Een nadere uitwerking naar typen en randvoorwaarden

# Data-analyse in de uitvoeringsfase van de audit

9 november 2017

Barney de Rooij, Wilco Schellevis, Angelique Koopman

Data-analyse wordt steeds vaker ingezet bij de controle van de jaarrekening. Om de uitkomsten hiervan als betrouwbare controle-informatie te kunnen gebruiken, dienen deze echter wel aan voorwaarden te voldoen. Onderzoek naar de opzet, bestaan en effectieve werking van de key General IT-Controls wordt in de literatuur daarbij vaak als een van deze voorwaarden benoemd. In de nadere voorschriften controle- en overige standaarden wordt echter vrijwel geen directe aandacht besteed aan data-analyse. Dit in tegenstelling tot bijvoorbeeld het gebruik van steekproeven bij een controle, waar een gehele standaard aan gewijd is. In dit artikel gaan we in op de vraag aan welke kwaliteitseisen met betrekking tot General IT-Controls en overige voorwaarden data-analyse dient te voldoen in het kader van de jaarrekeningcontrole om als betrouwbare controle-informatie gebruikt te worden. Hierbij is het studierapport Jaarrekening controle in het mkb: IT audit geïntegreerd in de controle-aanpak [SCHE14] gebruikt voor onder andere de definitie van de verschillende categorieën General IT-Controls, application controls en authorisation controls.

Dit artikel is mede gebaseerd op het referaat van Barney de Rooij over dit onderwerp, in het kader van de Executive Master IT Auditing aan de Erasmus Universiteit. In dit artikel ligt de nadruk op de uitkomsten van het uitgevoerde onderzoek dat heeft geresulteerd in de uitwerking van een conceptueel model, waarin verschillende typen data-analyse worden beschreven. Ook is per type data-analyse een uitwerking gemaakt van relevante randvoorwaarden. Dit artikel gaat alleen over de vormen van data-analyse die bruikbaar zijn in de uitvoeringsfase van de controle. Het gebruik van data-analyse in de planningsfase van de audit – bijvoorbeeld voor *understanding the entity* – en de risico-inschatting valt buiten de scope van dit artikel.

## Voorbereiding van de data-analyse: controle-informatie over de data-extractie

In overeenstemming met standaard 500 'Controle-informatie' dient de accountant te overwegen in welke mate de informatie die als controle-informatie zal worden gebruikt, voldoende betrouwbaar is voor de doeleinden van de accountant (500.9). Voor data-analyse wordt vaak gebruikgemaakt van lijstwerk, waarbij onttrekking via de applicatie

of rechtstreeks uit de database mogelijk is. Om vast te stellen of de gegevens die worden gebruikt bij de data-analyse voldoende nauwkeurig en volledig zijn, dient de accountant controle-informatie te verkrijgen over de volgende vragen.

1. Heb ik voldoende zekerheid omtrent rechtmatigheid van rechtstreekse mutaties in de database?
2. Zijn de juiste parameters ingesteld bij het onttrekken van de data?
3. Is de data tussen het moment van genereren en het verkrijgen door de accountant niet gemuteerd?

Het beantwoorden van deze vragen maakt geen onderdeel uit van dit artikel. In dit artikel gaan we ook niet in op detailcontroles die uitgevoerd worden om de gebruikte data bij data-analyses aan te sluiten op onderliggende stukken om de nauwkeurigheid ervan te valideren. Door de NOREA-kennisgroep IT & Financial Audit is overigens recent een voorbeeldaanpak gepubliceerd over dit thema.

## Documentatie: controleerbaarheid en de reproduceerbaarheid

In overeenstemming met standaard 230 'Controledocumentatie' dient de accountant de controledocumentatie zo op te stellen dat die voldoende is om een ervaren accountant die niet eerder bij de controle betrokken was, in staat te stellen om inzicht te verwerven in onder andere de aard, timing en omvang van de controlewerkzaamheden inclusief de uitkomsten ervan, alsmede de verkregen controle-informatie. Deze standaard geldt voor alle vormen van controledocumentatie en dus ook bij de toepassing van data-analyse. Een toereikende vastlegging om de uitgevoerde data-analyse controleerbaar en reproduceerbaar te maken is essentieel.

