Rapporteren over cultuur en gedrag vergroot vertrouwen bij uitbesteding

Soft controls en ISAE 3402

Veel organisaties hebben bedrijfskritieke processen uitbesteed aan serviceorganisaties. Via ISAE 3402-rapportages leggen veel serviceorganisaties verantwoording af over de kwaliteit van hun interne beheersing. De interne beheersing omvat de combinatie van zogenaamde hard controls, zoals autorisaties, functiescheiding en geautomatiseerde controls, en cultuur en gedrag binnen de organisatie (soft controls). Soft controls zijn daarbij een belangrijk fundament en randvoorwaardelijk voor de uitvoering van hard controls. Niet-effectieve hard controls zijn veelal ook het gevolg van tekortkomingen in soft controls. Het rapporteren over soft controls door serviceorganisaties is echter nog erg beperkt. In onze ervaring zorgt dit voor spanning op de vertrouwensrelatie tussen de uitbestedende organisatie en de serviceorganisatie. Door te rapporteren over soft controls kan het onderlinge vertrouwen worden versterkt en zijn beide organisaties beter 'in control'. In dit artikel geven we concrete voorbeelden van de wijze waarop dit kan worden uitgevoerd.

Laura Ploegsma
is senior consultant bij KPMG Advisory – Governance, Risk & Compliance Services.

Corine Tol
is senior manager bij KPMG Advisory – Governance, Risk & Compliance Services.

Jacco van Kleef
is partner bij KPMG IT Assurance & Advisory.

UITBESTEDING ONTSLAAT NIET VAN VERANTWOORDELIJKHEID

Van organisaties wordt verwacht dat zij aantoonbaar 'in control' zijn van hun bedrijfsvoering. Dit omvat ook activiteiten die zij hebben uitbesteed aan andere partijen (zogenaamde serviceorganisaties). Hoe vaak lees je echter niet over datalekken, fraudes of andere incidenten in de keten van bedrijfsvoering? Ondanks veelal in opzet effectieve hard controls, gaat het toch mis. Evaluaties hiervan laten zien dat de oorzaak hiervan vaak te vinden is in de kwaliteit van soft controls in de uitbestedende organisatie of de serviceorganisatie. Dit pleit ervoor dat deze partijen meer aandacht besteden aan soft controls.

VERANTWOORDING OVER UITBESTEDING RAAKT VOORAL NOG DE HARD CONTROLS

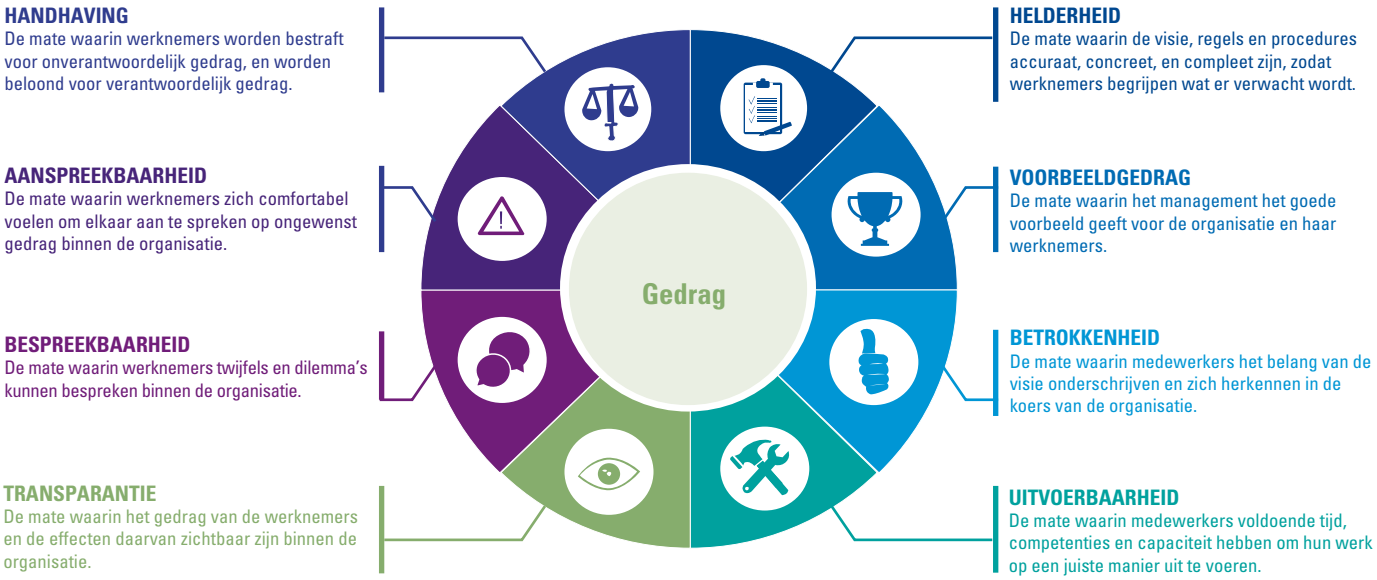
Het is gebruikelijk dat serviceorganisaties verantwoording afleggen over de kwaliteit van hun interne beheersing via International Standard for Assurance Engagements 3402-rapporten (hierna: 'ISAE 3402-rapporten').[1] In deze rapporten wordt de interne beheersing van de organisatie door een onafhankelijk accountant getoetst.

