voor de serviceorganisatie, service-auditor, gebruikersorganisatie en haar accountant.

INLEIDING

Anno 2017 komen organisaties er niet meer onderuit: delen van of gehele bedrijfsprocessen worden uitbesteed aan derde partijen. De strategische keuze om een deel van de bedrijfsprocessen door een gespecialiseerde dienstverlener te laten uitvoeren is steeds meer een normaal onderdeel van de bedrijfsvoering. Het kan de uitbesteding betreffen van een applicatie of IT-helpdesk, maar ook gehele bedrijfsprocessen (bijvoorbeeld de salarisverwerking) worden uitbesteed. Het management van de uitbestedende organisatie draagt echter de verantwoordelijkheid voor het geheel met betrekking tot de financiële verslaggeving, dus ook voor de onderdelen die zijn uitbesteed. Voor uitbestedingen die een (indirect) verband hebben met de financiële verslaggeving van de uitbestedende organisatie is specifiek het ISAE3402-assurancerapport ontwikkeld, meestal aangeduid als Service Organisatie Control-rapport (SOC1-rapport). Een ISAE3402-assurancerapport is bestemd voor de uitbestedende organisatie (de gebruiker) en haar accountant.

Een belangrijk onderdeel in de assurancerapportage is de paragraaf 'user control considerations'. Deze wordt ook wel 'complementary user entity controls' of in het Nederlands 'aanvullende beheersingsmaatregelen binnen de gebruikende entiteit' genoemd in een assurancerapportage. In deze paragraaf wordt beschreven welke beheersingsmaatregelen de gebruikersorganisatie moet inrichten in haar processen om gebruik te kunnen maken van de assurancerapportage. Dit artikel zal aan de hand van de huidige constateringen van de Autoriteit Financiële Markten, de implementatie van de SSAE18-standaard in de Verenigde Staten en de richtlijnen van De Nederlandsche Bank (DNB) een toelichting geven op het wijzigende assurancerapportagelandschap. De user control considerations nemen in deze wijziging een belangrijke plaats in, want in de huidige richtlijnen is dit een vrijblijvend en weinig eenduidig onderdeel. In de praktijk zien wij organisaties eveneens worstelen met deze user control considerations. Aan de hand van een aantal praktijkvoorbeelden zal hier nader op worden ingegaan, waarna praktische handvatten en adviezen worden gegeven waar zowel serviceorganisaties en gebruikersorganisaties direct mee aan de slag kunnen.

> Het management van de uitbestedende organisatie draagt de verantwoordelijkheid voor de financiële verslaggeving

MEERWAARDE VAN EEN ISAE3402-ASSURANCERAPPORT

Het assurancerapport komt voort uit de regels voor onderlinge informatieuitwisseling tussen auditors. Een ISAE3402-assurancerapport sluit naadloos aan op de vereisten uit de COS-standaard 402: 'overwegingen met betrekking tot controles van entiteiten die gebruikmaken van een serviceorganisatie'. Deze auditstandaard geeft de accountant aan hoe te handelen in situaties waarin zijn controleklant de voor de financiële verslaggeving relevante processen heeft uitbesteed aan een serviceorganisatie ([NBA17]).

In de COS-standaard 402 wordt een aantal stappen onderscheiden voor het controleren van serviceorganisaties. Allereerst dient de accountant inzicht te verwerven in de aard en significantie van de uitbestede diensten. Vervolgens wordt bepaald wat het effect daarvan is op de interne beheersing van de gebruikersorganisatie. Als laatste dienen de risico's geïdentificeerd te worden en dient de accountant in te schatten waar afwijkingen van materieel belang kunnen zijn. Hierbij kan een ISAE3402-assurancerapport behulpzaam zijn. Aan de hand van het assurancerapport kan worden bepaald welke controleinformatie nodig is om in te spelen op de ingeschatte risico's en afwijkingen van materieel belang. Als de interne beheersingsmaatregelen van de gebruikersorganisatie effectief lijken te zijn, heeft de accountant een drietal opties met betrekking tot de uitbestede diensten:

1. het verkrijgen van een ISAE3402 type 2-assurancerapport;
2. het zelf verrichten van passende toetsingen bij de serviceorganisatie;
3. het gebruikmaken van een andere accountant of Internal Audit-afdeling om namens hemzelf toetsingen te laten verrichten.

Aangaande de eerste optie (zie figuur 1) ontvangt de accountant een ISAE3402 type 2-rapport betreffende een specifieke periode, meestal zes maanden tot een jaar. Dit rapport beschrijft de processen en de toereikendheid van de beheersingsmaatregelen, zoals deze gedurende de gedefinieerde periode zijn toegepast voor de serviceorganisatie om de beheersdoelstelling te bereiken. De service-auditor toetst de toereikendheid van de beschre-

ven beheersingmaatregelen voor het bereiken van de beheersingsdoelstelling en stelt vast dat de implementatie ervan gedurende de rapportageperiode in overeenstemming met de beschrijving is. Daarnaast wordt de effectiviteit (werking) getest door de service-auditor. Het resultaat hiervan is het ISAE3402-assurancerapport, dat via de serviceorganisatie wordt verstrekt aan de gebruikersorganisatie, die dit rapport kan delen met de gebruikersaccountant. De gebruikersaccountant kan dit assurancerapport vervolgens gebruiken bij zijn jaarrekeningcontrole, om na te gaan of er geen risico's zijn gelopen met betrekking tot afwijkingen van materieel belang bij de serviceorganisatie.