# Conceptueel model

In tabel 1 is het conceptueel model opgenomen. Dit model geeft voor diverse toepassingen van data-analyses in de uitvoeringsfase van de audit de randvoorwaarden waaraan de data-analyses dienen te voldoen om als bruikbare en betrouwbare controle-informatie te kunnen dienen.

| | | | Voorwaarden | | | | | |
|---|---|---|---|---|---|---|---|---|
| Soort data-analyse | Gecontroleerde Bewering | Controle-werkzaamheid | LTB[1] | Change manage-ment | Controle data-extravtie | Controleer- en repro-duceer-baar | Gehele standaard | Overige |
| Interne verbandscontrole | Volledigheid | Cijferanalyse | (X)** | X* | X | X | 520 | a |
| Interne verbandscontrole | Juistheid | Cijferanalyse | | | X | X | 520 | |
| Externe verbandscontrole | Juistheid en volledigheid | Cijferanalyse | | | X | X | 520 | b |
| Selectie specifieke items | Juistheid | Inspectie | | | X | X | | c |
| Autorisatie/ functiescheiding | Juistheid | Inspectie | X** | | X | X | | d |

**Tabel 1:** Het conceptueel model

# Legenda

| | |
|---|---|
| **1** | **1** |
| **LTB: Logische Toegangsbeveiliging** | LTB: Logische Toegangsbeveiliging |
| **1** | **X** |
| **LTB: Logische Toegangsbeveiliging** | Aan voorwaarde dient voldaan te worden. |
| **1** | **(X)** |
| **LTB: Logische Toegangsbeveiliging** | Afhankelijk van situatie dient beperkt (application controls) of volledig (autorisation controls) te worden voldaan. |
| **1** | * |
| **LTB: Logische Toegangsbeveiliging** | Voorwaarde geldt voor applicatie waaruit data wordt onttrokken (basis SOLL-positie). |
| **1** | ** |
| **LTB: Logische Toegangsbeveiliging** | Alleen voor de onderdelen identificatie en authenticatie dient hieraan te worden voldaan. |
| **1** | **a** |
| **LTB: Logische Toegangsbeveiliging** | De opzet, het bestaan en de werking van relevante application en/of autorisation controls dient vastgesteld te worden voor applicatie waaruit data wordt onttrokken ter bepaling van de verwachting (SOLL-positie) ten behoeve van vergelijking met IST-positie. |
| **1** | **b** |
| **LTB: Logische Toegangsbeveiliging** | Er dient vastgesteld te worden dat er gebruik wordt gemaakt van een externe bron als basis voor de verwachting (SOLL-positie). – Begin- en eindstanden van relevante jaarrekeningposten zoals liquide middelen, bankschulden en begin- en eindvoorraden dienen vastgesteld te worden indien dit van belang is voor het bepalen van de verwachting (SOLL-positie). |
| **1** | **c** |
| **LTB: Logische Toegangsbeveiliging** | Er dient een onderbouwing opgenomen te worden voor de gekozen kenmerken ter selectie van specifieke items – Het niet geselecteerde deel van de populatie dient (mits materieel) ook in de detailcontrole betrokken te worden, gegeven de controlerisico's, materialiteit en overige reeds uitgevoerde controlewerkzaamheden. |
| **1** | **d** |
| **LTB: Logische Toegangsbeveiliging** | Op ongeautoriseerde en/of niet in functiescheiding tot stand gekomen items dienen (mits materieel) detailcontroles uitgevoerd te worden. |

## Interne verbandscontrole voor het vaststellen van de volledige verantwoording van het object van onderzoek

Bij deze soort data-analyse wordt een verband gelegd tussen meerdere intern gegenereerde populaties, waarbij voor geen van de populaties een (bruikbaar) verband gelegd kan worden met een externe bron. Deze soort data-analyse kan bijvoorbeeld toegepast worden voor ondernemingen waar geen verband tussen in- en verkoop aanwezig is (zoals bij de verkoop van e-books). Deze analyse is tevens bruikbaar als het verband tussen in- en verkoop om praktische redenen niet gelegd kan worden.

