



Wergroep IT & Financial Audit stelt zich voor

# Samenwerking IT-audit en Financial audit; het is vanzelfsprekend maar gaat niet vanzelf

8 december 2020

**Dát een naadloze samenwerking tussen IT-audit en financial audit pure noodzaak is, daarover bestaat geen discussie. En toch gaat het nog niet altijd goed en halen we niet altijd het maximale uit de samenwerking. In drie workshops gingen NBA en NOREA samen met enkele tientallen auditors op zoek naar *root causes* en praktische adviezen voor verbetering vanuit de jaarrekeningcontrole gezien. Conclusie: een wederzijdse investering in de samenwerkingsrelatie, zodat aan beide kanten het gevoel ontstaat dat je een volwaardige partner van elkaar bent, verdient zich dubbel en dwars terug.**

In dit artikel geven wij voorbeelden van twee actuele casussen hoe de financial auditor en IT-auditor elkaar versterken.

Uit de praktijk van alledag gegrepen:

- Een IT-auditor die vol enthousiasme en energie de IT-audit heeft uitgevoerd en daarbij diverse bevindingen heeft geconstateerd, maar heeft nagelaten tijdig de financial auditor hiervan op de hoogte te stellen.
- Een auditteam dat gaandeweg ontdekt dat de IT-auditor niet naar functiescheidingen in een ERP-omgeving heeft gekeken – mogelijk vitale zaken voor het verkrijgen van controlezekerheid voor de jaarrekeningcontrole.
- Onduidelijke en/of onvolledige afspraken tussen de financial auditor en de IT-auditor. Hierdoor worden niet alle relevante (IT-)risico's afgedekt of niet de juiste werkzaamheden uitgevoerd die nodig zijn voor het verkrijgen van controlezekerheid voor de jaarrekening.
- De financial auditor en IT-auditor hebben moeite om elkaar het belang en impact van IT op de werkzaamheden van de financial auditor uit te leggen.
- Een financial auditor die zonder aanwezigheid van de IT-auditor een management letter met de CFO/CEO bespreekt, vol wezenlijke IT-verbeterpunten en risico's, waardoor die bevindingen niet de juiste urgentie en diepgang krijgen.
- Een IT-auditor die erachter komt dat hij in een offerte van zijn collega-financial auditor voor tien dagen werk staat zonder dat er overleg over het urenbudget is geweest.
- Een financial auditor die vlak voor afronding van zijn controle erachter komt dat na de interimcontrole geen werk meer is uitgevoerd door de IT-auditor. Er ontbreken dus drie essentiële maanden in de scoping van diens werk.

## Herkenning

We hebben rond dit thema drie workshops georganiseerd. De casuïstiek in deze en andere voorbeelden bleek zeer herkenbaar bij de circa veertig auditors – een mix van IT-auditors en financial auditors vanuit diverse werkomgevingen: accountantskantoren en internal auditororganisaties, groot-klein, diverse sectoren. Er is veel verbeterd in de samenwerking in de afgelopen tien jaar en dat was ook pure noodzaak. Veel organisaties zijn sterk afhankelijk van een (steeds complexer wordend) IT-landschap en alleen een naadloos geïntegreerde aanpak van financial en IT-auditors kan daarin op efficiënte wijze de zekerheid bieden die nodig is voor het afgeven van een controleverklaring. De complexiteit van dat landschap is soms zeer hoog en mede daarom is de gezamenlijk analyse en dialoog met klant erover zo relevant. Ook daarover was in de workshops geen discussie. In een ideale auditwereld is een geïntegreerde manier van werken dan ook de normaalste zaak van de wereld. Helaas is de praktijk weerbarstiger.

## Verschillen

Die ideale wereld bestaat niet. In de kern is dat terug te voeren tot een heel simpele constatering: een IT-auditor is geen financial auditor en omgekeerd. Ze hebben ieder hun specialismen die een verschillend beeld van de problematiek kunnen geven, en waarmee ze elkaar juist kunnen versterken.

De verschillen uiten zich op diverse manieren.

Ten eerste natuurlijk in de kennis. IT-auditors zijn geschoold en ervaren op het vlak van (beheersing van risico's binnen) IT, een onderwerp waarin financial auditors minder thuis zijn. Omgekeerd zijn financial auditors vanzelfsprekend helemaal thuis in de controle van de jaarrekening, en dat is niet een onderwerp waar de IT-auditor alle details van beheerst.

Ten tweede in de wijze waarop ze bepalen welke werkzaamheden er nodig zijn om goed zicht te krijgen op bestaan en werking van bepaalde controls binnen de IT – de scoping van werkzaamheden. Een financial auditor redeneert bij die scoping primair vanuit de risico's op fouten in de informatie die leidt tot de jaarrekening; de IT-auditor redeneert van nature (ook) vaak vanuit andere risico's – zoals informatiebeveiliging en continuïteit, die breder zijn dan risico's voor de financiële gegevensverwerking alleen.