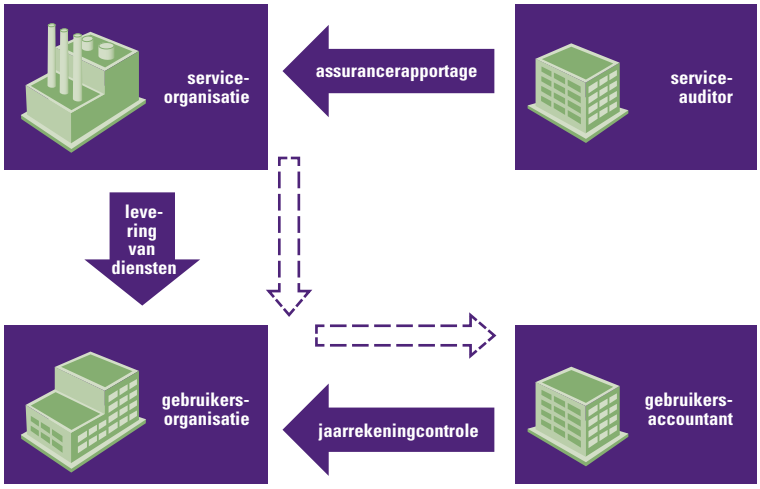
De andere twee opties zijn minder aantrekkelijk voor de serviceorganisatie. Deze opties leiden er uiteindelijk toe dat elke gebruikersorganisatie haar toetsingen laat verrichten bij de serviceorganisatie. Dit is verre van efficiënt en tijdrovend voor de serviceorganisatie. Vervolgens moet de accountant van de gebruikersorganisatie evalueren of de verkregen controleinformatie voldoende is.

Het ISAE3402-assurancerapport geeft invulling aan de onbekendheid van het controleraamwerk van de serviceorganisatie, die ontstaan is doordat de gebruikersorganisatie niet in staat is de volledigheid, juistheid en tijdigheid van de uitbestede processen te controleren. De controle kan alleen op indirecte wijze plaatsvinden, op basis van opgeleverde informatie als servicelevel- en incidentenrapportages. Een ISAE3402-assurancerapport is een prima sluitstuk voor het management van de gebruikersorganisatie en haar accountant om zekerheid te krijgen over het totaalbeeld.

In de gebruikersorganisatie kunnen zowel de eerste, tweede als derde lijn gebruikmaken van de informatie uit het assurancerapport. De servicelevelmanager (eerste lijn) kan nagaan of de diensten worden uitgevoerd conform het overeengekomen contract. De risicomanager (tweede lijn) kan een betere risicoinschatting maken van de uitbestede diensten. In het geval van een derde lijn in de gebruikersorganisatie kan de interne auditor het grotere plaatje beoordelen voor de gehele organisatie en haar uitbestedingsbeleid. Het assurancerapport wordt door de accountant van de gebruikersorganisatie gebruikt, in plaats van de eigen testwerkzaamheden voor de werking van de interne controles, die van belang zijn voor de juistheid en volledigheid van de financiële verantwoording van de uitbestedende organisatie. Op basis van het door een collega-auditor afgegeven auditorsrapport en de in het asurancerapport opgenomen resultaten van de testwerkzaamheden kan de accountant beoordelen welke aanvullende werkzaamheden nodig zijn voor de controle van de jaarrekening van zijn opdrachtgever: de uitbestedende organisatie.

De accountant van de gebruikersorganisatie kan controleren of er wordt voldaan aan alle user control considerations

Figuur 1. Four-corner-model van ISAE3402-assurancerapportages.



Een belangrijk onderdeel in de assurancerapportage is de paragraaf 'user control considerations'/'complementary user entity controls', of in het Nederlands 'aanvullende beheersingsmaatregelen binnen de gebruikende entiteit'. Deze paragraaf bevat de beheersingsmaatregelen die de gebruikersorganisatie zelf moet inbedden in haar eigen processen om gebruik te kunnen maken van het ISAE3402-assurancerapport. De accountant van de gebruikersorganisatie kan controleren of deze voldoet aan alle user control considerations. Dit zijn bijvoorbeeld controles vanuit de gebruikersorganisatie of de gegevens juist, tijdig en volledig worden aangeleverd aan de serviceorganisatie, of dat transacties geautoriseerd worden door de gebruikersorganisatie, alvorens deze worden aangeleverd bij de serviceorganisatie. Vanuit de gedachte dat er sprake is van een procesketen, waarvan een gedeelte is uitbesteed, moeten de user controls van de gebruikersorganisatie en de controls in het assurancerapport van de serviceorganisatie naadloos op elkaar aansluiten. In de praktijk blijken veel gebruikers en accountants zich niet volledig bewust van de samenhang tussen beide elementen en de eigen verantwoordelijkheid daarin. Door de huidige constateringen van de Autoriteit Financiële Markten (AFM), de implementatie van de SSAE18-standaard in de Verenigde Staten en de richtlijnen van De Nederlandsche Bank (DNB) zullen de user control considerations de komende jaren een prominentere rol innemen in de assurancerapportage.

Toezichthouder AFM

In Nederland houdt de Autoriteit Financiële Markten toezicht op de accountantsorganisaties, met als doel de kwaliteit van de wettelijke controles te verhogen en duurzaam te waarborgen. In het rapport van 25 september 2014 doet de AFM verslag van het reguliere onderzoek bij de Big 4-accountantsorganisaties ([AFM14]). Sinds 1 januari 2014 kan de AFM die resultaten openbaar maken. In het kader van dit artikel is gekeken in hoeverre het ISAE3402-assurancerapport voorkomt in deze rapportage. In de bevindingen over de wettelijke controles wordt een aantal keer gesproken over het gebruikmaken van ISAE 3402-assurancerapportages als onderdeel van de werkzaamheden van de accountant. Er staan weinig specfieke bevindingen in, maar wel wordt in één geval vastgesteld dat de effectieve werking van de relevante beheersingsmaatregelen onvoldoende is.