In dergelijke gevallen dienen intern waarborgen getroffen te worden om de volledigheid van de populatie te waarborgen. Voor een organisatie die e-books verkoopt zullen bijvoorbeeld waarborgen getroffen kunnen worden dat bij het versturen van een downloadlink automatisch een registratie in een beveiligd bestand plaats dient te vinden. De accountant zal in dat geval willen vaststellen dat deze *application control* in opzet aanwezig is, bestaat en werkt. Indien in dit bestand vervolgens geen regels meer verwijderd kunnen worden, zal de accountant dit tevens willen vaststellen. Indien verwijderen wel mogelijk is, maar slechts door (een beperkt aantal) bevoegde functionarissen, is sprake van een *authorisation control*. Ook hiervan zal de accountant de opzet, het bestaan en de werking willen vaststellen. Aan de volgende eisen met betrekking tot General IT-Controls dient voldaan te worden (tabel 2 ontleend aan [SCHE14]).

| | Change management | Logische Toegangsbeveiliging |
|---|---|---|
| Application control | Werking | Bestaan |
| Autorisation control | Werking | Werking |

**Tabel 2:** Eisen met betrekking tot General IT-Controls

De enkele asterisk in het model (tabel 1) geeft aan dat alleen voor de applicatie waaruit data onttrokken wordt aan de voorwaarden met betrekking tot change management en logische toegangsbeveiliging voldaan dient te worden. Aangezien de output uit de financiële administratie een IST-positie oplevert, is het niet nodig om voor die applicatie werkzaamheden voor de General IT-Controls te verrichten.

## Interne verbandscontrole voor het vaststellen van de juiste verantwoording van het object van onderzoek

Ook bij deze soort data-analyse wordt een verband gelegd tussen meerdere intern gegenereerde populaties. Deze soort data-analyse zal met name toegepast worden als meerdere vastleggingen aanwezig zijn met betrekking tot een post in de jaarrekening, waarvan de accountant deze geschikt acht om ze met elkaar in verband te brengen. Een bekend voorbeeld is de *three-way-match* inkopen, waar een verband wordt gelegd tussen de bestelling, ontvangst en de facturatie van inkopen. Overigens is een three-way-match aan de inkoopzijde vaak alleen geschikt als vastgesteld kan worden dat de vastlegging van bestelling, ontvangst en facturatie van inkopen gescheiden tot stand is gekomen. Om vast te stellen dat dit daadwerkelijk het geval is, zal deze interne verbandscontrole vaak gecombineerd worden met een toets of de vastleggingen daadwerkelijk door verschillende functionarissen tot stand zijn gebracht. Indien de accountant deze scheiding wil vaststellen door middel van data-analyse, dient aan de voorwaarden van de vijfde soort data-analyse voldaan te worden. Indien de onderneming zelf afdwingt dat een functionaris geen toegang heeft tot de vastlegging van zowel de bestelling, ontvangst als/of inkoop, is sprake van een authorisation control. De accountant dient in dat geval werkzaamheden uit te voeren om de opzet, het bestaan en de werking van deze interne beheersingsmaatregel vast te stellen (inclusief bijbehorende General IT-Controls).