In de meeste ISAE 3402-rapporten van serviceorganisaties ligt de focus echter op hard controls. Er wordt weinig tot geen aandacht geschonken aan het gedrag van de mens, dat over het algemeen het fundament vormt en randvoorwaardelijk is voor de effectiviteit van de harde beheersingsmaatregelen. Dit is opmerkelijk, vandaar dit visiestuk op de verantwoording over soft controls in ISAE 3402-rapporten.

Het belang van cultuur en gedrag wordt inmiddels ook onderkend in Handreiking 1148 ([NBA22]) van de Nederlandse Beroepsorganisatie voor Accountants (NBA). Deze handreiking roept op om meer aandacht te schenken aan cultuur en gedrag in jaarrekeningcontroles en andere werkvelden van de accountant waar de effectiviteit van de interne beheersing relevant is. Omdat serviceorganisaties in een ISAE-rapport verantwoording afleggen aan hun gebruikers over hun interne beheersing, en om de waarde van de rapporten voor hun gebruikers te vergroten, pleiten wij ervoor dat cultuur en gedrag ook in deze rapporten prominenter aandacht krijgen. Dit sluit aan op het vereiste in een ISAE 3402-rapport waarin aandacht wordt gevraagd voor (andere) aspecten van de beheersingsomgeving van de serviceorganisatie ([NBA16][2]; zie ook de vergelijkbare NOREA-richtlijn 3402: [NORE16]). De vraag is op welke wijze en waar cultuur en gedrag in een ISAE 3402-rapport kunnen terugkomen.

1 Of andere serviceorganisatie-controleopdrachten waarin interne beheersing wordt getoetst, zoals ISAE 3000 en SOC2/SOC3.

2 NBA Standaard 3402 paragraaf 16 sub 8 ([NBA16]): "Andere aspecten van de beheersingsomgeving van de entiteit, het risico-inschattingsproces, het informatiesysteem (inclusief daarmee verband houdende processen) en communicatie, de beheersingsactiviteiten en de monitoringsbeheersingsmaatregelen die relevant zijn voor de diensten die worden verleend."



Figuur 1. Soft-controls-model van Muel Kaptein.

Voor het concretiseren en meetbaar maken van cultuur en gedrag kan worden gebruikgemaakt van het algemeen aanvaarde soft-controls-model dat is ontwikkeld door Muel Kaptein ([Kapto3]; [Kapt14]) en dat ook door de NBA als uitgangspunt wordt gebruikt in haar handreiking. Voordat we ingaan op de vraag hoe cultuur en gedrag in ISAE-rapporten terug kunnen komen, lichten we in de volgende paragraaf eerst het hiervoor genoemde soft-controls-model toe.

