Testen we nog general IT controls bij het toepassen data-analyse?

27 augustus 2021 NOREA-werkgroep IT & Financial Audit

(Publicatiedatum: 27 augustus 2021)

Van oudsher hechten we groot belang aan het testen van de general IT controls om tot een oordeel over de jaarrekening te komen. Dit artikel behandelt de vraag of dit nog wel altijd nodig is, gegeven de groeiende nadruk op datagedreven audits.

Een datagedreven auditaanpak krijgt een steeds belangrijkere rol in de jaarrekeningcontrole. IT-systemen bevatten vandaag de dag immers een grote hoeveelheid data die relatief eenvoudig toegankelijk is. Daarnaast zijn er voldoende middelen beschikbaar om deze data te analyseren en vervolgens conclusies te trekken. De basis voor een goede data-analyse ligt in het beoordelen of de te analyseren data voldoende betrouwbaar zijn voor het doel van de analyse. Al naar gelang de situatie zijn de eisen aan deze betrouwbaarheid hoger of lager. Als de gegevens worden gebruikt om de jaarrekening van een organisatie te controleren, stellen we hoge eisen aan de betrouwbaarheid.

Hoewel ook diverse andere factoren van invloed zijn op de betrouwbaarheid van data, worden de general IT controls vaak gezien als randvoorwaardelijk voor een (blijvend) juiste registratie van data. Tegelijkertijd constateren we in de praktijk ook dat regelmatig niet op general IT controls kan worden gesteund of dat ze zelfs niet worden getest. En dat plaatst de accountant voor een vraagstuk dat de laatste tijd veelvuldig onderwerp van discussie is: *Kan ik de data uit de systemen van de gecontroleerde gebruiken voor mijn jaarrekeningcontrole als er niet op de general IT controls wordt gesteund?*

Doel van dit artikel is om deze vraag op hoofdlijnen te beantwoorden. We hebben niet het oogmerk voor elke mogelijke falende general IT Control de specifieke risico's of aanvullende werkzaamheden te benoemen. Dit blijft context-afhankelijk.

Onze belangrijkste conclusie is dat effectieve general IT controls niet per se noodzakelijkerwijs een randvoorwaarde zijn om data-analyse voor gegevensgerichte werkzaamheden te kunnen toepassen. Of dat zo is, hangt af van de situatie.

Toepassingen

Laten we eerst de belangrijkste toepassingen van data-analyse in kaart brengen. De NBA-handreiking 1141 Data-Analyse noemt de volgende toepassingen (we laten de richtlijnen in het kader van SOX/ICOFR hier buiten beschouwing):

- Data-analyse als onderdeel van de risico-inschattingswerkzaamheden, bijvoorbeeld om transactiestromen of trends en onverwachte verbanden in kaart te brengen. Dit levert input voor het bepalen van de controleaanpak.
- Data-analyse als onderdeel van het evalueren van interne beheersingsmaatregelen, bijvoorbeeld door te analyseren of inkooporder, goederenontvangst, inkoopfactuur en betaling overeenkomen.[1]
- Data-analyse als onderdeel van gegevensgerichte werkzaamheden, met als doel om afwijkingen van materieel belang op het niveau van beweringen te identificeren.

Daarnaast is er een onderscheid tussen data-analyse op primaire, respectievelijk secundaire registraties. Primaire registraties in IT-systemen zijn veelal niet te onderbouwen met fysieke documentatie. Bij een telecomprovider bestaan ze bijvoorbeeld uit de verbruikte 'telefoontikken'. De secundaire registraties in IT-systemen zijn gebaseerd op brondocumenten zoals een fysieke inkooporder, verkooporder, goederenontvangst en dergelijke. Ineffectieve general IT controls hebben bij primaire registraties een grotere impact op de controleaanpak dan bij secundaire registraties.

Randvoorwaarden

De standaard 500 NV COS bepaalt dat de accountant moet overwegen in welke mate de verkregen data relevant en voldoende betrouwbaar zijn. Als data wordt gebruikt voor een risicoanalyse wordt er over het algemeen minder belang gehecht aan de betrouwbaarheid van de data. Als we de data voor gegevensgerichte werkzaamheden willen gebruiken, is het specifieke doel van de data-analyse relevant. Dit lichten we verderop toe in de paragraaf 'Effectieve general IT controls niet per se noodzakelijk'.