Ten derde in de werkplanning en -routines. Het aantal IT-audituren bij jaarrekeningcontroles is een onderdeel van de totale hoeveelheid uren, waarbij in een korte periode de IT-auditors betrokken zijn bij een groot aantal opdrachten. Deze logistieke uitdaging heeft vaak meer impact op de samenwerking dan velen denken. Als de inzet van de IT-auditors bijvoorbeeld niet tijdig of onrealistisch wordt gepland komt de uitvoering van het werk al snel onder druk te staan.

## Communicatie

Goed omgaan met deze verschillen vergt drie zaken: communicatie, communicatie en communicatie. Dat mag dan een open deur van jewelste zijn, er blijkt op dat punt nog veel ruimte voor verbetering te zijn. Meer specifiek noemen we de volgende thema's rond communicatie waar verbetering nodig is.

**Hoe eerder, hoe beter.** Juist in de planning en voorbereiding van een controle is het zaak om verwachtingen en richting van de controleaanpak duidelijk uit te wisselen. Het team dient gezamenlijk na te denken over de controledoelstellingen, de risico's en de vertaling naar het controleplan. Door samen aan de risicoanalyse te werken wordt deze niet alleen beter, maar wordt ook voorkomen dat er gaandeweg het controleproces verrassingen ontstaan door verschillende zienswijzen over de aanpak. Kortom, in de planningsfase moeten de financial auditor en de IT-auditor samen aan de slag.

**Niet uitbesteden, maar samenwerken.** De neiging bestaat nog wel eens om een IT-auditor als een subcontractor te zien. Het resultaat is dat er dan geen gezamenlijkheid ontstaat. Beter is het om, ook op senior niveau, gelijkwaardigheid in het team te laten zien. Het onderling uitwisselen van activiteiten in de controle kan daaraan bijdragen en bovendien het werk voor beide partijen uitdagend en leerzaam houden. Zoek elkaar op vanaf de planningsfase en zorg voor een gezamenlijke risicoanalyse. Kortom, de IT-auditor en financial auditor zijn gedurende de hele jaarrekeningcontrole sparringpartners op het snijvlak van IT en de financial audit.

**Nieuwsgierig zijn naar elkaars werelden.** Als een financial auditor onvoldoende kennis van IT(-controls) heeft, kan die geneigd zijn dat stuk van de controle over te laten aan een specialist. Maar de financial auditor kan ook nieuwsgierig zijn om het beter in de vingers te krijgen, en omgekeerd. Met elkaar meelopen dus, dat werkt vaak beter. Een mooi neveneffect ervan is dat de financial auditor en IT-auditor worden geprikkeld om in klare taal (zonder jargon) hun bevindingen uit te leggen en te vertalen in risico's en onzekerheden, zodat het ook voor de klant goed te begrijpen is. Dat is pure winst, want dat is ook in de relatie met de klant essentieel.

**Samenwerken is emotie.** In elke samenwerking komen lastige zaken of verrassingen voor en de auditwereld is daar zeker niet uniek in. Die lastige zaken of verrassingen kun je beter aan als de relatie goed is. De bereidheid om the *extra mile* te gaan komt immers niet voort uit ratio maar uit emotie. Auditors die actief inzetten op meer teamgeest en *bonding* tussen de verschillende 'bloedgroepen' zullen dat dus rijkelijk terugverdienen in de vorm van een betere samenwerking.

## Quick wins

Uit de discussies tussen de deelnemers kwamen de volgende quick wins naar voren.

### Zet in op persoonlijk contact

Doemt er een probleempje op? Hoeveel moeite is het dan om even (virtueel) langs te lopen in plaats van het over de schutting te gooien in een mail? Kleine moeite, groot plezier.

### Stem klantbezoeken af

Plan je een klantbezoek in? Probeer het zodanig te plannen dat IT-auditor en financial auditor er tegelijkertijd zijn. Dat is niet alleen goed voor de samenwerking, maar geeft ook de klant een onmiskenbaar signaal over de geïntegreerde werkwijze.

### Stel je kwetsbaar en nieuwsgierig op; wees concreet

Begrijp je als IT-auditor niet goed waar de financial auditor zich op richt? Of snap je als financial auditor niet wat nu exact de aanpak van de IT-auditor is? Durf je kwetsbaar op te stellen door dit aan te geven. Vraag waarom en hoe bepaalde werkzaamheden bijdragen aan de doelstelling van de audit. Mensen blijken dan heel bereidwillig om de helpende hand toe te steken. Wees hierbij zo concreet mogelijk; bespreek gewoon wat je precies van elkaar wilt weten om te kunnen vertrouwen op de IT-omgeving van de klant. Start bij welk risico je precies onderkent en welke vraag je daarbij beantwoord wilt zien.