## Externe verbandscontrole gericht op het vaststellen van de juiste en/of volledige verantwoording van het object van onderzoek

Kenmerkend onderscheid tussen deze data-analyse en de interne verbandscontrole is dat de SOLL-positie tot stand komt op basis van een externe bron. Op basis van een koppeling met de geldbeweging kan door middel van deze soort data-analyse vastgesteld worden dat alle betaalde inkopen zijn verantwoord in de financiële administratie. Dit geldt zowel voor inkopen van goederen als uren. Deze soort data-analyse kan ook gehanteerd worden als de inkopen rechtstreeks door de leverancier bevestigd worden. Een bekend voorbeeld is de autodealer, die haar nieuwe auto's alleen inkoopt bij de importeur. Rekening houdend met de vaststelling van de accountant van de juist- en volledigheid van de verantwoorde begin- en eindvoorraden, kan met de bevestiging van de importeur van de ingekochte auto's een SOLL-positie opgesteld worden voor de verkochte auto's. De bevestiging door de importeur van het aantal ingekochte auto's betreft een externe confirmatie. Deze dient te voldoen aan de standaard 505 'externe confirmaties'.

In de standaarden wordt geen onderscheid gemaakt tussen interne en externe verbandscontroles. Beide verbandscontroles kunnen in theorie op een zelfde wijze en voor

hetzelfde doel ingezet worden. De randvoorwaarden om de betrouwbaarheid vast te stellen zijn wel verschillend, zoals blijkt uit het conceptueel model.

## Vereisten aan gegevensgerichte cijferanalyse

Aangezien alle verbandscontroles in de categorie cijferanalyse als controlewerkzaamheid vallen, is de standaard 520 'Cijferanalyses' volledig van toepassing op de eerste drie categorieën data-analyses. Hierin zijn de volgende vereisten opgenomen met betrekking tot de gegevensgerichte cijferanalyse.

- De geschiktheid van bepaalde gegevensgerichte cijferanalyses voor gegeven beweringen dient bepaald te worden. Kortom, draagt deze data-analyse wel bij aan het terugbrengen van geïdentificeerde risico tot een aanvaardbaar niveau?
- De betrouwbaarheid van gegevens die de basis zijn voor de verwachting van de accountant over vastgelegde bedragen of ratio's dient vastgelegd te worden. Hierbij wordt rekening gehouden met het bronsysteem waaruit de data is onttrokken, de vergelijkbaarheid en de aard en relevantie van de beschikbare informatie, alsmede met interne beheersingsmaatregelen met betrekking tot de opstelling van de informatie. Deze eis is relevant aangezien vanuit de data-analyse een SOLL-positie wordt berekend, die getoetst wordt aan de financiële administratie (IST-positie). Hoe de betrouwbaarheid vastgesteld kan worden is afhankelijk van de bron van de data (intern of extern) en de te controleren bewering (volledigheid of juistheid). In de toelichting op de verschillende soorten verbandscontroles wordt ingegaan welke randvoorwaarden voor de betrouwbaarheid relevant zijn.
- Er dient een voldoende nauwkeurige verwachting bepaald te worden van vastgelegde bedragen of ratio's. Een bekend voorbeeld van een geformuleerde verwachting van de omvang van de verkochte aantallen goederen en/of diensten betreft de goederenbeweging, waar een verband wordt gelegd tussen inkopen en begin- en eindvoorraad, rekening houdend met eventuele verstoringen. Door middel van data-analyse kan deze verwachting op elk gewenst detailniveau bepaald worden (totaalniveau, artikelgroep, artikel enz).

Ook de omvang van een eventueel verschil tussen de vastgelegde bedragen (IST-positie) en de verwachte waarde (SOLL-positie) dat aanvaardbaar is zonder verder onderzoek te verrichten, dient vastgesteld te worden. Door middel van data-analyse wordt vaak een exact verschil gedefinieerd, dat tegen dit maximaal aanvaardbare verschil afgezet kan worden. Indien het verschil uit de data-analyse het gedefinieerde maximum overstijgt, dient nader onderzoek verricht te worden.

## Selectie specifieke items

Door inspectie van digitale vastgelegde gegevens kunnen eenvoudig items geselecteerd worden die aan bepaalde kenmerken voldoen. Het selecteren van posten op deze manier is in standaard 500 'Controle-informatie' gedefinieerd als het selecteren van specifieke items.