In de samenvatting van het rapport heeft de AFM ook een aantal generieke tekortkomingen opgenomen; er wordt voor de systeemgerichte werkzaamheden geconstateerd dat de meest voorkomende tekortkoming is dat de accountant met zijn werkzaamheden de effectieve werking van de interne beheersingsmaatregelen niet toereikend heeft getoetst. Opvallend is ook de bevinding dat de AFM in meerdere gevallen oordeelt dat de controlewerkzaamheden, die de externe accountant heeft aangemerkt als 'systeemgericht', in feite 'gegevensgericht' zijn. In die gevallen heeft de externe accountant namelijk niet de interne beheersingsmaatregelen getest, maar zelf een vorm van detailcontrole uitgevoerd. Je zou ook kunnen zeggen dat de AFM zichtbaar heeft gemaakt dat het principe van 'trust me, show me, prove me' ook van toepassing is op het dossier van de accountant.

Op 28 juni 2017 heeft de AFM een nieuw rapport uitgebracht aangaande het reguliere onderzoek bij de Big 4-accountantsorganisaties ([AFM17]). Deze rapportage bevat wederom weinig specifieke bevindingen met betrekking tot het ISAE3402-assurancerapport, en bevestigt daarmee het beeld uit 2014. Uiteraard is er door de accountantskantoren inmiddels veel gedaan om verbeteringen door te voeren en de negatieve bevindingen uit het onderzoek weg te nemen. In dit artikel staan wij specifiek stil bij wat dit in de praktijk betekent voor het gebruik van de ISAE3402-assurancerapportage en de user control considerations. Centraal daarin staat de rol van de accountantscontrole, maar het is ook relevant voor de gebruikersorganisaties zelf. Deze gebruiken de rapporten ook in het kader van de interne controle, en dienen dus ook de effectieve werking van de beheersingsmaatregelen zelf vast te stellen. Lang niet elke gebruikersorganisatie is zich hiervan bewust!

Implementatie van de SSAE18-standaard in de Verenigde Staten

Recent is in de Verenigde Staten de nieuwe SSAE18-standaard ingevoerd ter vervanging van de standaard SSAE16. Deze standaard is van toepasssing op alle assurancerapporten (Service Organization Control-reports; SOC1, SOC2 en SOC3), gedateerd op of na 1 mei 2017. In de publicatie van KPMG uit september 2016 worden alle aspecten behandeld van de gewijzigde standaard en de impact hiervan op de assurancerapportage ([Palm16]). Voor dit artikel is met name het stuk over complementary user entity controls relevant. De aanpassing die hierin wordt doorgevoerd benadrukt dat de complementary user entity controls alleen die controls moeten bevatten die noodzakelijk zijn om de controledoelstellingen te behalen, zoals deze beschreven zijn in de systeembeschrijving van het management. Voor de serviceorganisatie betekent dit dat zij de huidige lijst met complementary user entity controls moet beoordelen, en vervolgens de controls verwijderen die niet noodzakelijk zijn voor het bereiken van de beheersingsdoelstellingen. In de nieuwe standaard wordt benadrukt dat het niet de bedoeling is dat in het rapport een algemene lijst met verantwoordelijkheden van de gebruiker wordt beschreven.

Door deze ontwikkeling zien wij heel duidelijk dat hier de verantwoordelijkheid voor de procesketen wordt

benadrukt. Controles van de serviceorganisatie moeten in samenhang worden gezien met controles van de gebruikersorganisatie, waardoor uiteindelijk het systeem van interne controle naadloos op elkaar aansluit. Het is zelfs mogelijk de noodzakelijke gebruikerscontroles op te nemen in de controlematrix in de bijlage van het rapport; zo wordt de samenhang en procesgedachte nog meer benadrukt. De gebruiker van het rapport dient na te gaan welke user control considerations in het rapport zijn opgenomen, of deze relevant zijn, en aan te geven of er opvolging gegeven is aan de uitvoering van de controles.

Uit overleg met collega's in de Verenigde Staten is duidelijk geworden dat veel van de aanpassingen in SSAE18 ook voortkomen uit bevindingen van de PCAOB: de Amerikaanse toezichthouder. Het is daarom nuttig voor de Nederlandse praktijk om kennis te nemen van de SSAE18-standaard, en te bepalen wat deze wijzigingen voor impact kunnen hebben op de ISAE3402-standaard.

Richtlijnen van De Nederlandsche Bank

Ten derde is het in Nederland nog van belang om stil te staan bij de rol van De Nederlandsche Bank (DNB), die toezicht houdt op de financiële sector. Veel financiële instellingen hebben een deel van hun werkzaamheden uitbesteed aan serviceorganisaties, bijvoorbeeld de IT-infrastructuur. DNB vindt de beheersing van deze uitbesteding belangrijk, en heeft zodoende richtlijnen opgesteld waaraan uitbesteding zou moeten voldoen, waaronder ook de volgende aandachtspunten vallen:

- het kiezen van de uitbestedingspartij;
- het opzetten van een uitbestedingscontract;
- het inrichten van de interne organisatie en de uitbestedingsrelatie;
- het monitoren en evalueren van de uitbesteding.