## Actuele voorbeelden

In de volgende twee voorbeelden laten we zien hoe financial auditors en IT-auditors samenwerken in een complexe omgeving. De conclusies die uit deze voorbeelden naar voren komen zijn het resultaat van twee workshops die NBA samen met NOREA heeft gehouden over de onderwerpen *blockchain* en *agile*. De deelnemers aan de workshops waren financial auditors, IT-auditors en materiedeskundigen.

### Blockchain

Blockchain, een complexe en relatief jonge technologie, stond centraal tijdens een event van het NBA en NOREA. Circa twintig financial auditors, IT-auditors en blockchainspecialisten van verschillende organisaties kwamen samen onder het motto 'Together is better' om met elkaar in gesprek te gaan over de impact van blockchaintechnologie op het vakgebied en de werkzaamheden van de auditor. Enkele voorbeelden van vragen die centraal stonden tijdens dit event waren:

- *Hoe controleer je als auditor een organisatie waarbij een of meerdere processen worden ondersteund met blockchaintechnologie?*
- *Met welke mate van diepgang moet je een blockchain auditen?*

Het uiteindelijke doel was om met elkaar te brainstormen over risico's en impact van het gebruik van blockchain voor een audit en de gevolgen hiervoor voor de controleaanpak.

Conclusie is dat er bij blockchain diverse sterke controlemiddelen zijn. Bijvoorbeeld verbandscontroles, die maken dat met een goede mix van controletechnieken gegevensgericht controleren om een blockchain heen nog steeds mogelijk is.

Wenselijk is echter om een combinatie van technieken te gebruiken waarbij diepgaand inzicht wordt verkregen in de opzet, bestaan en werking van de blockchain, smart contracts waarmee wordt gewerkt en de link naar andere bedrijfskritische systemen. De samenwerking tussen financial auditor en IT-auditor is hierbij cruciaal.

Het event werd afgesloten met een discussie over de wijze waarop een auditor verantwoording zou moeten afleggen. Conclusie was dat er een redelijke kans is dat het maatschappelijke verkeer in de toekomst een soort van nieuwe NV COS-standaard verwacht. Gedacht werd aan standaarden rond blockchain audits waarbij een IT-auditor assurance geeft via met ISAE vergelijkbare rapporten.

## Agile

De doelstelling van het door NBA en NOREA georganiseerde agile event was de volgende:

- Bijdragen aan een verdergaande integratie van de werkzaamheden van de financial auditor en de IT-auditor.
- Daarmee faciliteren dat beide beroepsgroepen nog beter op elkaar kunnen aansluiten en elkaar aanvullen.

De vraag die in de verschillende discussies centraal stond was: *Past het traditioneel toetsen van de drie general IT controls 'incident-', 'problem-' en 'change management' nog wanneer agile systeemontwikkeling wordt toegepast?*

Aan de hand van een realistische case study van een organisatie die het agile-concept heeft omarmd, werden discussies gevoerd rondom de audit en businessrisico's en de (on)mogelijkheden van een controleaanpak.

Doordat de discussies werden gevoerd tussen de verschillende disciplines werden risico's vanuit verschillende invalshoeken benaderd en duidelijk gedefinieerd, juist om elkaar vanuit de verschillende disciplines uit te leggen wat en waarom er een risico werd geconstateerd.

In de discussies rondom een mogelijke controleaanpak kwam naar voren dat ten aanzien van de traditionele aanpak (preventieve en formalistische controls) in een agile-omgeving veel meer gesteund zal gaan worden op detectieve controls en ook dat er een verschuiving is te verwachten van hard controls naar soft controls.

## Ten slotte

Ons pleidooi voor intensievere samenwerking hebben wij afgesloten met twee actuele voorbeelden hoe de financial auditor en IT-auditor elkaar kunnen versterken. Deze voorbeelden zijn tijdens drie interactieve sessies met IT-auditors, financial auditors en materiedeskundigen besproken. De afdrank is dat een naadloze samenwerking tussen IT-audit en financial audit pure noodzaak is, daarover bestaat geen discussie. We gingen met enkele tientallen auditors op zoek naar root causes en praktische adviezen voor verbetering van de samenwerking in de context van de jaarrekeningcontrole. Wat blijkt? We halen nog niet altijd het maximale uit de samenwerking. De conclusie uit de sessies over blockchain en agile, waarbij vertegenwoordigers van NBA en NOREA op zoek gingen naar antwoorden luidt: laat zien en voelen dat je een volwaardige partner bent van elkaar. Een wederzijdse investering in de samenwerkingsrelatie verdient zich dubbel en dwars terug. Dat is tweerichtingsverkeer!

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