Discussiedocument

Continuous Assurance

November 2015

NBA

Opdrachtgever:
Ledengroep Intern en Overheidsaccountants (LIO) van de NBA.

Eindverantwoordelijk bestuurslid:
Ingrid Doerga

1 | Inleiding

1.1 Internal audit en continuous assurance

Internal audit functie (IAF) vervult een belangrijke rol in het governance model van veel organisaties. Een rol die op vele manieren wordt ingevuld, van strategisch tot operationeel. Ongeacht de invulling wordt het bestaansrecht van de IAF vaak bevestigd bij (het signaleren van) falend risk management, fraudes of imperfecties in operationele processen. Het gebruik van *data*- en *process mining* hierbij zal ook in de komende jaren toenemen. De verwachting is dat onderwerpen als *big data* en *predictive analytics* ook een effect gaan hebben op de wijze waarop ondernemingen interne beheersing invullen. Ontwikkelingen die de IAF dus niet kunnen ontgaan.

Wat *continuous assurance* precies inhoudt en hoe het zich verhoudt tot *continuous monitoring* en *continuous auditing*, is niet altijd evident. Duidelijk is wel dat elke organisatie op een of andere manier gebruik zal maken van *continuous monitoring* bij de toepassing van haar risk management en internal control functie. Dit zal het toepassen van continuous auditing faciliteren, waardoor de basis voor continuous assurance is gelegd. Met dit document wil LIO[1] haar bijdrage leveren aan de discussie over Continuous Assurance.

1.2 Definities

Er zijn verschillende definities en vele meningen over wat continuous monitoring (CM) en continuous audit (CAu) nu eigenlijk betekent. Bepaalde kernelementen komen bij beide terug:

- het gaat om data en controles;
- de methode is hoog-geautomatiseerd; en
- de frequentie is hoger en/of continue en/of de intervallen zijn gestandaardiseerd.

De uitvoerder is bij beide vormen anders: voor CM is de business of het management de gebruiker, bij CAu de auditor. De definities van IIA's Global Technology Audit Guide (GTAC) 3 voor de termen CM, CAu en Continuous Assurance (CAss) sluiten aan op deze kernelementen:

Continuous monitoring (CM) zijn processen die het management implementeert om ervoor te zorgen dat het beleid, procedures, en primaire processen doelmatig functioneren. De termen *continuous risk monitoring* en *continuous control monitoring* worden in deze context ook vaak gebruikt. Uit de latere tekst van GTAC 3 en IIA's Practice Advisory 2320-4 kan worden afgeleid dat "on-going" en automatisering hier kernelementen zijn.

1 Met dank aan de leden van de voormalige werkgroep Uiting Continuous Assurance van LIO en IIA Nederland: Elly Stroo Cloeck (projectleider), Eddy van der Geest, Joris Hulstijn, Joris Joppe, Wim van't Einde, Arie Pronk en Luc Jalink.

Continuous auditing (CAu) is een door de auditor gebruikte methode om frequenter geautomatiseerde evaluaties uit te voeren van beheersingsmaatregelen en risico's.

Voor **continuous assurance (CAss)** zijn veel minder definities voorhanden. In het algemeen wordt CAss geïnterpreteerd als de combinatie van CM en CAu. Gesteld kan worden dat CAss de uitkomst is van de combinatie van CM en CAu.

In dit discussiedocument spreken wij over CAss als het gebied dat zowel CM als CAu afdekt.

1.3 Three lines of defence

Een IAF is vaak de plaats waar een stelsel voor het continue monitoren van beheersmaatregelen (het eerst) wordt ingericht. Hierbij kan aansluiting worden gezocht bij het 'three lines of defence' model (IIA 2013) zoals hieronder wordt toegelicht.

1st line: het operationele management

Het operationele management is verantwoordelijk voor de beheersing van de processen die onder haar verantwoordelijkheid worden uitgevoerd. Het management zal continu aandacht moeten hebben voor de risico's binnen hun organisatieonderdeel. Dat betekent dat het management doorlopend risico's (en wijzigingen daarin) signaleert, beoordeelt, beheerst en beperkt. Het stelsel van maatregelen zal door het management regelmatig op effectiviteit moeten worden getoetst. Het management kan hiervoor CM gebruiken.

