

Met continuous monitoring naar continuous data level assurance; de volgende stap in interne beheersing

Hans Verkruijsse

SAMENVATTING Door allerlei technologische ontwikkelingen neemt de hoeveelheid elektronische data exponentieel toe. Eenzelfde ontwikkeling volgen de rekencapaciteit van computers en de datacommunicatiemogelijkheden. In het maatschappelijk verkeer verschuift de focus van documentuitwisseling naar data-uitwisseling. De vraag is dan ook gerechtvaardigd wat de waarde is van al die data. Zijn de huidige concepten van monitoring wel ingesteld op deze ontwikkeling? Het antwoord is helaas ontkenkend. In dit artikel wordt ingegaan op een drietal nieuwe concepten die samen een oplossing kunnen bieden: (1) continuous monitoring, (2) continuous internal auditing en (3) continuous data level assurance. De concepten worden aan de hand van een framework toegelicht.

RELEVANTIE VOOR DE PRAKTIJK Met behulp van continuous monitoring is het management in staat om snel en adequaat te reageren op afwijkingen die optreden in productieprocessen waardoor deze processen efficiënter en effectiever worden, hetgeen een positief effect heeft op de totale bedrijfsvoering. Met behulp van continuous internal auditing is de internal auditor in staat snel risico's te identificeren en het management te adviseren omtrent te nemen maatregelen als ook in continuïteit te kunnen rapporteren over de juistheid van de individuele gegevens. Daarnaast blijkt dat kostenbesparingen te behalen zijn (Vasarhelyi et al., 2004; Murcia et al., 2008; Kogan et al., 1999; Brown et al., 2007). Alles et al. (2006a) stelden vast dat 75% van alle handmatige controles bij een grote onderneming geautomatiseerd konden worden.

1 Inleiding

Het onderzoeksbureau International Data Corporation (IDC) en IBM, zo rapporteert Forbes (2015), voorspellen dat we in 2020 kunnen beschikken over 40 zet-

tabytes aan opgeslagen data¹. ABI research (2013) voorspelt dat met de introductie van 'internet of things' in 2020 meer dan 30 miljard apparaten draadloos met elkaar in verbinding staan en, al dan niet met menselijke tussenkomst, data in continuïteit met elkaar uitwisselen. In het maatschappelijk verkeer is dit zichtbaar aan het worden, getuige de visie van het kabinet op de digitale overheid 2017, neergelegd in de visiebrief van Minister Plasterk aan de Tweede Kamer van mei 2013, waaraan onderstaand citaat is ontleend. *De samenleving verandert in hoog tempo en de manier waarop burgers en overheden met elkaar communiceren verandert mee. Digitale communicatie heeft de afgelopen jaren een hoge vlucht genomen. Het traditionele verkeer per papieren post is op zijn retour. Digitale communicatie gaat vaak sneller, is makkelijker en goedkoper dan communicatie via papier. De samenleving heeft zich de laatste jaren ontwikkeld van een e-samenleving, waarin de nadruk lag op technologische mogelijkheden, naar een i(nformatie)-samenleving waarin informatiestromen van steeds groter belang zijn. Hierbij past een transparante overheid die de digitale mogelijkheden inzet voor betere dienstverlening en gegevensuitwisseling, en een overheid die burgers centraal stelt in de informatiestromen. Een opstelling van de overheid die de effectiviteit en efficiency van overheidshandelen niet in de weg staat, maar deze juist versterkt, mits we dit op een goede manier gezamenlijk aanpakken.* (Ministerie Binnenlandse Zaken en Koninkrijksrelaties, 2013).

Maar wat zijn al die data waard als de juistheid van die data onbekend is? Veel van die data en apparaten maken onderdeel uit van organisaties en alleen als de interne beheersing van die organisaties voldoet aan de daaraan te stellen eisen, kan een uitspraak gedaan worden over de juistheid van die data. Het continue aspect van het met elkaar uitwisselen van data maakt dat het vaststellen van de juistheid van die data eveneens in continuïteit dient plaats te vinden. Daar komt nog bij

dat die uitgewisselde data vallen in de categorie van ‘big data’² en dus niet alleen financiële data hoeven te zijn. Ook aan niet-financiële data wordt de eis gesteld van juistheid, immers een data-ontvangende partij – met menselijke dan wel kunstmatige intelligentie – zal de ontvangende data gaan gebruiken voor eigen besluitvorming. Een data-ontvangende partij kan zowel binnen de data-verstrekende organisatie, afdeling of dochter, gesitueerd zijn als daarbuiten.

Vanuit de traditionele auditgedachte wordt sterk de nadruk gelegd op het getrouwe ‘beeld’ dat door het geheel van en de samenhang tussen alleen financiële data wordt opgeroepen. Dit is gebaseerd op de assumptie dat managers hun beslissingen grotendeels baseren op financiële data en in het bijzonder op financiële verantwoordingsstukken. Echter, in de huidige economie wordt niet-financiële data in toenemende mate gebruikt bij de besturing van organisaties en in de besluitvormingsprocessen van onder meer managers, klanten, leveranciers en banken. Het verkrijgen van zekerheid omtrent de juistheid van al die data is dan ook al jaren evident (Greenstein & Ray, 2002; Vasarhelyi, 2002; Vasarhelyi et al., 2004). De vorenstaande wijziging van het periodiek uitwisselen van documenten naar een real time uitwisselen van data leidt tot een wijziging in het geven van zekerheid daarbij en wel van periodiek document-level assurance naar continuous data-level assurance. Hiervoor dient een conceptueel framework ontwikkeld te worden waardoor het management van een organisatie die zekerheid kan krijgen die noodzakelijk is om gebruik te kunnen maken van de gegevens in haar besturende rol. In dit artikel wordt een aanzet is gegeven voor de ontwikkeling van een dergelijk framework. Het is gericht op de internal audit functie. Het meenemen in dit artikel van de external audit functie zou het artikel te omvangrijk maken.