Goed inzicht in soft controls levert samen met de analyse van hard controls een completer beeld op van de interne beheersingsomgeving en de mogelijke effectiviteit van de genomen interne beheersingsmaatregelen. ([NBA22])

GESTRUCTUREERD MODEL VOOR HET ANALYSEREN EN METEN VAN SOFT CONTROLS

In het model van Kaptein zijn soft controls gedefinieerd als acht niet-tastbare gedragsbeïnvloedende factoren in een organisatie die van belang zijn voor het realiseren van de organisatiedoelstellingen. In figuur 1 wordt dit model weergegeven met een uitleg van de acht soft controls.

Wij zien effectieve soft controls als het fundament en als randvoorwaardelijk voor een effectieve werking van hard controls. Het draait dus niet om het vervangen van hard controls door soft controls, maar om het verrijken van het inzicht in de effectiviteit van de interne beheersingsomgeving door de evaluatie van soft controls hier expliciet in mee te nemen.

EFFECTIEVE SOFT CONTROLS DRAGEN BIJ AAN EEN GOEDE INTERNE BEHEERSING

Soft controls zijn weliswaar minder makkelijk meetbaar en kwalificeerbaar, maar zijn wel degelijk van invloed op de effectieve werking van de beheersingsmaatregelen. Onderstaand een aantal voorbeelden die dit laten zien.

Voorbeelden van de relatie tussen hard en soft controls

Voorbeeld 1
Een procuratiehouder heeft als taak betalingen dagelijks goed te keuren. Hij heeft daarnaast meerdere dagelijkse taken en verantwoordelijkheden. De goedkeuring van de betalingen vindt veelal pas aan het einde van de dag plaats. In extreme gevallen komt het dan voor dat deze medewerker om 11 uur 's avonds nog betalingen goedkeurt.

Er is dus sprake van een minder effectieve soft control, namelijk een te lage uitvoerbaarheid. De kans bestaat dat de kwaliteit van d uitvoering van deze betalingen negatief wordt beïnvloed door het gebrek aan tijd. Ondanks dat de hard control lijkt te werken, wordt de kans op onterechte betalingen groter.

Voorbeeld 2
Een procesbeschrijving met hierin de stappen die door een medewerker moeten worden uitgevoerd, kan goed werken om de helderheid en uitvoerbaarheid voor deze medewerker te vergroten. In de praktijk kan zo'n procesbeschrijving echter als inconsistent en daarmee als onvoldoende helder worden ervaren, waardoor de procedure in het proces niet door elke medewerker op dezelfde wijze wordt uitgevoerd.