2nd line: ondersteunende functies

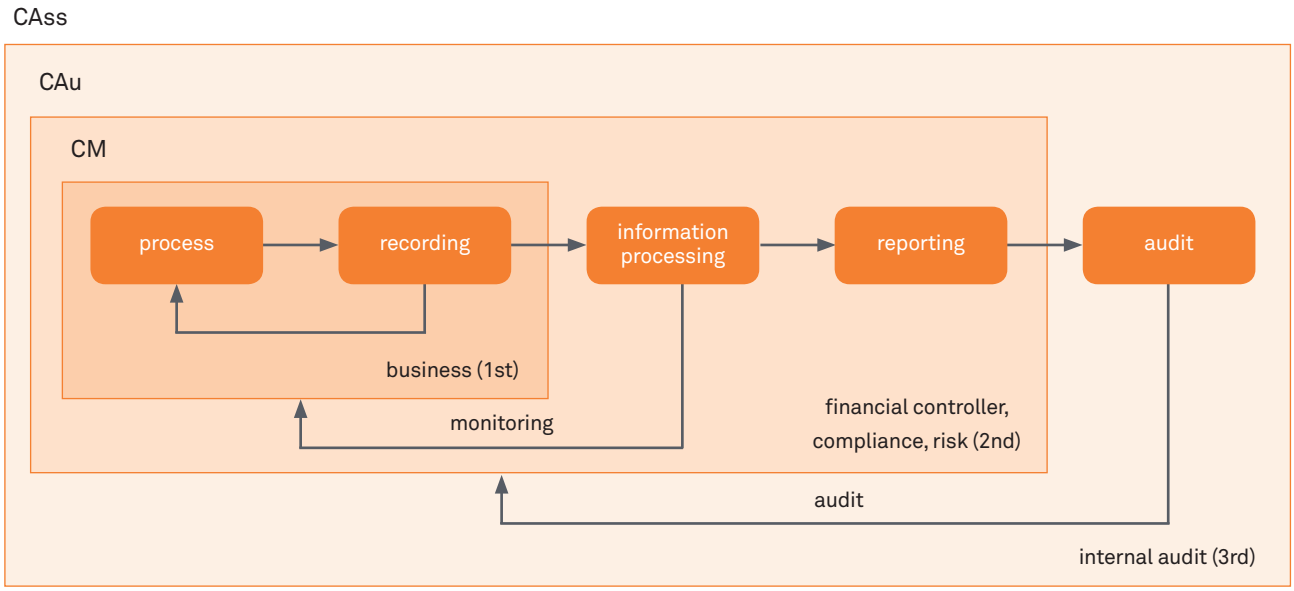
De ondersteunende functies helpen de 1st line met het inrichten van de benodigde beheersingsmaatregelen en eventueel bij het beoordelen ervan. Zij geven vaak kaders en richtlijnen voor hun aandachtsgebied. Deze ondersteunende functies kunnen per organisatie verschillen. Voorbeelden zijn de afdelingen Financiën, Beveiliging, Risicomanagement, Kwaliteit, Interne Controle, (Business) controlling, Compliance en Legal en Juridische zaken.

De 2nd line kan gebruik maken van de resultaten van CM en de opvolging van uitzonderingen door de 1st line, om haar ondersteunende en beoordelende rol in te vullen. Zij kan ook zelf CM implementeren en uitzonderingen laten afhandelen. Het is logisch om te veronderstellen dat de 2nd line haar CM activiteiten projecteert op de wijze waarop de 1st line met interne beheersing om gaat.

3rd line: de Interne Audit Functie (IAF)

De IAF is door haar plaats binnen de organisatie onafhankelijk ten opzichte van de 1st en 2nd line. IAF geeft een oordeel over de effectiviteit van de besturing, het risicomanagement en de interne beheersing. Daarbij maakt IAF gebruik van de (beheers-)activiteiten die in de 1st en 2nd line zijn uitgevoerd. Dit kan betekenen dat het systeem van CM wordt beoordeeld. Als er geen CM is, kunnen CAu activiteiten in de vorm van het (geautomatiseerd en hoogfrequent) testen van controls worden uitgevoerd.

Figuur 1. Overview van de werkzaamheden in een stelsel voor Continuous Assurance



Uitgangspunt is dat risicobeheersingsmaatregelen moeten worden getroffen in drie opeenvolgende lines. De uiteindelijke verantwoordelijkheid voor restrisico's en het niet halen van doelstellingen ligt bij de 'business'. Daar is ook het budget beschikbaar voor investeringen in een betere beheersing.

2 | Implementatie van Continuous Assurance

2.1 Business case

Primaire voorwaarde voor de implementatie van CAss is dat er een heldere business case moet bestaan. Hoewel de techniek beschikbaar kan zijn om op continue basis assurance te verlenen, wil dat niet direct zeggen dat er ook behoefte aan is. Een behoefte voor de implementatie van CAss dient te worden bezien vanuit verschillende perspectieven, zoals stakeholders, management en de behoefte van de IAF om een deel van haar auditaanpak te richten op Continuous Audit.