De gebruikersorganisaties moeten kritisch kijken naar de geleverde prestaties en assurancerapportages van de serviceorganisaties. De meeste gebruikers kiezen daarom voor het verkrijgen van een ISAE3402-assurancerapport van de serviceorganisatie. Een ISAE3000-rapport kan echter ook bruikbaar zijn voor de gebruikersorganisatie en haar accountant, mits het voldoende processen voor de financiële verslaggeving afdekt. Uiteraard geldt dat alleen het verkrijgen van het assurancerapport niet voldoende is. Het assurancerapport dient ook te worden beoordeeld om een beeld te krijgen of er nog aanvullende interne controlemaatregelen noodzakelijk zijn. Hierbij speelt ook het aspect van de aantoonbaarheid van de uitgevoerde werkzaamheden door de gebruikersorganisatie een rol. In toenemende mate is dit ook van belang voor DNB, zoals blijkt uit het gevraagde volwassenheidsniveau op het gebied van informatiebeveiliging. Recent heeft DNB aangekondigd dat er een onderzoek komt naar de beheersing van de uitbesteding in de pensioensector, waar naar verwachting ook user control considerations nadrukkelijker aan de orde zullen komen.

ERVARINGEN VANUIT DE PRAKTIJK

In de afgelopen jaren hebben wij verscheidene ISAE3402-assurancerapportages mogen afgeven aan serviceorganisaties, maar ook als accountants van de gebruikersorganisatie de assurancerapportages mogen beoordelen in het kader van de jaarrekeningcontrole. Deze afgegeven en ontvangen assurancerapportages verschillen in omvang, zijn door verscheidene accountants opgesteld en hebben elk een unieke scoping. Door de huidige constateringen van de AFM, de implementatie van de SSAE18-standaard in de Verenigde Staten en de richtlijnen van DNB is er een verhoogd bewustzijn ontstaan voor de user control considerations in ISAE3402-assurancerapportages. Dit heeft geleid tot een analyse van de user control considerations van zowel de afgegeven als ontvangen assurancerapportages. De conclusie van deze analyse is dat er zich verschillende situaties kunnen voordoen aangaande de user control considerations. De vier meest opvallende situaties zijn de volgende:

1. Er staan geen user control considerations in de assurancerapportage;
2. De formulering van de user control considerations is onvoldoende concreet;
3. De rapportage bevat een wildgroei aan user control considerations;
4. De gebruikersorganisatie heeft onvoldoende kennis en kunde van (het interpreteren en gebruiken van) assurancerapportages.

Deze vier situaties hebben één overeenkomst, namelijk dat de accountant van de gebruikersorganisatie altijd meer werk heeft aan het beoordelen van de assurancerapportage, en daarmee de uitbestedingsrelatie. De assurancerapportage heeft als doel de werkzaamheden voor de ontvangende partij te beperken, maar in bovengenoemde situaties is dat niet het geval. Dit heeft als gevolg dat de kosten van de accountantscontrole kunnen stijgen. Om deze situaties te kunnen voorkomen, worden ze hieronder kort toegelicht.

1. Geen user control considerations

In de eerste situatie heeft de accountant van de gebruikersorganisatie in het kader van de jaarrekeningcontrole een ISAE3402-assurancerapportage ontvangen waarin geen user control considerations zijn benoemd. Een assurancerapportage zonder user control considerations is uitzonderlijk, en vergt daarom extra attentie van zowel de gebruikersorganisatie als de ontvangende accountant. Bij de uitbesteding van de salarisadminstratie zal de gebruikersorganisatie bijvoorbeeld altijd een akkoord

moeten geven voor de juistheid van de uit te keren salarissen door de serviceorganisatie. Dit is een typische user control consideration in een dergelijke uitbesteding. Als deze niet benoemd is in de assurancerapportage is het de vraag of de uit te keren salarissen juist zijn. In het geval er geen user control considerations zijn, zal er dus een naadloze aansluiting moeten zijn tussen het proces van de serviceorganisatie en de gebruikersorganisatie, waarbij er geen afhankelijkheden worden verwacht tussen de partijen.

De gebruikersorganisatie was niet op de hoogte van deze uitzonderlijke situatie, waardoor de ontvangende accountant aanvullende werkzaamheden heeft moeten verrichten. De ontvangende accountant heeft immers tot doel de juistheid en volledigheid van de financiële verslaggeving vast te stellen voor de gebruikersorganisatie, en een onderdeel daarvan is dat moet worden nagegaan of bijvoorbeeld de serviceorganisatie niet ongeautoriseerd transacties doorvoert of modificaties kan maken in de data van de klant.

Door bestudering van het uitbestedingscontract heeft de ontvangende accountant onderzocht wat de afhankelijkheden waren tussen de twee partijen. Daarnaast is ook het controleraamwerk van de gebruikersorganisatie aangesloten op de controlewerkzaamheden uit de assurancerapportage, om na te gaan of er geen 'gaten' in het proces zijn ontstaan. Op basis van de aanvullende werkzaamheden kan worden geconcludeerd dat deze werkzaamheden voldoende zijn, en daarmee dat de juistheid en volledigheid van de financiële verslaggeving geborgd is. Er kan echter ook worden geconcludeerd dat er nog extra aanvullende werkzaamheden moeten worden uitgevoerd bij de gebruikers- of serviceorganisatie, omdat er 'gaten' zijn in de procesketen. In dat geval zal de gebruikersaccountant bijvoorbeeld een bezoek brengen aan de serviceorganisatie en daar de toegangsrechten tot de specifieke applicatie beoordelen.

Uit deze situatie kan dus worden geconcludeerd dat het niet opnemen van user control considerations zorgt voor onzekerheden aangaande de verantwoordelijkheden bij de uitbestedingsrelatie en derhalve ook zorgt voor meer werk bij zowel de gebruikers- als serviceorganisatie.