Duidelijkheid omtrent de mate van juistheid van de data is dan ook een voorwaarde sine qua non. Het continu monitoren van de maatregelen van interne beheersing en het geven van continue zekerheid omtrent juistheid van die data ligt aan de basis van een drietal nieuwe concepten, te weten; (1) continuous monitoring, (2) continuous internal auditing en (3) continuous data level assurance. Al een aantal jaren wordt door grote organisaties, zoals Siemens, IBM, HCA en the Royal Canadian Mounted, met deze concepten ervaring opgedaan (Alles et al., 2006a; Alles et al., 2006b, Nelson, 2004). Dat de interesse in het onderwerp leeft blijkt wel uit een search naar continuous auditing op Google. Alles et al. (2006b) kregen op 26 juni 2006 76.000 hits, vier jaar waren dit 284.000 hits en op 13 augustus 2015 waren dat al meer dan 52 miljoen hits. In dit artikel worden in paragraaf 2 de drie continuous concepten nader beschouwd. In paragraaf 3 is het Conceptueel Continuous Framework beschreven aan de

hand van een schematische weergave. Hierin zijn tevens een aantal mogelijke methoden en technieken weergegeven die in andere wetenschapsgebieden zijn uitgewerkt en al jaren lang worden gehanteerd. In paragraaf 4 wordt antwoord gegeven op de vraag die impliciet volgt uit de titel van dit artikel, te weten of de interne beheersing zich verder ontwikkelt richting het in continuïteit verstrekken van assurance op dat niveau.

2 De drie continuous concepten nader beschouwd³

2.1 Algemeen

Niet altijd wordt onderscheid gemaakt tussen de drie concepten (Brown et al., 2007) en worden de begrippen door elkaar gebruikt, hetgeen onjuist is (Verkruisje, 2012). Door deze verschillen expliciet te maken, wordt de toegevoegde waarde van de concepten zichtbaar. Continuous monitoring kan op sommige punten overeenkomsten vertonen met continuous internal auditing, echter de verantwoordelijkheid van een goed geheel van interne beheersingsmaatregelen in het kader van continuous monitoring ligt bij het management. Het uitvoeren van controles in het kader van continuous internal auditing is de verantwoordelijkheid van de internal auditor (Vasarhelyi et al., 2004), evenals het geven van assurance op data level. Het is mogelijk de concepten los van elkaar in de organisatie te implementeren hoewel een combinatie is aan te bevelen door de synergievoordelen die met een gecombineerde implementatie van concepten gepaard gaan. Om de uitkomsten van deze continue aanpak in de vorm van assurance zichtbaar te maken en te koppelen aan de individuele data is het noodzakelijk dat gebruik wordt gemaakt van een ‘tagged-data’ formaat dat daarvoor geschikt is, zoals XML⁴ en XBRL⁵.

2.2 Continuous monitoring

Continuous monitoring stelt het management van een organisatie in staat om continu ‘in-control’ te zijn. In continuïteit wordt de werking van de bedrijfsprocessen en de naleving van procedures vastgesteld aan de hand van vooraf vastgestelde normen (IIA, 2005). Door de implementatie van continuous monitoring komt de benodigde informatie omtrent de interne beheersing sneller beschikbaar (Brown et al., 2007; Vasarhelyi et al., 2004; Nelson, 2004; Kogan et al., 1999; Murcia et al., 2008; Willems & Vredenberg, 2008). Daarnaast verhoogt het sneller beschikbaar komen van data de kwaliteit van de besluitvorming van het management en alle andere gebruikers van die data. Door het integreren van interne beheersingsmaatregelen die patronen kunnen herkennen en afwijkingen ervan kunnen rapporteren en verklaren in het geautomatiseerde systeem kan vorm worden gegeven aan conti-

uous monitoring van alle geautomatiseerde processen en procedures die van invloed zijn op de data. Deze wijze van monitoring sluit aan bij de twee meest belangrijke COSO-rapporten⁶ en beperkt zich overeenkomstig die rapporten niet tot de betrouwbaarheid van financiële verslaggeving. Door toepassing van het concept van 'management by exception' is het management in staat direct tot actie over te gaan indien een geconstateerde afwijking valt buiten een vooraf vastgestelde bandbreedte.