Uiteraard is het proces rondom de extractie van belang om te borgen dat de relevante data juist en volledig uit het systeem of systemen worden verkregen. Dit is namelijk een randvoorwaarde bij het toepassen van data-analyse. Bij een datagedreven auditaanpak stelt de accountant met de data-analyse vast dat een juiste en volledige vastlegging en verwerking van gegevens in het systeem heeft plaatsgevonden. Een van de fundamentele vragen hierbij voor de accountant is hoe deze gegevens in het systeem zijn ingevoerd, om te bepalen of andere controlemiddelen dan data-analyse nodig zijn.

Voor primaire registraties wordt hierbij veelal gesteund op application controls zoals bevoegdheden, authenticatie en interface-controles en op general IT controls. Veelal zijn dergelijke controls essentieel om de (initiële) betrouwbaarheid van de vastlegging te borgen. Denk aan telecomproviders met geregistreerde verbruiks-tikken of energieleveranciers met registratie van verbruikte kilowatturen en kubieke meters gas.

Ook bij secundaire registraties wordt bij een systeemgerichte aanpak gesteund op dergelijke IT-gebaseerde controles. Als deze controles effectief zijn en het hele jaar hebben gewerkt, wordt een hogere mate van betrouwbaarheid aan de data toegekend. Dat is relevant voor een accountant die deze gegevens gebruikt voor gegevensgerichte werkzaamheden. Hierin ligt dus de toegevoegde waarde van effectieve general IT controls.

Welke general IT controls relevant zijn, kan per situatie verschillen. Algemeen gesteld vormen effectieve general IT controls het fundament van de effectieve werking van application controls, interface controls en bevoegdheden. Het gaat hierbij vooral om logische toegangsbeveiliging, wijzigingsbeheer en backup/recovery. In de praktijk betekent dit dat falende general IT controls diverse vragen oproepen over de betrouwbaarheid van de gegevens. En wat te doen als de general IT controls niet zijn getest, omdat de accountant niet steunt op application controls? Of omdat een volledig gegevensgerichte datagedreven controleaanpak wordt toegepast? We geven in de volgende paragraaf aan, welke vragen er rijzen als ineffectieve general IT controls zijn geconstateerd.

Vragen bij ineffectieve general IT controls

Falende general IT controls geven aanleiding tot vragen zoals:

- Zit alle data in het systeem én zit er niet teveel data in het systeem? Lacunes in wijzigingsbeheer en/of bevoegdheden brengen immers het risico met zich mee dat data onbevoegd/onterecht wordt aangepast.
- Hebben de application controls wel het hele jaar gefunctioneerd?
- Hoe weten we dat de noodzakelijke functiescheiding niet is doorbroken?
- Hoe weten we dat het terugzetten van data na een IT-incident (restore) niet heeft geleid tot verlies van gegevens?
- Hoe weten we dat de registratie van gebruikers-id's bij transacties betrouwbaar is?

Doordat falende general IT controls afbreuk kunnen doen aan de werking van procesmatige beheersmaatregelen in IT-systemen, vallen er waarborgen weg voor de betrouwbaarheid van de data.

Zoals gezegd, willen we niet alle mogelijk voorbeelden van falende general IT controls en de specifieke risico's benoemen. We gaan nu even uit van een situatie waarin door falende general IT controls de procesmatige beheersmaatregelen niet effectief kunnen worden getoetst, of helemaal niet zijn getoetst. De vraag is dan in welke mate we bij onze jaarrekeningcontrole toch gebruik kunnen maken van data uit de systemen van de klant.

Effectieve general IT controls niet per se noodzakelijk

Belangrijk uitgangspunt is dat de principes voor het vaststellen van de betrouwbaarheid van de te controleren data niet anders zijn dan bij traditionele auditwerkzaamheden.