In de standaard wordt als voorbeeldkenmerk de omvang van een transactie genoemd. Andere kenmerken zijn echter ook mogelijk, zoals het onderverdelen van transacties naar dagboek (bijvoorbeeld memoriaalboekingen). Indien de accountant van deze vorm van data-analyse gebruik wenst te maken, dient hij vast te leggen waarom hij vindt dat het gekozen kenmerk relevant is. Daarnaast is in de standaard expliciet opgenomen dat de resultaten van controlewerkzaamheden die worden toegepast op items die op deze manier zijn geselecteerd niet kunnen worden geprojecteerd op de gehele populatie. De accountant zal voor de resterende populatie dienen te onderbouwen in hoeverre, gegeven de controlerisico's, materialiteit en overige reeds uitgevoerde controlewerkzaamheden, nadere analyse noodzakelijk is.

## Autorisatie/ functiescheiding

Deze vorm van data-analyse dient om vast te stellen of transacties aan relevante autorisatiestandaarden voldoen en/of in functiescheiding tot stand zijn gekomen. Het vaststellen van een onafhankelijk tot stand gekomen vastlegging van de bestelling, ontvangst en facturatie van de inkopen als onderdeel van de reeds eerder aangehaalde three-way-match is hiervan een bekend voorbeeld. Om vast te stellen dat de voor de data-analyse gebruikte vastlegging van de identiteit van de gebruiker van het geautomatiseerde systeem betrouwbaar is, dient de accountant met een redelijke mate van zekerheid vast te stellen dat degene die de transactie daadwerkelijk (fysiek) heeft uitgevoerd ook degene is die digitaal als uitvoerder van de transactie in het systeem wordt opgenomen. De onderneming dient derhalve waarborgen getroffen te hebben inzake de logische toegangsbeveiliging van de relevante applicatie. In dit geval zijn echter alleen de onderdelen identificatie en authenticatie van de logische toegangsbeveiliging relevant. Het autorisatiedeel, oftewel het vaststellen dat gecontroleerd rechten in de applicatie toegekend worden en het monitoren van de toegekende autorisaties, is niet relevant. Immers, door de data-analyse wordt vastgesteld dat de relevante autorisaties zijn verricht en/of de functiescheiding in de praktijk niet is doorbroken. Overigens zijn transacties die niet toereikend zijn geautoriseerd en/of de functiescheiding is doorbroken niet per definitie fout. De accountant zal echter wel toereikende detailcontroles uit dienen te voeren om vast te stellen dat de transacties niet fout zijn.

**Literatuur**

[SCHE14] Schellevis, Wilco en Vera van Dijk, *'Jaarrekening controle in het mkb: IT audit geïntegreerd in de controle-aanpak'*, NBA/NOREA, 2014

## B. (Barney) de Rooij MSc RA EMITA | registeraccountant en IT-Auditor bij *Baker Tilly Berk*

Barney de Rooij MSc RA EMITA heeft een gecombineerde functie van registeraccountant en IT-Auditor in de controlepraktijk van Baker Tilly Berk. Ook is Barney binnen NOREA actief in een werkgroep voor de combinatie IT en Financial Audit.

## Drs. W. (Wilco) Schellevis | Directeur bij *Refine-IT*

Drs. Wilco Schellevis is partner bij Visser & Visser Accountants-Belastingadviseurs en directeur van Refine-IT. Wilco is onder andere binnen NOREA en SRA actief op het snijvlak van IT & Financial Audit.

## Drs. A. (Angelique) J.M. Koopman RE RA | docent in de (post) master Accountancy *bij Tilburg University*

Drs. Angelique Koopman RE RA is partner Audit Innovation en verbonden aan Bureau Vaktechniek Accountants van Baker Tilly Berk. Angelique is eveneens werkzaam voor Tilburg University als docent in de (post) master Accountancy en actief binnen werkgroepen van de NBA en NOREA op het gebeid van Data-analyse & IT in de Audit.