2.3 Continuous internal auditing

Continuous internal auditing stelt de internal auditor in staat om in continuïteit controles uit te voeren gericht op de werking van de maatregelen van continuous monitoring om zodoende op ieder gewenst moment niet alleen een oordeel te kunnen geven over de interne beheersing van een organisatie (IIA, 2005) maar nog meer over de juistheid van de data. Het object van onderzoek zal hierbij voor de internal auditor het geheel van methoden en technieken zijn die door het management gebruikt worden in het kader van continuous monitoring. Aangezien in dat geheel van methoden en technieken alle processen, procedures en data betrokken zijn, zal de internal auditor zich voor wat betreft de werking van het geheel van methoden en technieken richten op gesignaleerde afwijkingen en de wijze waarop door het management met deze afwijkingen is omgegaan, dus een beoordeling van het continuous monitoring op basis van 'auditing by exception'.

Ook hier geldt het continuïteitsaspect, het omvat dus veel meer dan wat vaker een specifiek proces beoordelen of de data onderzoeken met behulp van een steekproef. De internal auditor zal zijn auditprocedures moeten integreren in de software van de organisatie waardoor hij direct gewaarschuwd wordt indien afwijkingen worden gesignaleerd door de interne beheersingsmaatregelen die groter zijn dan een vooraf vastgestelde norm en waardoor hij wordt geïnformeerd over de door het management getroffen acties. De kwaliteit van de internal audit zal hierdoor verhoogd worden. Door het integreren van de auditprocedures in het geautomatiseerde systeem neemt de kans op fouten, ten opzichte van handmatig uitgevoerde controles, in het controleproces af (Murcia et al., 2008; Vasarhelyi et al., 2004; Brown et al., 2007). Daarnaast zal de internal auditor periodiek en op basis van een vooraf uitgevoerde risicoanalyse kennis moeten nemen van de meta-data⁷ teneinde ontwikkelingen in de data te kunnen signaleren en beoordelen. Zijn auditprocedure richt zich op de interne beheersingsmaatregelen die zijn geïmplementeerd en zijn gebaseerd op patroonherkenning. Fraude zou hiermee in een vroeg stadium door de internal auditor kunnen worden opgespoord. Bovendien zal hier een preventieve werking van uitgaan. Medewerkers weten dat deze controles zijn geïmplemen-

teerd en dat zij in geval van fraude het risico lopen ontdekt te worden (Kogan et al, 2007; Koskivaara & Back, 2007).

De internal auditor richt zich dus voor wat betreft de werking van het systeem van interne beheersingsmaatregelen in het kader van continuous monitoring niet direct op de interne beheersingsmaatregelen zelf, maar op de signalen uit de monitoring op de werking van deze maatregelen. Daarom wordt ook wel gesproken van meta-control (De Aquino et al., 2010). Voor wat betreft de opzet en het bestaan van de interne beheersingsmaatregelen gericht op continuous monitoring zal de internal auditor in continuïteit de juistheid en toereikendheid van de gehanteerde methoden en technieken vaststellen.

2.4 Continuous data level assurance

Het nieuwe concept continuous data level assurance is de logische uitkomst van de hiervoor genoemde concepten en dient gezien te worden als een bijdrage aan de transparantie van een organisatie bij data-uitwisseling. Bij continuous data level assurance wordt continu een bepaalde mate van zekerheid gegeven en vastgelegd bij de individuele data zonder dat daar expliciet om gevraagd is door een individuele belanghebbende en zonder dat daar directe internal auditprocedures op zijn toegepast. Zolang noch de continuous monitoring interne beheersingsmaatregelen die geïntegreerd zijn in het geautomatiseerde systeem, noch de in de software geïntegreerde auditprocedures een onacceptabele afwijking signaleren, vindt het voegen van een bepaalde mate van zekerheid aan individuele data volledig geautomatiseerd plaats. Ook dit gedeelte is geheel gebaseerd op het concept 'management/auditing by exception'. Op basis van vooraf gedefinieerde en in de software geïmplementeerde algoritmes kan de mate van zekerheid gedurende de transacties waarbij de data worden gebruikt fluctueren. Zo neemt het niveau van juistheid van een gegeven toe naarmate het geconfronteerd kan worden met andere gegevens, bijvoorbeeld de gegevens in de 'three-way-match'. Ieder daarbij gehanteerd gegeven kan gecontroleerd worden, bijvoorbeeld op rekenkundige juistheid of het gebruik van het juiste tarief. Deze controles leveren slechts een laag niveau van juistheid op. Pas als alle gegevens beschikbaar zijn en met elkaar zijn geconfronteerd is het niveau van juistheid voor de daarbij gehanteerde gegevens maximaal.

Het vorenstaande heeft grote implicaties. Het concept continuous internal assurance is gericht op het data-level in plaats van op het document-level⁸. Daarnaast vraagt het concept continuous data level assurance om een continuüm van het assurance-begrip in plaats van de gebruikelijke vier assurance-niveaus⁹ die momenteel gangbaar zijn, zie het hiervoor gegeven voorbeeld met betrekking tot de 'three-way-match'. Omdat een dergelijk concept van assurance slechts ziet op individuele

data kan geen sprake meer zijn van een mate van assurance zoals dat behoort bij een verantwoordingsverslag, de zogenaamde 'beeld'-verklaring. Een beeld-verklaring geeft nauwelijks informatie over de mate van assurance bij individuele posten in het verantwoordingsverslag en helemaal niet over de mate van juistheid van de aan die post onderliggende individuele data. Indien een gebruiker geïnteresseerd is in één specifieke data dan geeft de beeld-verklaring onvoldoende tot geen zekerheid. Dit kan worden opgelost met een juistheid-verklaring die rechtstreeks gekoppeld is aan de individuele data. Daarbij is het dan noodzakelijk, zoals eerder is aangegeven, dat gebruik wordt gemaakt van een 'tagged-data' formaat. Indien een dergelijke stap wordt gemaakt heeft een verschuiving plaatsgevonden van document-level assurance naar data-level assurance.