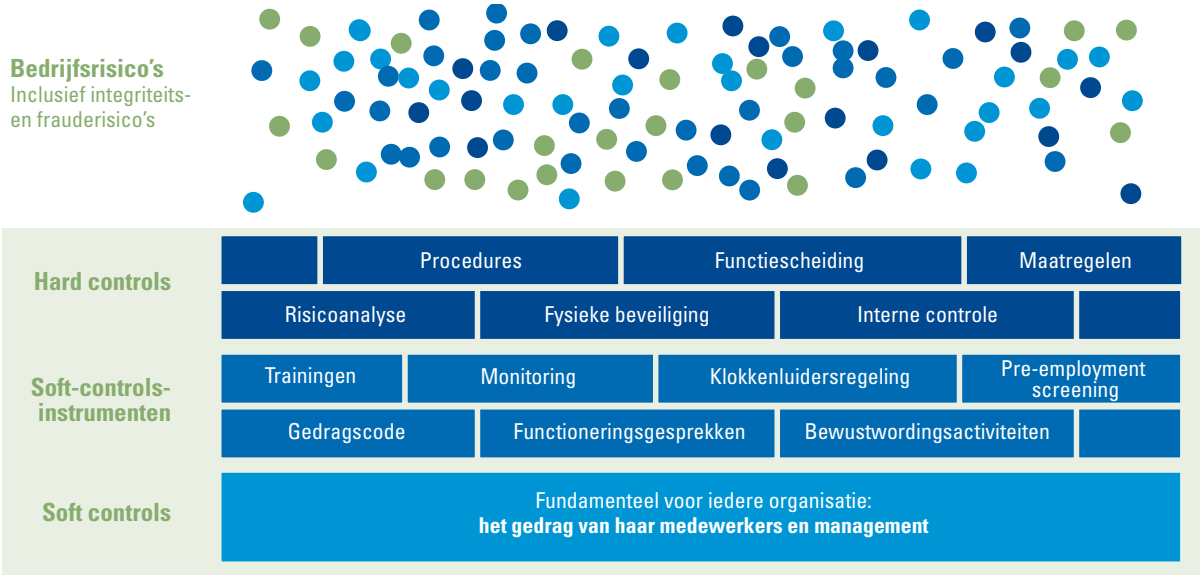
De relatie tussen hard en soft controls geven we in figuur 2 schematisch weer. Soft controls worden hier als het fundament getoond voor effectieve harde beheersingsmaatregelen. De soft-controls-instrumenten in de figuur zijn voorbeelden van middelen die kunnen worden ingezet om soft controls effectiever te laten zijn.
Door oog te hebben voor soft controls in de uitvoering van – en het rapporteren over – de interne beheersing kan een serviceorganisatie aan de klanten van haar dienstverlening een completer beeld geven van haar beheersing. Dit draagt bij aan de preventieve kant, door te zorgen voor de juiste omstandigheden voor de uitvoering van hard controls. Daarnaast draagt het ook in detectieve zin bij, door bij bevindingen aandacht te schenken aan de context waarin constateringen worden gedaan. Een paar voorbeelden:

- Mogen fouten worden gemaakt?
- In welke mate wordt er geleerd van incidenten die plaatsvinden?
- In welke mate worden medewerkers in staat gesteld hun werk goed uit te voeren, waardoor de kans op fouten afneemt?

Het soft-controls-model is heel effectief om het 'waarom' van bevindingen te analyseren en de root cause te identificeren. Het identificeren van de root cause leidt tot duurzamere oplossingen en daarmee tot een structureel betere interne beheersing. Dit draagt bij aan meer onderling vertrouwen tussen de serviceorganisatie en haar klant. Zij zijn zo aantoonbaar beter 'in control' van de processen.[3]

3 Zie ook voorbeelden van de relatie tussen soft controls en IT general controls in [Bast15].

Figuur 2. De relatie tussen hard en soft controls.



SUGGESTIES VOOR SOFT CONTROLS IN EEN ISAE 3402-RAPPORT

Wanneer een organisatie risico's identificeert, worden (harde) interne controlemaatregelen geïmplementeerd om de risico's te beheersen. In een ISAE 3402-rapport worden deze vervolgens getest op hun effectieve werking. Een ISAE 3402-rapport bestaat grofweg uit twee onderdelen: de beschrijving van de serviceorganisatie en het hoofdstuk met de beheersingsdoelstellingen, de gerelateerde beheersingsmaatregelen en de bevindingen van de auditor naar aanleiding van de testwerkzaamheden. Hierna geven we een aantal suggesties hoe soft controls in deze twee onderdelen van een ISAE-rapport kunnen worden opgenomen.