Bij het opstellen van de business case is het van belang dat de zogenaamde 'cost of control' in ogenschouw wordt genomen. Bepaald moet worden dat de baten en voordelen die het hanteren van CAss (CM + CAu) oplevert ook opwegen tegen de kosten van implementatie en onderhoud.

Voor de kosten moet niet alleen naar de investering en de operationele kosten worden gekeken, maar ook naar de medewerkers. Zijn zij in staat mee te gaan met de nieuwe ontwikkelingen? Is extra training vereist of moeten afdelingen worden aangevuld met andere competenties? Waar ook rekening mee moet worden gehouden is de vraag of de processen van een onderneming wel in voldoende mate zijn toegerust op CAss. CAss impliceert dat frequenter verantwoording wordt afgelegd, waardoor het opvolgen van excepties met een grotere regelmaat zal plaatsvinden.

De baten (kwantitatief) en voordelen (kwalitatief) kunnen zeer divers zijn. In het algemeen geldt dat door het automatiseren van handmatige werkzaamheden de assurance kosten dalen. Een kwalitatief voordeel is dat er een betere en tijdige risicobeheersing of signalering ontstaat waardoor afwijkingen sneller worden gesignaleerd. In totaliteit leidt dit tot een betere beheersing van de organisatie.

2.2 Randvoorwaarden

Ook organisatorische en infrastructurele randvoorwaarden spelen een rol bij de implementatie van CAss. Het succes van CAss is afhankelijk van de bedrijfstypologie, het niveau van de interne beheersing, de betrokkenheid van het management, ruimte voor innovatie en de beschikking over voldoende budget.

Op infrastructureel niveau is het noodzakelijk dat de organisatie beschikt over een hoge mate van automatisering. De verschillende stappen in de processen dienen digitaal te worden geregistreerd. Zonder deze vastleggingen is CAss niet mogelijk. Een ander aspect betreft de data zelf. Zonder een syntactische en semantische standaardisatie van data wordt de implementatie van CAss een onmogelijk project. Ook moet rekening worden gehouden met de frequentie van transacties. Hoe hoger de frequentie, des te meer baat er is bij CAss. Het laatste aspect betreft de datakwaliteit.

Om de betrouwbare werking van CAss te garanderen is het noodzakelijk dat de juiste algemene IT-controls, zoals logische toegangsbeveiliging en change management, aanwezig zijn.

2.3 Capability maturity modellen voor Continuous Assurance

Een hulpmiddel voor het implementeren en het verder ontwikkelen van CAss zijn Capability Maturity Modellen (CMM). Een dergelijke model beschrijft het volwassenheidsniveau van een bepaald object, bijvoorbeeld een systeem, product of proces. Een organisatie is met een CMM in staat om het volwassenheidsniveau van verschillende objecten binnen haar eigen organisatie of tussen andere organisaties te vergelijken. Het is daarmee een goede methode voor het uitvoeren van benchmarks en om de stappen te bepalen hoe een hoger volwassenheidsniveau kan worden behaald.

Relevante maturity modellen voor CAss zijn het IIA Internal Audit Process Maturity model (2011), het Audit Analytic Capability (ACL) model voor CM (2013) en het KPMG volwassenheidsmodel (2013). Deze modellen hebben elk hun eigen aandachtsgebieden. Het IIA Internal Audit Process Maturity model is een zeer breed en uitgewerkt model dat zich richt op meerdere organisatorische aspecten, zoals verbeterprogramma's voor de kwaliteit van assurance, opleidingen, auditplanning, rapporteren en het gebruik van de informatietechnologie binnen de organisatie.

Het ACL model concentreert zich op de randvoorwaarden voor CM, zoals mensen, processen en techniek. Het model tracht de toegevoegde waarde van audit te transformeren van informerend achteraf, naar actueel inzicht en uiteindelijk voorspellend vermogen.

Data analyse en CAu staan centraal in het KPMG volwassenheidsmodel . Met dit model wordt specifiek gekeken naar het niveau van data analyses en de invloed hiervan op het niveau van internal audit, zoals de ontwikkeling van het auditplan, de uitvoering en de rapportage van uitzonderingen.