3 Een conceptueel model van frameworks

Onderstaand wordt op hoofdlijnen ingegaan op de drie nieuwe continuous-concepten, continuous monitoring, continuous auditing en continuous data level assurance, aan de hand van een doorontwikkelde schematische conceptuele weergaven (Verkruisje, 2010). In de onderstaande beschrijving wordt aan het conceptueel continuous framework gerefereerd onder CCF en een nummer. Het gaat te ver voor dit artikel nader in te gaan op alle methoden en technieken die bij de verdere uitwerking van de frameworks kunnen worden gehanteerd. De genoemde methoden en technieken zijn derhalve slechts richtinggevend. Deze methoden en technieken zijn mede ontleend aan andere wetenschapsgebieden waarvan enkele worden genoemd.

3.1 Het conceptueel continuous monitoring framework

De start van het continuous monitoring framework ligt in de onderkenning dat ieder uniek product het

gevolg is van zijn eigen unieke productieproces (CCF 1). Afwijkingen in het productieproces zullen altijd leiden tot afwijkingen in het product en vice versa heeft een aanpassing van het product altijd gevolgen voor het productieproces en daarmee eveneens voor de data die aan beide kan worden onttrokken. Uitgangspunt hierbij is dat een onlosmakelijk verband bestaat tussen afwijkingen in de productieproces-data en de product-data.

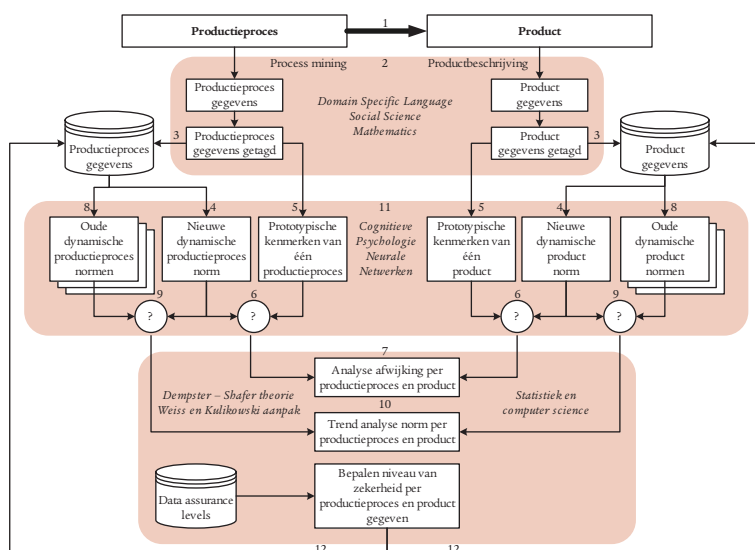
Ter wille van de leesbaarheid van deze beschrijving wordt met name ingegaan op de stroom productieproces-data. De stroom met product-data volgt exact dezelfde weg maar zal niet bij alle stappen even diep worden uitgewerkt.

Met behulp van process mining kunnen data uit de logging worden gehaald die betrekking hebben op het productieproces (Van der Aalst, 2011; Van der Aalst & Koopman, 2015; Jans et al., 2010). Hetzelfde kan gedaan worden voor het product. Voor de laatste zullen de gedetailleerde productbeschrijvingen geraadpleegd kunnen worden en kan de kennis van de 'subject matter experts' een waardevolle bijdrage betekenen. Naast de verworvenheden van process mining kan ook gebruik worden gemaakt van diverse ontwikkelingen vanuit andere wetenschappen (CCF 2).

Nadat de productieproces-data zijn geïdentificeerd worden deze data opgeslagen in een tagged-data formaat. In de tag die aan de data wordt gehecht wordt de betekenis van de data opgenomen. Door het toepassen van XBRL is het mogelijk om tevens in de tag een grote verscheidenheid aan interne beheersingsmaatregelen op te nemen. Hierbij kan gebruik worden gemaakt van 'domain specific language' een ontwikkeling vanuit 'Social science and Mathematics'-richting (CCF 3).

Aan de database met een groot aantal getagde data worden kennispatronen ontleend met behulp van patroonherkenningssoftware. Deze kennispatronen bestaan uit kenmerkende, prototypische eigenschappen waarmee het productieproces en het product het best kunnen worden beschreven. Hierbij wordt gebruik gemaakt van zelflerende systemen die gebaseerd zijn op neurale netwerken. Deze zelflerende systemen zijn het product van jarenlang onderzoek in onder meer de cognitieve psychologie (Rosch, 1978; Weiss & Kulikowski, 1991). Het samenstellen van een kennispatroon van kenmerkende prototypische eigenschappen dat een product beschrijft zal vaak gemakkelijker zijn dan dat van het productieproces. Naarmate de kennispatronen het productieproces en het product beter beschrijven, is het onderscheidend en daarmee het voorspellende vermogen ook beter ontwikkeld. Het ontwikkelen van dit onderscheidend vermogen is gebaseerd op de frequentieverdelingen van de eigenschappen. Rekening dient gehouden te worden met het feit dat de kennispatronen opgebouwd zijn uit financiële en niet-financiële data.