Het gaat om de volgende principes:

- Externe informatie is over het algemeen betrouwbaarder dan interne informatie.
- Naarmate het belang dat we hechten aan de bewijslast groter is, moeten we meer bewijs hebben voor de betrouwbaarheid van de gegevens.
- komen we terug bij de vraag waar de data-analyse voor wordt gebruikt:
- Bij data-analyse als onderdeel van de risico-inschattingswerkzaamheden is over het algemeen begrip van de aard en bron van de data, in combinatie met interviews voldoende.
- Bij data-analyse als onderdeel van het toetsen van interne beheersingsmaatregelen zijn de reguliere IPE-testrichtlijnen[2] van toepassing.
- Bij data-analyse als onderdeel van gegevensgerichte werkzaamheden zijn eveneens de reguliere IPE-testrichtlijnen van toepassing. Maar als de auditprocedure met behulp van de data de hoofdcomponent vormt om de bewering rondom een account te staven, zijn aanvullende waarnemingen nodig. De aard en omvang hiervan wordt mede bepaald door het risico op een fout van materieel belang (low/medium/high).

In de praktijk betekent dit dat als we data over verkopen willen gebruiken voor gegevensgerichte werkzaamheden, we een combinatie van data-analyses uitvoeren. Voorbeelden zijn cijferanalyses, het onderzoeken van de bronnen van de omzetboekingen, het patroon van de verkoopboekingen en het verband tussen omzetboeking, debiteuren en ontvangst van betalingen. We kunnen de betrouwbaarheid van de hele tabel met verkopen bijvoorbeeld vaststellen door deelwaarnemingen op verkopen in de tabel aan te sluiten met de primaire registratie. Bij voorkeur is dat een externe bron. Voor het aspect 'juistheid' stellen we dan voor elk van een x-aantal verkopen vast dat er een orderbevestiging is, en dat het bijbehorende bedrag is ontvangen. Voor het aspect 'volledigheid' controleren we of voor goederenafgiftes de bijbehorende verkooptransacties zijn geregistreerd. Afhankelijk van de typologie van de onderneming zijn er andere methodes om de volledigheid van

de opbrengsten te controleren en na te gaan of deze juist en volledig in het systeem zijn geregistreerd.

Er zijn geen algemene voorschriften welke aantallen deelwaarnemingen nodig zijn om de betrouwbaarheid van de te analyseren data vast te stellen. In de praktijk zien we dat accountantskantoren hier eigen richtlijnen voor hanteren, veelal gebaseerd op statistische steekproeven.

Als deze deelwaarnemingen geen bijzonderheden aan het licht brengen – voor het beoordelen van afwijkingen hanteren kantoren specifieke richtlijnen – kan de hele dataset van verkopen worden gebruikt voor cijferanalyse. Dit leidt tot de conclusie dat, anders dan vaak wordt aangenomen, effectieve general IT controls niet per se noodzakelijk zijn. Hier komen we later nog op terug.

Natuurlijk kunnen er specifieke general IT controls zijn waar we hoe dan ook op willen steunen, maar dit is geheel afhankelijk van de auditaanpak. Stel, we willen de bewering van het management toetsen dat het management nooit handmatige boekingen in het financiële systeem maakt. Dan is het wellicht nodig de authenticiteit van gebruikers te toetsen en het risico op *management override* na te gaan.

Een andere belangrijke vraag is de impact van falende general IT controls in organisaties/toepassingen waar we te maken hebben met primaire vastleggingen (denk aan de telecomproviders met geregistreerde verbruikstikken of energieleveranciers met registratie van kilowatturen en kubieke meters). Dan is wellicht de betrouwbaarheid alleen vast te stellen door de beheersmaatregelen in en rondom de betrokken IT-systemen te toetsen.

Als de effectieve werking van de general IT controls niet is vast te stellen, kan de auditor niet vertrouwen op de werking van de application controls. Dan valt een geheel andere, arbeidsintensievere aanpak te overwegen. Dit probleem wordt minder groot als het mogelijk is de primaire registratie aan te sluiten met externe bronnen. Bij de energieleverancier kun je de betrouwbaarheid van de meterstanden bijvoorbeeld proberen vast te stellen door aansluiting te zoeken met de meetgegevens van de netbeheerder.

Hebben general IT controls dan geen toegevoegde waarde?