2. De user control considerations zijn onvoldoende concreet

Dat zowel de serviceorganisatie en service-auditor het lastig vinden om een goede user control consideration te formuleren, wordt zichtbaar in situatie twee. In deze situatie zijn er user control considerations geformuleerd in de assurancerapportage, maar deze zijn onvoldoende concreet gemaakt. De user control considerations zijn vaag geformuleerd, meestal multi-interpretabel en er wordt in het midden gelaten wie verantwoordelijk is.

Een voorbeeld hiervan is de volgende user control consideration: 'De scope van de interne beheersingsmaatregelen in dit rapport is dusdanig vormgegeven dat rekening is gehouden met het feit dat de gebruikers zelf over interne beheersingsmaatregelen beschikken, onder andere op het gebied van de juiste, volledige en tijdige overdracht van informatie tussen serviceorganisatie ABC en ontvangende partij XYZ.' Als deze user control consideration goed wordt gelezen is het eigenlijk een soort disclaimer, waarin de serviceorganisatie aangeeft dat wanneer de interne beheersingsmaatregel niet is opgenomen in de asssurancerapportage, deze onderdeel moet zijn van de interne beheersing van de gebruikersorganisatie. Ook het gedeelte 'onder andere' in deze user control consideration geeft aan dat de gebruikersorganisatie meer controles moet hebben geregeld in haar interne processen, maar deze user control consideration maakt niet duidelijk welke controles dat betreft.

In deze situatie is het voor zowel de gebruikers als de ontvangende accountant lastig een sluitend geheel te krijgen tussen het interne raamwerk en de uitbestede dienstverlening. Er wordt immers in het midden gelaten wie verantwoordelijk is voor de 'gaten' in het proces. De aangegeven user control consideration geeft geen norm, en maakt het daarom ook moeilijk deze te controleren door de ontvangende accountant. In zulke gevallen zullen een ontvangende accountant en de gebruikersorganisatie kritische vragen moeten stellen aan de serviceorganisatie, en wellicht ook aanvullende werkzaamheden uitvoeren om ervoor te zorgen dat de procesketen volledig wordt gecontroleerd.

3. Wildgroei aan user control considerations

Ter aanvulling op de onvoldoende concrete en multi-interpretabele user control considerations is in situatie drie geconstateerd dat er ook assurancerapportages zijn waarin meer dan vijfentwintig user control considerations zijn geformuleerd door de serviceorganisatie en service-auditor. In zowel de SSAE18-standaard als ISAE3402-standaard zijn geen richtlijnen opgenomen voor het aantal beheersingsmaatregelen als user control considerations. Voor de gebruikersorganisatie kan het echter veel werk zijn alle user control considerations in haar processen op te nemen, waarna het ook arbeidsintensief is voor de gebruikersaccountant om vast te stellen of alle user control considerations zijn afgedekt door de gebruikersorganisatie.

In een specifieke situatie met betrekking tot de wildgroei aan user control considerations was een groot aantal van de beheersingsmaatregelen duidelijk geformuleerd en

ingebed in de dagelijkse processen van de gebruikersorganisatie. Er was echter ook een aantal beheersingsmaatregelen dat vaag en multi-interpretabel was omschreven en waarvan zowel de gebruikersorganisatie als haar accountant niet begreep waar de serviceorganisatie exact op doelde. Wederom is in deze situatie een vergelijking gemaakt tussen het uitbestedingscontract en de user control considerations, waarbij de uitkomst uitwees dat er geen 1-op-1-connectie tussen deze twee documenten gemaakt kon worden. Een intensieve exercitie tussen de gebruikersorganisatie en ontvangende accountant was in dit geval nodig om er zeker van te zijn dat alle user control considerations waren afgedekt door de interne processen van de gebruikersorganisatie.

Zoals eerder beschreven zijn deze exercities arbeidsintensief, hetgeen niet het doel is van de assurancerapportage. Zowel in situatie één, twee als drie had het aanvullende werk beperkt kunnen worden als er vroegtijdig contact was gelegd tussen de serviceorganisatie en gebruikersorganisatie aangaande de scope van de assurancerapportage.

4. Kennis en kunde van de gebruikersorganisatie

De voorgaande drie situaties gingen veelal in op de inhoud en formulering van de user control considerations. Deze voorgaande situaties raken echter ook de vierde situatie die zich heeft voorgedaan in onze analyse: de kennis van de gebruikersorganisaties is niet altijd up-to-date met betrekking tot ISAE3402-assurancerapportages.

1. In situatie één ondernam de gebruikersorganisatie pas actie na een constatering van de gebruikersaccountant. De gebruikersorganisatie wist immers niet dat er user control considerations benoemd hadden moeten worden in de assurancerapportage.
2. In situatie twee ging de gebruikersorganisatie er op basis van de user control considerations van uit dat ze geen extra werkzaamheden hoefde uit te voeren voor de assurancerapportage, behalve het op orde hebben van haar interne beheersing. Dit is natuurlijk een voorwaarde voor het gebruiken van een assurancerapportage, maar de vage en multi-interpretabele formulering zorgt voor onduidelijkheden over welke interne beheersing en verantwoordelijkheden dit precies omhelst.
3. In de derde situatie wist de gebruikersorganisatie zich geen raad met de wildgroei aan user control considerations. Deze zorgde wederom voor onduidelijkheid en tevens veel aanvullende werkzaamheden voor de gebruikersorganisatie en haar accountant.

Er kunnen verschillende redenen zijn voor de beperkte kennis en kunde op het gebied van assurancerapportages bij de gebruikersorganisatie. Een daarvan is dat het contractmanagement en monitoren van de uitbestedingsrelatie onderdeel is van een meeromvattende functie van één werknemer. De IT-manager is hier bijvoorbeeld verantwoordelijk voor, maar deze moet daarnaast ook de IT-afdeling managen en de interne beheersing op orde houden. Hierdoor wordt diens beschikbare tijd verspreid over verschillende werkgebieden. Derhalve zal er beperkt aandacht zijn voor de uitbestede dienstverlening, waardoor een gedegen beoordeling van de uitbestedingsrelatie en ISAE3402-assurancerapportage te wensen overlaat.