Figuur 1 Het Conceptueel Continuous Framework (CCF)



Zelflerende systemen ontwikkeld vanuit de cognitieve psychologie, met daarin opgenomen kunstmatige intelligentie, zijn in staat te verklaren waarom en hoe zij gekomen zijn tot deze kennispatronen. Een waarschuwing is daarbij wel op zijn plaats. Dit soort systemen kunnen ook fouten maken. Het valideren van de kennispatronen is daarom cruciaal. Subject matter experts met betrekking tot de producten kunnen betrokken worden bij de validatie van de product-kennispatronen hetgeen niet eenvoudig is bij de productieproces-kennispatronen. Voor het valideren van deze kennispatronen kan gebruik worden gemaakt van methoden en technieken die ontwikkeld zijn vanuit de Computer Science. Met behulp van de door Weiss en Kulikowski (1991) ontwikkelde methode kan het niveau van de voorspellende waarde van een kennispatroon worden bepaald.

De zo ontwikkelde kennispatronen worden gehanteerd als de normen waaraan de individuele productieproces-data en product-data in continuïteit zullen worden getoetst. Deze normen zijn, in tegenstelling tot wat normaal van normen mag worden verwacht, niet statisch. Om die reden worden zij aangeduid met dynamische norm (CCF 4).

Nadat de dynamische normen als te hanteren normstelling zijn gevalideerd door 'subject matter experts' wordt van iedere volgende transactie enerzijds alle productieproces-data en product-data getagd ingevoerd in de desbetreffende databases om op een later tijdstip begrepen te worden in de opbouw van nieuwe dynamische normen (CCF 3). Anderzijds worden van die individuele transactie de prototypische eigenschappen, zoals die opgenomen zijn in de dynamische norm (CCF 5), zowel van het productieproces als van het product vergeleken met de op dat moment geldende dynamische normen (CCF 6). De daarbij geconstateerde afwijkingen worden geanalyseerd met behulp van methoden en technieken, zoals bijvoorbeeld de Dempster-Shafer-theorie, die gebaseerd is op de Bayesiaanse statistiek en patroonherkenningssoftware ontwikkeld vanuit 'Statistics and Computer Science'. Indien uit de analyse blijkt dat de afwijking van de prototypische eigenschappen ten opzichte van de geldende dynamische normen binnen de vooraf vastgestelde bandbreedte blijft, worden geen verdere acties ondernomen. Indien de afwijking buiten de vooraf vastgestelde bandbreedte valt zal de volledige transactie worden aangeboden aan de 'subject matter experts' ter validatie van de transactie. Op deze wijze wordt recht gedaan aan het 'management by exception'-concept (CCF 7).

Nadat van een vooraf gedefinieerd aantal transacties alle productieproces-data en product-data zijn getagd en ingevoerd in de databases worden opnieuw dynamische normen met behulp van patroonherkenningssoftware ontwikkeld (CCF 8). Deze nieuwe dynami-

sche normen ondergaan dezelfde validatieprocedure als hiervoor genoemd. Daarnaast vindt een analyse plaats van de ontwikkeling in de dynamische normen (CCF 9). Immers het aantal transacties begrepen in de databases waaruit de kennispatronen en daarmee de dynamische normen eerder waren ontwikkeld is altijd lager dan het aantal transacties dat na verwerking in de databases is opgenomen. De voorspellende waarde van kennispatronen wordt positief beïnvloed naarmate bij het ontwikkelen van kennispatronen gebruik kan worden gemaakt van een groter aantal data.

Afwijkingen tussen twee elkaar opvolgende sets aan dynamische normen, die vallen binnen een vooraf vastgestelde bandbreedte, zullen niet leiden tot nadere analyses. Bij afwijkingen die vallen buiten de bandbreedte dient nagegaan te worden in hoeverre deze trendbreuk veroorzaakt wordt door een strategiewijziging van de organisatie en dient het topmanagement hiervan op de hoogte te worden gesteld. Anders is dit indien iedere keer een kleine afwijking wordt geconstateerd tussen elkaar opvolgende sets aan dynamische normen. Door nu periodiek nieuwe dynamische normen aan de databases te ontfemen kan een langjarige trendanalyse worden uitgevoerd op de ontwikkeling van de dynamische normen. Daar deze dynamische normen beschrijvingen zijn van zowel het productieproces als van het product zou die trendanalyse tot dezelfde ontwikkeling moeten komen als de ontwikkeling in de beschrijving van het productieproces en het product volgens de organisatorische eenheid die hiervoor verantwoordelijk is, bijvoorbeeld het bedrijfsbureau (CCF 10). Hiermee worden eventueel frauduleuze manipulaties in de getagde data die leiden tot elkaar versterkende kleine afwijkingen in de dynamische normen en het daardoor onjuist signaleren van afwijkingen op transactieniveau in een vroegtijdig stadium ontdekt.