2.4 Good practices

Hoewel de implementatie van CAss per organisatie zal verschillen, zijn er wel generieke aanbevelingen voor deze implementatie:

- implementeer CM- en CA-tools niet ad hoc, maar op basis van een gedegen voorstel binnen de gehele organisatie. Met andere woorden: zorg dat op operationeel, tactisch en strategisch niveau draagkracht is en dat de veranderingen worden omarmd, ondanks de mogelijke implementatieproblemen;
- ambieer geen volledige omzetting van traditionele interne beheersing naar volledige continue monitoring. Focus op de belangrijkste processen, risico's en controls en op processen die zich daar goed voor lenen;
- zorg voor samenwerking van alle 3 lines of defence en binnen de verschillende functies van de 2nd line. Gebruik IAF en/of Risk Management als katalysator richting de business zodat die zoveel mogelijk werkende CM-oplossingen krijgen aangedragen;
- gebruik pilotprojecten om steun te vergaren en momentum te genereren. Het devies hierbij is om klein te beginnen;
- (her)prioriteer projecten op basis van ervaringen en ontwikkelingen. Blijf kritisch projecten vergelijken met de oorspronkelijke business case om tijdig bij te kunnen sturen;
- verplaats volwassen CA-activiteiten van IAF en/of Risk Management naar de 1st line, en zorg dat de monitoring van de 2nd en 3rd qua techniek en frequentie aansluit op de wijze van CM door de 1st line;
- stel beheersingsmaatregelen op om bij het ontsluiten van de data de exclusiviteit van data te waarborgen.

3 | De toekomst van Continuous Assurance

In het vorige hoofdstuk is ingegaan op de randvoorwaarden voor CAss. Ook is aangegeven op welke manier CAss kan worden geïmplementeerd en zich verder kan ontwikkelen. Maar zal CAss daadwerkelijk een vlucht gaan nemen? Welke factoren zijn hierbij van invloed? In dit hoofdstuk wordt een overzicht gegeven van de trends die van invloed kunnen zijn op de toekomst van CAss en worden enkele stellingen ter discussie voorgelegd.

3.1 De trends

Het is onmogelijk om een complete lijst op te stellen van alle trends die invloed zouden kunnen hebben op het gebruik van CAss. Onderstaande lijst is geenszins limitatief.

- Het toezicht neemt toe, waardoor er sprake is van meer rapportageverplichtingen. De regeldruk neemt toe;
- De noodzaak van het management om op excepties sneller te reageren. De weerbaarheid van de organisatie moet worden vergroot.
- Voor de kwaliteit van de rapportages zal steeds meer worden gesteund op de interne beheersing van bedrijven. Een voorbeeld hiervan is de invoering van Horizontaal Toezicht bij de Belastingdienst;
- Stakeholders willen vaker en diepgaander geïnformeerd worden, niet alleen over resultaten, maar ook over de processen van interne beheersing;
- Nieuwe ICT-ontwikkelingen volgen zich steeds sneller op. Big Data is inmiddels alledaags. Augmented en virtual reality, semantic web en Internet of Things staan op de vooravond om gemeengoed te worden;
- Ketensamenwerking wordt steeds belangrijker. Hierdoor neemt het belang toe van data-standaardisatie, zoals het gebruik van XBRL GL en RGS;
- De behoefte naar de omslag van cyclisch naar dynamisch auditen;
- Het toenemende gebruik van data analytics en process mining tooling, met daarbij de trend dat deze tooling steeds meer functionaliteit krijgt.

3.2 Stellingen voor discussie

Op basis van externe factoren, zoals de maatschappelijke behoefte aan verantwoording, de dynamiek van de omgeving en de technologische ontwikkeling, met daarbij de richting van de interne beheersing en de mate van standaardisatie van tooling, leggen wij u de volgende stellingen voor:

- Door een grote behoefte aan verantwoording neemt CAss sterk toe, eerst bij innovators, later ook bij anderen vanwege kopieergedrag en druk vanuit toezichthouders;
- De toenemende regeldruk leidt er toe dat CAss steeds breder zal worden toegepast.
- Voor een succesvolle implementatie van CAss speelt standaardisatie een grote rol.
- De toepassing van CAss voor interne doeleinden zal vrijwillig toenemen zonder de aanwezigheid van externe druk.
- Alleen in de situatie dat er voldoende wordt geïnvesteerd in de basisvoorwaarden voor een goede beheersing van de organisatie zal de toepassing van CAss slagen.
- De rol van IAF verandert bij toepassing van CAss maar zal niet verdwijnen.

Reacties op deze stellingen en/of dit discussiedocument kunnen gestuurd worden naar de secretaris van het Ledengroepbestuur Intern en Overheidsaccountants (LIO) van de NBA: J.Scheffe RA RO CIA, j.scheffe@nba.nl.

Literatuur

IIA (2011) Internal Audit Process Maturity model

ACL (2011) Audit Analytic Capability Model Whitepaper

IIA (2013). The Three Lines of Defense in Effective Risk Management and Control. IIA Position Papers

IIA (2015) Global Technology Audit Guide (GTAC3)

IIA's Practice Advisory (PA) 2320-4

KPMG (2013) Transforming Internal Audit

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

Antonio Vivaldistraat 2 - 8
1083 HP Amsterdam
Postbus 7984
1008 AD Amsterdam

T 020 301 03 01
E info@nba.nl
I www.nba.nl