De kennis bij de gebruikersorganisaties met betrekking tot ISAE3402-assurancerapportages is niet altijd up-to-date

Daarnaast kan het ook zo zijn dat de serviceorganisatie delen van haar bedrijfsvoering heeft uitbesteed, waardoor ook sub-serviceorganisaties zijn opgenomen in de assurancerapportages. Deze sub-serviceorganisaties maken de procesketen complexer, waardoor deze voor de gebruikersorganisatie ongrijpbaar kan worden. De gebruikersorganisaties moeten dan namelijk nagaan of deze sub-serviceorganisaties ook invloed hebben op de interne beheersingsmaatregelen, wat het geheel ingewikkeld maakt.

Daarom is het van belang dat de gebruikersorganisatie zich ervan bewust is dat ze de ISAE3402-assurancerapportage moet beoordelen, hier conclusies uit trekt en daarover (tijdig) in gesprek gaat met haar serviceorganisatie. Daarbij hoort ook de controle of de user control considerations onderdeel zijn van de interne beheersing van de gebruikersorganisatie. In de praktijk zien wij dat gebruikersorganisaties veelal de assurancerapportage lezen, maar hier geen of nauwelijks actie door ondernemen. Daarom is aan dit artikel een stappenplan toegevoegd voor het reviewen van een ISAE3402-assurancerapportage.

Stappenplan voor de review van een ISAE3402-rapportage

Zoals hiervoor al beschreven is, hebben vele gebruikersorganisaties moeite met een gedegen beoordeling van de ontvangen assurancerapportage. Enerzijds komt dit doordat niet altijd de kennis en kunde hiervoor aanwezig zijn in de organisatie, anderzijds is de hiervoor verantwoordelijke werknemer van de gebruikersorganisatie ook belast met andere werkzaamheden. Derhalve is in figuur 2 een stappenplan op hoofdlijnen opgenomen, om in de toekomst over te gaan tot een efficiëntere accountantscontrole, waarin gebruikersorganisaties voorbereid zijn op het reviewen van een assurancerapportage.

Stap 1: Lees de ontvangen assurancerapportage
Neem de tijd om de assurancerapportage goed door te nemen. De rapportage hoeft niet in detail te worden bestudeerd; de tekst – met name Sectie III met daarin de beschrijving van de serviceorganisatie – kan globaal worden gelezen. Als lezer moet je gevoel krijgen met de inhoud van de assurancerapportage.

Stap 2: Bepaal het type rapport, de periode en het bereik van de assurancerapportage
In deze stap wordt de assurancerapportage grondiger bestudeerd. Hierbij dienen de volgende vragen te worden beantwoord:

• *Wat voor type assurancerapport heeft de gebruikersorganisatie ontvangen?* In het kader van de jaarrekeningcontrole zijn ISAE3402-rapportages het meest geschikt, aangezien deze specifiek bedoeld zijn voor de financiële verantwoording. Een ISAE3000-rapportage kan in sommige gevallen echter ook worden gebruikt voor de accountantscontrole, nadat is vastgesteld dat de relevante processen hiervoor zijn opgenomen in de rapportage. Daarnaast zou een gebruikersorganisatie de voorkeur moeten hebben voor een type 2-rapportage, want hierin wordt ook de werking van de controles getest, en niet enkel de opzet en het bestaan ervan, zoals in een type 1-rapport.

• *Welke auditor heeft de assurancerappportage opgesteld?* En kan de gebruikersorganisatie vaststellen dat deze auditor voldoende professionele kennis, reputatie, objectiviteit en onafhankelijkheid bezit ten opzichte van de serviceorganisatie?

• *Welke periode dekt de assurancerapportage af?* Om als accountant van de gebruikersorganisatie te kunnen steunen op de controles van de serviceorganisatie, zal de werkingsperiode overeen moeten komen met de periode van de accountantscontrole. In het geval van een kortere of verschoven werkingsperiode (bijvoorbeeld een assurancerapportage voor de periode 1 januari tot en met 30 september, terwijl de accountantscontrole tot en met 31 december loopt), zal een zogeheten bridgeletter moeten worden afgegeven door de serviceorganisatie, dan wel zullen er aanvullende werkzaamheden moeten worden verricht door de gebruikersaccountant.