Doordat steeds opnieuw nieuwe normstellende kennispatronen worden vastgesteld en gevalideerd, wordt bewerkstelligd dat de dynamische normstelling gelijke tred kan houden met eventuele verandering in het eindproduct danwel het productieproces, voor zover dit geen veranderingen zijn die de trendmatigheid verstoren. Dit gehele proces van samenstellen van normstellende kennispatronen, het analyseren van afwijkingen van deze kennispatronen in de tijd bezien, alsmede het vrijgeven van een set aan nieuwe dynamische normen, om vervolgens hun bijdrage te leveren aan de validatie van nieuwe individuele transacties wordt gezien als het proces van dynamiseren van de normstelling.

3.2 Het conceptueel continuous internal auditing framework

Het moge duidelijk zijn dat door de grote betrokkenheid van het geautomatiseerde informatiesysteem bij de realisatie van het continuous monitoring framework een zware wissel wordt getrokken op de betrouw-

baarheid van het geautomatiseerde informatiesysteem van een organisatie. Zonder in dit artikel in detail erbij stil te staan wordt wel verwezen naar het grote belang van een goede beheersing en implementatie van de general IT-controls en met name de logische toegangsbeveiliging en de change management-procedures. Immers de interne beheersingsmaatregelen in het kader van continuous monitoring als ook de auditing procedures zijn ingebed in de software die gehanteerd wordt bij het verwerken van de transacties. Het conceptueel continuous internal auditing framework is dan ook gebaseerd op een goed werkend en beheerd geautomatiseerd informatiesysteem voorzien van door de internal auditor gecontroleerde maatregelen van (on-)vervangbare interne beheersing. De internal auditor dient zich naast vorenstaande tevens een oordeel te vormen omtrent de software die gehanteerd wordt in het kader van proces mining en de tagging van de data. Hiervoor is een groot aantal standaardsoftware-pakketten voorhanden.

Specifiek voor het komen tot data-level assurance dient de internal auditor zich een oordeel te vormen omtrent de wijze waarop het taggen van de gegevens (CCF 3) alsmede de patroonherkenningssoftware is ingezet bij het ontlenen van de kennispatronen (CCF 11). Daarnaast is het van belang dat de internal auditor nagaat op welke wijze de validatie van de kennispatronen heeft plaatsgevonden alsmede door welke functionaris de kennispatronen tot dynamische norm zijn verheven en door welke functionaris de bandbreedtes zijn opgegeven waarbinnen afwijkingen geaccepteerd worden (CCF 4). Uitgaande van de signalering vanuit zijn eigen auditprocedures die geïntegreerd zijn in de transactiesoftware, dient de internal auditor kennis te nemen van alle afwijkingen die geconstateerd zijn en die vallen buiten de vooraf vastgestelde bandbreedte en de acties die het management heeft genomen (CCF 7 en 10). De internal auditor dient vast te stellen of de daartoe genomen actie daadwerkelijk heeft plaatsgevonden en of de actie adequaat is geweest. Dit is de controle op het 'management by exception'-concept. De internal auditor richt zich dus niet rechtstreeks op de data zelf maar op de meta-data van de gemonitoring.

Zoals uit het vorenstaande blijkt richten de auditprocedures van de internal auditor zich op de juistheid van de data door het vormen van een oordeel omtrent de opzet, het bestaan maar vooral de continue werking van de interne beheersingsmaatregelen in het kader van continuous monitoring, genaamd het meta-controlconcept, en de juistheid van de data, genaamd het meta-dataconcept. Dit geheel is niet anders dan wat in het vak Auditing conceptueel wordt gedoed. Iedere keer dat een audit plaatsvindt dient eerst een audit te worden gedaan op de normstellingen, bij continuous internal auditing is dat op meta-controlniveau. Daarna vindt de audit plaats van de data zelf, bij continuous

internal auditing is dat op meta-dataniveau. De conceptuele gedachten achter auditing blijven derhalve dezelfde; alleen verschuiven de objecten van de audits naar een hoger abstractieniveau. De audittechnieken zullen daarop zeer zeker moeten worden aangepast.

3.3 Het conceptueel continuous internal data level assurance framework

Indien de afwijkingen, zowel tussen de prototypische eigenschappen en de dynamische normen als de afwijkingen tussen de opeenvolgende dynamische normen, binnen de vooraf vastgestelde bandbreedte blijven wordt automatisch in de XBRL-'tag' van de data een vooraf vastgesteld niveau van assurance vastgelegd. Het toegekende niveau van assurance is enerzijds afhankelijk van het proces waarin de transactie heeft plaatsgevonden en anderzijds van de procedurestap binnen het proces waarin de transactie zich bevindt. Daarnaast is de zwaarte van de in de software geïntegreerde controle van belang. Het vaststellen van de verschillende niveaus van assurance dat aan de data kan worden toegekend alsmede de daarbij gehanteerde procedure is de verantwoordelijkheid van de internal auditor. Immers de internal auditor is degene binnen de organisatie die verantwoordelijk is voor de uitvoering van de internal audit en het verstrekken van assurance. De internal auditor zal wel diepgaande kennis moeten hebben van de productieprocessen en de producten.

Aangezien de door de internal auditor gegeven assurance ziet op de data en niet op een document en daarnaast alleen het aspect juistheid afdekt is, is te verwachten dat de internal auditor onvoldoende mogelijkheden heeft om zijn oordeel uit te spreken gebruik makend van de huidige set van vier niveaus van assurance. Gelet op de huidige stand van de techniek in het zichtbaar maken van glijdende schalen is het mogelijk data level assurance te vervatten in een assurance continuüm zonder hieraan absolute waarden toe te kennen.