Soft controls in de beschrijving van de serviceorganisatie

In de beschrijving van de serviceorganisatie zien we in de praktijk dat een aantal soft-controls-instrumenten worden benoemd (zoals een gedragscode, personeelsbeleid, regelingen rondom integriteit of klokkenluidersregelingen). In onze visie zou je als organisatie niet alleen het instrumentarium moeten toelichten dat wordt gebruikt om op cultuur en gedrag te sturen, maar juist de kwaliteit en effectiviteit van dit instrumentarium. Denk hierbij bijvoorbeeld aan de uitkomsten van een jaarlijks medewerkerstevredenheidsonderzoek. Het gaat er hierbij niet om dat er een onderzoek is, maar dat bijvoorbeeld uit het onderzoek blijkt dat het merendeel van de medewerkers onduidelijkheid ervaart in wat van hen verwacht wordt. Een dergelijke uitkomst geeft context aan bevindingen op de interne beheersingsmaatregelen.

Een goed voorbeeld van hoe je reflecteert op een instrumentarium is wat ons betreft het jaarverslag 2021 van

Nationale Nederlanden. Hierin wordt bijvoorbeeld op pagina 54 duidelijk beschrijven hoe zij hun waarden en normen monitoren en levend houden in het kader van hun 'Living our Values'-programma ([NN22]).

Zoals hiervoor al benoemd, zijn soft controls ook heel effectief voor root-cause-analyses. In de beschrijving van de serviceorganisaties kan bijvoorbeeld worden uitgelegd in hoeverre root-cause-analyses worden uitgevoerd, inclusief een omschrijving van wat deze analyse omvat, wat de resultaten hiervan zijn en wat de ondernomen acties zijn. Dit zou bijvoorbeeld met de volgende tekst kunnen worden gerealiseerd:

Om meer inzicht te krijgen in onze cultuur voert de organisatie een aantal keer per jaar een root-cause-analyse uit op incidenten waarvan de omvang van de gevolgen voor de organisatie belangrijk is en op bevindingen waar meerdere organisatieonderdelen bij betrokken zijn. De root-cause-analyses worden uitgevoerd door een speciaal daarvoor gevormd team en worden voornamelijk uitgevoerd op basis van interviews met betrokkenen.

De analyses van het afgelopen jaar laten zien dat vooral de kwaliteit van de soft controls 'helderheid' en 'bespreekbaarheid' aandacht vroegen: diverse medewerkers hadden onvoldoende helderheid over hun rol en verantwoordelijkheden en voelden zich niet comfortabel genoeg om hierover vragen te stellen. In reactie hierop heeft de organisatie taken en verantwoordelijkheden duidelijker omschreven en gecommuniceerd. Daarnaast zijn verschillende intervisiesessies georganiseerd om de bespreekbaarheid te vergroten.

Soft controls in het hoofdstuk over de beheersingsdoelstellingen

Ook in het tweede deel van het rapport, het hoofdstuk over de beheersingsdoelstellingen, kunnen soft controls worden geïntegreerd. Het is gebruikelijk in dit hoofdstuk gesignaleerde bevindingen van de auditor te voorzien van managementcommentaar, veelal als bijlage in het rapport.

In de praktijk zien wij vaak managementreacties die gaan over de harde component van een control, bijvoorbeeld: *'Wij onderkennen de bevinding van de accountant en hebben de procedure voor komend jaar aangepast.'* Positief hieraan is dat de bevinding wordt erkend door het management en dat er actie op wordt ondernomen. Het commentaar bevat echter geen reflectie op de context van de bevinding, zoals een antwoord op de vragen waarom er überhaupt sprake was van een bevinding en hoe de organisatie hiervan heeft geleerd. Een voorbeeld van een sterkere reactie is wat ons betreft:

'Wij erkennen dat deze control niet effectief is geweest. Direct na constatering hebben wij de oorzaak hiervan onderzocht. Voor de uitvoerder van de beheersingsmaatregel waren het doel en de wijze van deze control onvoldoende helder, waardoor in augustus de control niet goed is uitgevoerd. Bij de ontwikkeling van het beleid had geen afstemming plaatsgevonden met de medewerkers die hieraan uitvoering moesten geven. De taal van het beleid sloot hierdoor niet aan op de belevingswereld van de uitvoerder. Wij hebben het werkproces rondom deze control vereenvoudigd en met de medewerkers op de afdeling besproken. Bij de totstandkoming van nieuw beleid is de afstemming met de uitvoerders nu in het proces opgenomen. Wij verwachten dat de maatregel hierdoor ook komend jaar effectief uitgevoerd kan worden.'