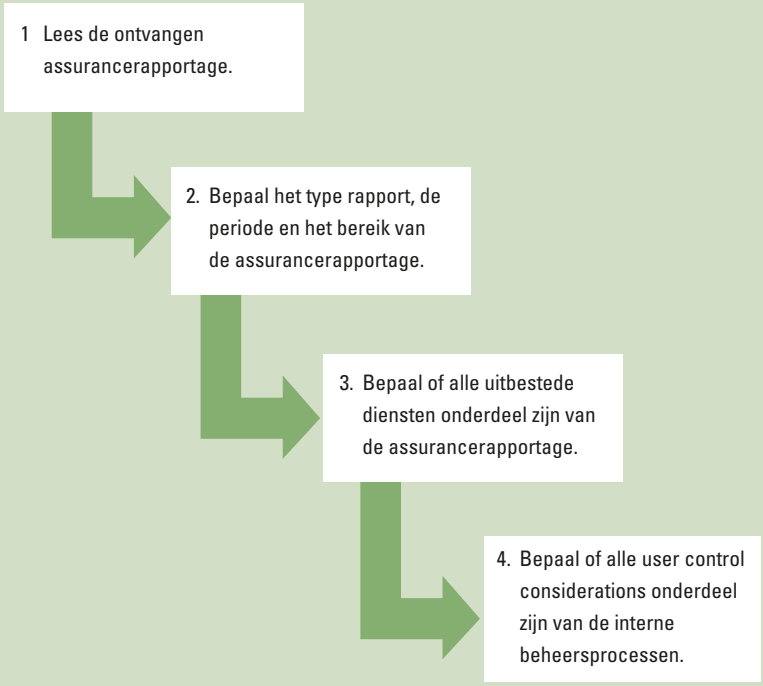
• *Is er sprake van subserviceorganisaties?* Het kan zijn dat de serviceorganisatie ook weer diensten heeft uitbesteed; in dat geval moet na worden gegaan of er sprake is van een zogenaamde 'carve-out'- of 'inclusive'-methode.
In het geval van een carve-out zijn de diensten van de subserviceorganisatie niet opgenomen in de assurancerapportage, en dient de gebruikersorganisatie een afweging te maken of deze uitbesteding relevant is voor de afgenomen diensten. Ook moet worden nagegaan of er user control considerations zijn opgenomen aangaande deze subserviceorganisatie. Als de gebruikersorganisatie de subserviceorganisatie dermate relevant vindt voor de interne beheersing, moet een assurancerapport worden opgevraagd bij de betreffende subserviceorganisatie. Bij een inclusive-methode zijn de controles opgenomen in de assurancerapportage, en dient de gebruikersorganisatie enkel na te gaan of deze van belang zijn voor de afgenomen diensten.

Stap 3: Bepaal of alle uitbestede diensten onderdeel zijn van de assurancerapportage
In deze stap dient de gebruikersorganisatie vast te stellen of alle uitbestede diensten worden afgedekt door het controleraamwerk van de serviceorganisatie. De gebruikersorganisatie kan deze controle uitvoeren door het uitbestedingscontract en de daarin overeengekomen uitbesteding te vergelijken met de user control considerations en de gecontroleerde diensten in de assurancerapportage van de serviceorganisatie. Indien deze op elkaar aansluiten zijn er geen 'gaten' in het proces en is er sprake van een volledige keten.

In het geval dat er bevindingen zijn bij de uitbestede diensten, dient de gebruikersorganisatie te overleggen met haar serviceorganisatie om na te gaan wat de impact van deze bevindingen is op de gebruikersorganisatie.

Stap 4: Bepaal of alle user control considerations onderdeel zijn van de interne beheersingsprocessen
In deze stap dient de gebruikersorganisatie na te gaan welke user control considerations zijn opgenomen in de rapportage en voor haar accountant aan te tonen dat deze onderdeel zijn van de interne beheersingsprocessen. Op deze manier toont de gebruikersorganisatie aan dat de procesketen sluitend is.

Figuur 2. Stappenplan voor de beoordeling van een ISAE3402-assurancerapportage.



OP PRAKTISCHE WIJZE OMGAAN MET USER CONTROL CONSIDERATIONS

Ter aanvulling op het stappenplan geven wij tot slot nog een aantal praktische tips voor het op een goede manier omgaan met user control considerations. Het uitgangspunt voor de user control considerations is dat er sprake is van een procesketen waarvan een gedeelte door de gebruikersorganisatie is uitbesteed aan een serviceorganisatie. Sommige controles in de keten worden uitgevoerd door de serviceorganisatie, maar om de keten sluitend te maken, dient de gebruikersorganisatie nog een aantal zaken te controleren. Zoals aangegeven in het stappenplan dient de gebruikersorganisatie dus altijd na te gaan welke user control considerations zijn opgenomen in de assurancerapportage. Op basis van onze analyse vanuit de praktijk kunnen we daarbij drie situaties onderscheiden.

1. De user control considerations zijn duidelijk en toegesneden op de situatie
Deze situatie is het meest eenvoudig. De accountant moet van de gebruikersorganisatie nagaan of deze de gevraagde testwerkzaamheden aantoonbaar heeft uitgevoerd. Als uit deze testwerkzaamheden verder geen bijzonderheden zijn gebleken kan dit worden gedocumenteerd in samenhang met de verwerking van het assurancerapport.

2. De user control considerations ontbreken in de assurancerapportage
In dit geval zal de gebruikersorganisatie zelf moeten evalueren of ze nog aanvullende controles moet uitvoeren om de keten sluitend te krijgen. Indien dit het geval is zullen deze alsnog aantoonbaar moeten worden uitgevoerd, zodat er geen gaten in de interne beheersing ontstaan. Het is logisch dat er in deze situatie goed overleg moet plaatsvinden met zowel de accountant van de gebruikersorganisatie als de accountant van de serviceorganisatie, zodat duidelijkheid ontstaat over de relevante user control considerations in de keten en wie deze uitvoert. Op deze manier wordt zowel het risico van gaten in de keten, dan wel dubbel werk, zo veel mogelijk voorkomen en in de toekomst kunnen er verbeteringen worden doorgevoerd in het overzicht van de ketencontroles.

3. De user control considerations zijn aanwezig in de assurancerapportage, maar onvoldoende concreet, of het zijn er te veel
In deze situatie zal de gebruikersorganisatie een eigen risicoanalyse moeten opstellen. Deze risicoanalyse zal uitwijzen welke risico's de gebruikersorganisatie loopt in de procesketen. Indien de user control considerations onvoldoende concreet zijn, is het verstandig te overwegen daarvoor in de plaats eigen controles uit te voeren die wel relevant zijn om de risico's af te dekken. Indien er te veel user control considerations in het assurance-

rapport zijn opgenomen, kan gebruik worden gemaakt van de eigen risicoanalyse om te documenteren dat de controles uit het rapport te breed zijn geformuleerd, dan wel niet relevant zijn. Ook hierbij kan worden verwezen naar de eigen controles die aantoonbaar zijn uitgevoerd om de risico's alsnog af te dekken. Ook in deze situatie is het verstandig nauwe afstemming te zoeken met de accountant van zowel de gebruikers- als de serviceorganisatie, om tot consensus te komen en de situatie in de toekomst transparant te maken.