4 Conclusie

In de titel van deze bijdrage werd de vraag gesteld of met continuous monitoring een volgende stap gezet kon worden in de interne beheersing van een organisatie door te gaan naar continuous data level assurance. Zoals uit vorenstaande blijkt is het antwoord volmondig ja. Wel betekent dit een revolutionaire omwenteling in het denken van managers, auditors en stakeholders met betrekking tot gegevens en informatie. Niet meer een 'one-size fits all'-gedachte achter het ter beschikking stellen van informatie aan allerlei in- en externe stakeholders maar daarvoor in de plaats het verstrekken van alleen die gegevens die een stakeholder nodig heeft voor het nemen van zijn/haar beslissingen. Dit sluit aan bij de achterliggende gedachten van de ontwikkelingen van XBRL en SBR¹⁰. Het is daarbij niet meer aan de data-aanleverende partij te be-

sluiten welke data een uitvragende partij nodig heeft; dit primaat is komen te liggen bij de data-uitvragende partij. Dit is ongeacht of de data-uitvragende partij een persoon dan wel een computer is alsmede of die data-uitvragende partij wel of niet tot de organisatie van de data-aanleverende partij behoort. De data-aanleverende partij hoeft zich alleen te buigen over de juistheid van de individuele data en hoeft zich niet meer druk te maken of de samenhang van de aangeleverde data een getrouw beeld oplevert. De data-uitvragende partij kan zelf, aan de hand van het niveau van assurance op dataniveau, vaststellen wat de invloed van deze verschillende data-level-assurance-niveaus is in het kader van zijn/haar besluitvormingsproces. Daarnaast kan sneller binnen de organisatie ingespeeld worden op afwijkingen zodat de mogelijke negatieve gevolgen beperkt blijven. Ten slotte kunnen kostenbesparingen gerealiseerd worden door een verlaging van de personeelskosten.

In de toekomst zal invulling gegeven worden aan alle mogelijke combinaties binnen deze drie continuous frameworks. Verschillende disciplines zullen met elkaar in gesprek raken om gezamenlijk te kunnen voldoen aan de data- en assurance-behoefte vanuit het maatschappelijk verkeer. Conceptueel is al aangetoond

dat continuous monitoring en in haar kielzog continuous internal auditing en in de toekomst continuous data level assurance veel mogelijkheden kent. Praktijkervaringen zullen leidend zijn in het optimaal benutten en ontdekken van de vele mogelijkheden. De snelheid van deze ontwikkelingen zal bepalen hoe de inrichting van de interne beheersing binnen organisaties en de werkzaamheden van de internal auditor in de nabije toekomst eruit zal gaan zien. ■

Prof. dr J.P.J. (Hans) Verkruisje RE RA is hoogleraar Bestuurlijke Informatie Verzorging aan de Tilburg University. Hij is voorzitter van de Raad van de Beroepsethiek van de NOREA, de Raden van toezicht inzake betrouwbaar administreren, XBRL Nederland, lid van de Member Assembly van XBRL International Inc., International research director bij het Global Accountancy Transparency Institute en doet onderzoek naar continuous monitoring, auditing en assurance en is editor voor het blad Journal of Information Systems. Jarenlang was hij partner bij Ernst & Young en internationaal (IFAC/IAASB/IAESB) en nationaal (CCR) standaard zetter voor accountants.

Noten

1 40 zettabytes = 400.000 miljard gigabytes is geprint ongeveer 36 triljoen pagina's van 1200 tekens dat achter elkaar gezet een lengte heeft van 76 miljoen keer de aarde rond.

2 Op de website van IBM wordt een omschrijving gegeven wat verstaan moet worden onder big data. Big data comes from sensors, devices, video/audio, networks, log files, transactional applications, web, and social media - much of it generated in real time and in a very large scale (<http://www-01.ibm.com/software/data/infosphere/hadoop/what-is-big-data-analytics.html>). Big data kan het best omschreven worden als het geheel van gestructureerde data, zijnde data in een vast formaat zoals jaarrekeningen en spreadsheets, en ongestructureerde data, zijnde

niet eenvoudig te classificeren data, zoals foto's, e-mails, worddocumenten, pdf's, powerpoint etc.

3 Gelet op de strekking van dit artikel worden de concepten continuous internal auditing en continuous data level assurance gezien vanuit de internal auditfunctie. De external auditor zal van de werkzaamheden en bevindingen van de internal auditor gebruik maken en hieromtrent instructies geven. Het gaat te ver om in dit artikel hier verder aandacht aan te geven.

4 XML is eXtensible Markup Language.

5 XBRL is eXtensible Business Reporting Language.

6 Internal Control – Integrated Framework uit mei 2013 en Enterprise Risk Management – Integrated Framework uit september 2004. Zie

<http://www.coso.org/guidance.htm>.

7 Meta-data zijn data die iets zeggen over de karakteristieken van andere data.

8 Zoals momenteel verantwoordingsstukken als jaarrekeningen.

9 (1) 100% assurance, (2) reasonable assurance, (3) limited assurance, (4) no assurance.