EEN STAP VERDER MET SOFT CONTROLS ALS ONDERDEEL VAN HET CONTROLERAAMWERK

Door het laatste voorbeeld komt de vraag op of soft controls ook onderdeel kunnen zijn van de interne beheersingsmaatregelen in het controleraamwerk waarop de auditor zijn testwerkzaamheden uitvoert. In onze optiek zou dit op twee manieren kunnen:

- Ten eerste kun je specifieke gedragsrisico's koppelen aan een beheersingsdoelstelling. Vanuit dit gedragsrisico kan worden aangegeven op welke wijze soft controls de effectieve werking van de hard controls ondersteunen.
  Als voorbeeld: een harde beheersingsmaatregel die omschrijft dat een manager een declaratie moet goedkeuren, is pas effectief op het moment dat die manager met de juiste kennis daadwerkelijk vaststelt dat de declaratie voldoet aan alle voorwaarden die eraan gesteld zijn. De manager moet zich hier verantwoordelijk voor voelen, het moet duidelijk zijn wat er van de manager verwacht wordt en de manager moet hier voldoende tijd voor hebben.
  Wat ons betreft is de lastigheid hierbij met name de aantoonbaarheid van soft controls. Een ISAE 3402-onderzoek is erop gericht om een redelijke mate van zekerheid te geven over de effectieve werking van de interne beheersing. Dit vraagt om hoogwaardige documentatie en controles. Bij de meeste organisaties is de aantoonbaarheid van soft controls nog niet op het niveau om hier iets met een redelijke mate van zekerheid over te zeggen. Daarnaast is het ook moeilijk om voor een specifieke periode aan te tonen dat de soft controls effectief waren.
- Een tweede manier om soft controls op te nemen in het controleraamwerk, eentje die makkelijker toe-

pasbaar is, is door een harde beheersingsmaatregel op te nemen op het gebied van cultuur. Denk hierbij bijvoorbeeld aan het jaarlijks uitvoeren van een risicobewustzijnsonderzoek waarbij je bij controleigenaren meet in hoeverre de soft controls ondersteunend of belemmerend zijn als het gaat om effectieve risicobeheersing, en hier vervolgens actiepunten op formuleert.

CONCREET AAN DE SLAG MET SOFT CONTROLS

Hiervoor hebben we geschetst hoe een serviceorganisatie in haar ISAE 3402-rapport zou kunnen beginnen met het rapporteren over soft controls: het beschrijven van soft controls, het integreren van soft controls in managementreacties en het uitvoeren van root-cause-analyses van soft controls als onderdeel van het controleraamwerk.

Om structureel te kunnen rapporteren over soft controls in de interne beheersing en hier als organisatie actief mee bezig te zijn, zou het volgende stappenplan kunnen worden gevolgd:

- Soft controls beginnen bij het management. De eerste stap is het creëren van draagvlak bij het management van de serviceorganisatie: staat het management hiervoor open? Is het bereid zich kwetsbaar op te stellen?
- Het gefaseerd opleiden van de organisatie op het gebied van soft controls. Dit zorgt ervoor dat mensen in de organisatie dezelfde taal gaan spreken als het gaat om cultuur en gedrag. Een goede route hiervoor is te beginnen bij de controleigenaren, compliance en internal audit. Daarna kan als een olievlek worden uitgebreid naar de rest van de organisatie.
- Het inrichten van een model voor het analyseren van root causes. Zoals hiervoor geschetst, leidt een goede root-cause-analyse tot een betere interne controle; hiervoor is wel een robuust proces nodig.
- Het uitvoeren van soft-controls-metingen. Bijvoorbeeld door het uitvoeren van een hiervoor al genoemd onderzoek (via vragenlijsten) onder medewerkers die beheersingsmaatregelen uitvoeren. Neem de reflectie van de organisatie op deze resultaten dan ook op in het ISAE 3402-rapport.