CONCLUSIE

Door de huidige constateringen van de AFM, de implementatie van de SSAE18-standaard in de Verenigde Staten en de richtlijnen van DNB zullen user control considerations de komende jaren een belangrijke rol spelen in assurancerapportages voor zowel gebruikers- als serviceorganisaties. Op basis van onze praktijkervaring zien wij dat er ruimte is voor verbetering, en gezien de huidige ontwikkelingen is het ook noodzaak om organisaties bewuster te maken van de user control considerations. De huidige praktijk zorgt voor veel onduidelijkheden, onzekerheden en meer werk, zowel voor gebruikers- en serviceorganisaties als hun accountants. De betrokken partijen doen er daarom goed aan om de volgende aanbevelingen mee te nemen in hun toekomstige werkzaamheden aangaande de user control considerations.

Om te beginnen kan er meer duidelijkheid worden gecreëerd aangaande de formulering. Bij de user control considerations is het van belang dat door de serviceorganisatie en haar accountant aandachtig wordt gekeken naar de formulering van de maatregelen. Een user control consideration moet geen dubbelzinnigheden bevatten en helder zijn, voor zowel de service- als gebruikersorganisatie. Er moet een norm in beschreven staan die ook voor de ontvangende accountant toetsbaar is. De service-auditor kan dit toetsen door de user control considerations te bekijken vanuit het perspectief van de gebruikersorganisatie.

Daarnaast moeten de serviceorganisatie en service-auditor een balans vinden in het aantal user control considerations dat ze opnemen in de assurancerapportage. Hoewel er geen richtlijnen aangaande het aantal op te nemen maatregelen zijn, is het voor de gebruikersorganisatie en haar accountant een arbeidsintensief proces om na te gaan of alle user control considerations relevant zijn voor de gebruikersorganisatie en of deze afgedekt zijn in het interne beheersproces.

Ook is het van belang dat de gebruikersorganisatie vroegtijdig op de hoogte is van de user control considerations. Deze zouden gezien het uitbestedingscontract geen verassing mogen zijn, maar de uitbestedingsrelatie is ermee geholpen als de verantwoordelijkheden duidelijk zijn afgesproken. In het uitbestedingscontract moet daarom beschreven zijn welke partij welke werkzaamheden uitvoert en wie er verantwoordelijk is bij eventuele incidenten. Op deze manier kan de gebruikersorganisatie haar interne beheersing goed inrichten en ontstaan er geen 'gaten' in de procesketen. Indien dit niet voldoende gespecificeerd is kan de gebruikersorganisatie voor verrassingen komen te staan, zoals aanvullende werkzaamheden en extra kosten van haar accountant, in het geval de user control considerations niet zijn opgenomen in de interne processen. De gebruikersaccountant dient namelijk na te gaan of de gehele procesketen wordt gevolgd, voor de juistheid en volledigheid van de financiële verslaggeving.

Als laatste is het van belang dat de gebruikersorganisatie haar kennis aangaande assurancerapportages actueel houdt en deze ook kan toepassen in de praktijk. Ze moet weten welke elementen van belang zijn voor een gezonde uitbestedingsrelatie en wat ze van haar serviceorganisaties moet vragen. De accountant van de gebruikersorganisatie kan tot op zekere hoogte altijd diens klant hierin adviseren en begeleiden.

Literatuur

[AFM14] Autoriteit Financiële Markten, *Uitkomsten onderzoek kwaliteit wettelijke controles Big 4-accountantsorganisaties*, AFM, 25 september 2014.

[AFM17] Autoriteit Financiële Markten, *Uitkomsten van onderzoeken naar de implementatie en borging van verandertrajecten bij de OOB-accountantsorganisaties en de kwaliteit van wettelijke controles bij de Big 4-accountantsorganisaties*, AFM, 28 juni 2017.

[Beek12] J.J. van Beek, *Praktijkgids 4; Service Organisatie Controlrapport, ISAE3402*, KPMG, 2012.

[NBA17] Koninklijke Nederlandse Beroepsorganisatie van Accountants, *402 Overwegingen met betrekking tot controles van entiteiten die gebruikmaken van een serviceorganisatie*, Handleiding Regelgeving Accountancy, 2017.

[Palm16] D. Palmer, *Clarified attestation standards – SSAE 18*, KPMG, september 2016.

Over de auteurs

Drs. J.J. van Beek RE RA is als partner werkzaam bij KPMG IT Advisory. Hij heeft meer dan 30 jaar ervaring met alle aspecten van het vakgebied IT-audit, met een focus op opdrachten voor cliënten in Financial Services. Binnen Nederland en Europa is hij leider van de KPMG-serviceline IT attestation, en verantwoordelijk voor de ontwikkeling van diensten op dit gebied en auteur van diverse praktijkgidsen.

Ir. R.P.A.C. van Vught is als senior consultant werkzaam bij KPMG IT Advisory. Zij is gespecialiseerd op het gebied van assurancerapportages en service level management in het kader van de jaarrekeningcontrole. Het afgelopen jaar heeft zij voor verschillende klanten en diensten werkzaamheden verricht aangaande assurancerapportages en daarbij veel praktijkervaring opgedaan, die in dit artikel wordt gedeeld.