10 SBR staat voor Standard Business Reporting, een programma dat onder auspiciën van de Nederlandse overheid wordt geïmplementeerd, is gebaseerd op XBRL en gericht op het meerdere malen gebruik maken van dezelfde gegevens. Na een wetswijziging zullen ondernemingen vanaf boekjaar 2016 hun jaarrekeningen moeten deponeren in XBRL via het SBR-programma bij de Kamer van Koophandel.

Literatuur

■ Aalst, W.M.P. van der (2011). *Process mining: Discovery, conformance and enhancement of business processes*. Berlin-Heidelberg: Springer Verlag.

■ Aalst, W.P.M. van der, & Koopman, A. J.M. (2015). Process mining & data analytics: de kunst van algoritmes. *Maandblad voor Accountancy en Bedrijfsconomie*, 89(10), dit

themanummer.

■ ABI Research (2013). 'More than 30 billion devices will wirelessly connect to the Internet of everything in 2020'. Geraadpleegd op <http://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-connect>

■ Alles M.G., Kogan, A., & Vasarhelyi, M.A. (2002). Feasibility and economics of conti-

nuous assurance. *Auditing: A Journal of Practice & Theory*, 21(1), 1-14.

■ Alles, M., Brennan, M.G., Kogan, A., & Vasarhelyi, M.A. (2006a). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems*, 7, 137-161.

- Alles, M.G., Tostes, F., Vasarhelyi, M.A., & Riccio, E.L. (2006b). Continuous auditing: the USA experience and considerations for its implementation in Brazil. *Journal of Information Systems and Technology Management*, 3(2), 221-224.
- Brown, C.E., Wong, J.A., & Baldwin, A.A. (2007). A review and analysis of the existing research streams in continuous auditing. *Journal of Emerging Technologies in Accounting*, 4, 1-28.
- De Aquino, C.E., Da Silva, W.L., & Vasarhelyi, M.A. (2010). On the road to continuous auditing. Working Paper, Rutgers University. Geraadpleegd op <http://raw.rutgers.edu/MiklosVasarhelyi/Resume%20Articles/PROFESSIONAL%20PAPERS/P32.%20on%20the%20road%20to%20cont%20auditing153.pdf>.
- Forbes, Thomas, J. (2015). Where is the world supposed to put all of its data. Forbes. Geraadpleegd op <http://www.forbes.com/sites/ibm/2015/02/17/where-is-the-world-supposed-to-put-all-of-its-data/>.
- Greenstein, M.M., & Ray, A.W. (2002). Holistic, continuous assurance integration: e-business opportunities and challenges. *Journal of Information Systems*, 16, 1-20.
- IIA, The Institute of Internal Auditors (2005). Continuous auditing: implications for assurance, monitoring, and risk assessment. Geraadpleegd op http://www.acl.com/pdfs/wp_gtag_may05.pdf.
- Jans, M., Alles, M., & Vasarhelyi, M.A. (2010). Process mining of event logs in auditing: Opportunities and challenges. Working paper Hasselt University, presented at the ISAR conference 2010. Geraadpleegd op SSRN: <http://ssrn.com/abstract=1578912>.
- Kogan, A., Sudit, E.F., & Vasarhelyi, M.A. (1999). Continuous online auditing: A program of research. *Journal of Information Systems*, 13(2), 87-103.
- Koskivaara, E., & Back, B. (2007). Artificial Neural Network Assistant (ANNA) for continuous auditing and monitoring of financial data. *Journal of Emerging Technologies in Accounting*, 4, 29-45.
- Ministerie Binnenlandse Zaken en Koninkrijksrelaties, (2013). Visiebrief Digitale overheid 2017. Geraadpleegd op <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/05/23/visiebrief-digitale-overheid-2017.html>.
- Murcia, F.D-R., De Souza, F.C., & Borba, J.A. (2008). Continuous auditing: A literature review. *Organizacoes em contexto*, 4(7), 1-17.
- Nelson, L. (2004). Stepping into continuous audit. *Internal Auditor*, 61(2), 27-29.
- Rosch, E. (1978). Principles of categorization. In E. Rosch & B.B. Loyd (eds.). *Cognition and categorization*, (pp. 28-48). Hillsdale, NJ: Lawrence Erlbaum.
- Vasarhelyi, M.A. (2002). Concepts in continuous assurance, In *Researching accounting as an information systems discipline* (chapter 12). American Accounting Association. Geraadpleegd op <http://raw.rutgers.edu/docs/research/M26.%20concepts%20in%20cont%20assurance.pdf>.
- Vasarhelyi, M.A., Alles, M.G., & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting*, 1, 1-21.
- Verkruisje, J.P.J. (2010). Bestuurlijke Informatieve-verzorging: Na het singularity point een nieuwe glanzende toekomst? Inaugurale rede Tilburg University.
- Verkruisje, J.P.J. (2012). Van 'jaarrekening-recht' naar recht op 'continuous assurance'. Liber amicorum voor prof. dr. mr. P.M. van der Zanden RA: De grenzen opzoekend.
- Weiss S.M., & Kulikowski, C.A. (1991). *Computer systems that learn*. San Mateo, California: Morgan Kaufmann Publishers Inc.
- Willems, T., & Vredenberg, S. (2008). Focus op continuïteit, *Audit Magazine*, 5, 27-30.