CONCLUSIE

Als een organisatie een bedrijfskritiek proces uitbesteedt aan serviceorganisaties, ontslaat dat die organisatie niet van het 'in control' zijn van de uitbestede processen. Aangezien die verantwoordelijkheid veelal wordt ingevuld via ISAE 3402-rapportages, zouden ISAE 3402-rapporten dan wel het volledige beeld moeten geven van de kwaliteit van de interne beheersing. Wij zijn echter van mening dat wanneer er geen aandacht wordt besteed aan soft controls, fundamentele inzichten ontbreken.

Zoals wij aan de hand van voorbeelden in dit artikel hebben geïllustreerd, kun je in onze optiek namelijk niet zeker zijn van de effectiviteit van hard controls als je geen aandacht hebt voor de kwaliteit van soft controls. Daarom pleiten wij ervoor ook te rapporteren over soft controls en zo het onderlinge vertrouwen te versterken, waardoor zowel de uitbestedende organisatie als de serviceorganisatie beter 'in control' is.

Literatuur

[Bast15] Basten A.R.J., Van Bekkum, E. & Kuilman, S.A. (2015). Soft controls: IT General Controls 2.0. *Compact, 2015*(1). Geraadpleegd op: https://www.compact.nl/articles/soft-controls-it-general-controls-2-0/

[Kapt03] Kaptein, M. & Kerklaan, V. (2003). Controlling the 'soft controls'. *Management Control & Accounting, 7*(6), 8-13.

[Kapt14] Kaptein, M. & Vink, H.J. (2014, 13 januari). *The Soft Side of Hard Controls: A Control Coding Theory.* Geraadpleegd op: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2378437

[NBA16] Nederlandse Beroepsorganisatie voor Accountants (2016, januari). *3402 Assurance-rapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie* (paragraaf 16 sub 8). Geraadpleegd op: https://www.nba.nl/tools/hra-2020/?folder=128057

[NBA22] Nederlandse Beroepsorganisatie voor Accountants (NBA) (2022, 8 februari). *NBA-handreiking 1148:* Het verkrijgen van inzicht in soft controls in het kader van de jaarrekeningcontrole. Geraadpleegd op: https://www.nba.nl/nieuws-en-agenda/nieuwsarchief/2022/februari/publicatie-nba-handreiking-over-soft-controls/

[NN22] NN Group (2022, 10 maart). *Serving customers in times of change: 2021 Annual Report* (p. 54). Geraadpleegd op: https://www.nn-group.com/nn-group/file?uuid=fe0ed772-850a-4697-95e5-06a1fe376e0f&owner=84c25534-c28a-4a64-9c78-5cc1388e4766&contentid=11805

[NORE16] NOREA (2016, 14 december). *NOREA Richtlijn 3402: Assurance-rapporten betreffende internebeheersingsmaatregelen bij een serviceorganisatie.* Geraadpleegd op: https://www.norea.nl/uploads/bfile/8973467d-2cb8-4167-be90-523eacab1282

Over de auteurs

Laura Ploegsma is senior consultant bij KPMG Advisory – Governance, Risk & Compliance Services. Zij ondersteunt organisaties bij het uitvoeren van assuranceopdrachten (ISAE 3402) en soft control assessments en bij het inbedden van soft controls in het risicodomein.

Corine Tol is senior manager bij KPMG Advisory – Governance, Risk & Compliance Services. Zij ondersteunt allerlei organisaties bij het inbedden van soft controls in hun volledige risicodomein, zoals internal audit, ORM en compliance.

Jacco van Kleef is partner bij KPMG IT IT Assurance & Advisory. In zijn rol als financieel auditor en IT-auditor helpt hij klanten bij jaarrekeningcontroles en assuranceopdrachten (ISAE 3000/3402).