Als in specifieke situaties, zoals eerder geschetst, effectieve general IT controls geen randvoorwaarde voor onze controle zijn, kunnen we dan concluderen dat general IT controls in die gevallen geen toegevoegde waarde hebben? Zo kunnen we dat niet stellen. Onze controlewerkzaamheden kijken terug in de tijd. Maar een organisatie heeft er belang bij om fouten in de gegevensverwerking te voorkomen of tijdig te signaleren. Een data-analyse achteraf draagt daar niet veel aan bij. Daarom is de toegevoegde waarde van general IT controls niet in de laatste plaats groot voor de organisatie zelf. Ook belangrijk om in gedachten te houden dat de accountant als onderdeel van de planningsfase van de audit een evaluatie dient uit te voeren van de IT-omgeving, IT-processen en welke rol IT heeft in de voor de accountant belangrijkste bedrijfsprocessen. Het doel hiervan is IT-risico's te identificeren en te evalueren of deze mogelijk van materieel belang zijn voor de controle van de jaarrekening en wat de accountant hiermee zal doen in de controleaanpak.

General IT controls moeten dus zeker niet aan de kant worden geschoven en de accountant en IT-auditor moeten bij het management het belang van goed functionerende general IT controls blijvend onderstrepen.

Conclusie

In dit artikel hebben we stapsgewijs op hoofdlijnen de aandachtspunten besproken bij het toepassen van een datagedreven auditaanpak en de impact van de general IT controls. Samengevat formuleren we twee uitgangspunten om te bepalen of je voldoende kunt vertrouwen op de data in de systemen om data-analyse te kunnen toepassen. Bedenk daarbij steeds dat het onder sommige omstandigheden anders zou kunnen zijn.

Uitgangspunt 1. Effectieve general IT controls zijn minder een noodzakelijke randvoorwaarde voor data-analyse op systemen die een secundaire vastlegging vormen, omdat er in veel gevallen aanvullende werkzaamheden kunnen worden uitgevoerd door een aansluiting te maken met een primaire registratie of een externe bron.

Uitgangspunt 2. Effectieve general IT controls zijn van groter belang voor data-analyse bij primaire registraties, of als er geen matching mogelijk is met externe bronnen.

Tot slot willen wij benadrukken dat de conclusies over de kwaliteit van de data en de keuze voor een aanpak verschillend kunnen zijn per gegevensstroom of per post in de jaarrekening. Trek dus niet te snel een overall conclusie, maar evalueer de noodzaak voor het testen van general IT controls en de mogelijke impact van niet-effectieve general IT controls per specifieke gegevensstroom of per post en aan de hand van de doelstelling van de specifieke data-analyse.

We sluiten af met te benadrukken dat de toegevoegde waarde van general IT controls niet in de laatste plaats groot is voor de organisatie zelf (zie tekstkader 'Hebben general IT controls dan geen toegevoegde waarde?'). Een organisatie heeft er immers zelf belang bij om fouten in de gegevensverwerking te voorkomen of tijdig te signaleren. General IT controls moeten dus zeker niet aan de kant worden geschoven en de accountant en IT-auditor moeten bij het management het belang van goed functionerende general IT controls blijvend onderstrepen.

Noten

[1] Opgemerkt dient te worden dat zorgvuldigheid geboden is om de werking van beheersmaatregelen effectief te verklaren op basis van gegevensgerichte werkzaamheden op transactieniveau. Echter, hiermee kan wel worden vastgesteld of transacties binnen de grenzen van interne beheersmaatregelen zijn gebleven.

[2] IPE: Information Produced by the Entity. Dit betreft informatie die wordt aangeleverd door de gecontroleerde partij als controlebewijs en die wordt gebruikt voor controls testing of gegevensgerichte werkzaamheden. Denk bijvoorbeeld aan een ouderdomslijst debiteuren. De controlerend accountant dient zich ervan te overtuigen dat deze informatie juist en volledig is alvorens deze als evidence te kunnen gebruiken.

Dit artikel is een product van de volgende leden van de NOREA-werkgroep IT & Financial Audit: Alex van der Harst, Angelique Koopman, Antoine Lucassen, Dave Jansen, Esther Bastiaanse, Ferry Geertman, Joram Dictus, Marcello Smalbil, Robert Johan, San Emmen, Wout van Kessel.

Alex van der Harst

Linkedin

Angelique Koopman

Linkedin

Antoine Lucassen

Linkedin

Dave Jansen

Linkedin

Esther Bastiaanse

Linkedin

Ferry Geertman

Linkedin

Joram Dictus

Linkedin

Marcello Smalbil

Linkedin

Robert Johan

Linkedin

San Emmen

Wout van Kessel

Linkedin