TRENDS EN ONTWIKKELINGEN IN RISICOMANAGEMENT & COMPLIANCE, ASSURANCE & BUSINESS IT

Jürgen van Grinsven, Koert Meijs, Theo de Joode, Rosanne Pouw, Ruud Fortuin en Peter Steenwijk.

Inleiding

De ontwikkeling van het mondiale systeem gaat gepaard met groeistuipen. De huidige kredietcrisis is daar een voorbeeld van. In dit essay bespreken we eerst kort wat er zoal mis ging. Vervolgens gaan we in op een aantal geleerde lessen en huidige reacties op de crisis. Tot slot geven we een korte schets van een aantal interessante trends en ontwikkelingen op het gebied van (1) risicomanagement & compliance (2) assurance en (3) business IT.

Wat ging er mis?

Begin jaren zeventig zijn veel financiële markten gedereguleerd en verder geliberaliseerd waardoor kapitaalstromen gemakkelijker zijn gaan vloeien tussen verschillende landen. Door de verdere globalisering en automatisering zijn we inmiddels hard op weg naar een mondiaal systeem [1]. Een kleine terugval hebben we reeds gezien met de dot-com (+/-1997-2000) crisis. Toen deze zeepbel uiteenspatte, veroorzaakte dit een wereldwijde lichte recessie. De huidige kredietcrisis begon in 2007 en zet nog steeds door in 2014. Zie tabel 1 voor een chronologisch overzicht. Wereldwijd moeten overheden, toezichthouders en ondernemingen ingrijpende maatregelen nemen om de

financiële stabiliteit te waarborgen. De huidige crisis heeft duidelijk gemaakt dat het risicoprofiel van elke onderneming buitengewoon snel kan veranderen [1]. Dat zal inmiddels niemand meer ontkennen. Welke lessen kunnen we trekken? Welke reacties geeft dat? Voor welke uitdagingen staan we zoal?

Tabel 1

Periode / jaartal	Gebeurtenis
1997-2000	Dotcom Crisis
maart-2007	Eerste beroering in de USA
juli-2007	Prof. Tissen waarschuwt voor een neergaande economie
augustus-2007	Europese aandelenbeurzen fors onderuit
september-2007	Kredietcrisis grijpt het bedrijfsleven
oktober-2007	Dow-Jones onder 14000 punten
februari-2008	Britse overheid nationaliseert Northern Rock
april-2008	ECB leent aan Nederlandse zakenbank
juli-2008	Reddingsplan Amerikaanse regering
september-2009	Lehman vraagt uitstel van betaling
oktober-2008	Overheden grijpen in
2008	Kapitaalinjecties: AEGON, ING
2008	Icesave
2008-2013	Nationalisaties: Fortis, SNS REAAL, ABN AMRO
2010	Verhoging garantie op deposito's
2014	Verscherpt Europees Toezicht en mogelijkheden tot ingrijpen

De lessen en de reacties

De impuls die uitgaat van geleden verliezen leeft blijkbaar maar kort. Ga maar na: wat hebben we geleerd van de dotcom crisis? Zagen we destijds de echte risico's van: de snel stijgende beurskoersen, stijgende winsten en de beursspeculaties? Begrijpen we nu de risico's van hetgeen waarin we willen beleggen? Beseffen ondernemingen nu het belang van het vertrouwen van hun klanten? Of we het nu leuk vinden of niet: de huidige kredietcrisis vertoont, uiteraard achteraf gezien, grote gelijkenis met de vorige crisis. De vraag is: willen we leren van de huidige kredietcrisis, of gaan we er wederom vanuit dat het ons niet meer zal overkomen? Welke reacties zien we tot op heden? De toezichthouders reageren met meer en verscherpt toezicht op risi-

comanagement, assurance en de informatie technologie [4]. De overheid en het publieke debat richt zich op de kwaliteit van accountants en de toekomst van de beroepsorganisaties voor accountants [5]. Ondernemingen vragen meer assurance (zekerheid) over de diensten van hun toeleveranciers middels 'verklaringen' zoals een ISAE3402, In Control Statement, informatie- en databeveiliging en andere assurance rapportages [10, 11, 12]. Kortom: men vertrouwt elkaar niet meer op de 'blauwe ogen'. We gaan steeds meer van 'show me' naar 'prove me'. Maar bewandelen we hiermee wel de juiste weg?

Trends en ontwikkelingen

We staan aan de vooravond van een ingrijpend veranderproces. De eerste contouren zijn al zichtbaar met grote reorganisaties, versnelde implementaties en verhoogde alertheid op risicomanagement & compliance, assurance en business IT. Inmiddels is duidelijk geworden dat de kredietcrisis binnen de financiële sector grote impact heeft op andere sectoren. Vele ondernemingen buiten deze sector zijn gegrepen door de kredietcrisis. Hieronder schetsen we een aantal trends en ontwikkelingen op het gebied van (1) risicomanagement & compliance (2) assurance en (3) business IT die relevant zijn voor vele ondernemingen.

1. Risicomanagement & Compliance
De uitvoerige discussies in onder andere de wetenschap, overheid, bedrijfsleven en media wijzen veelal in de richting van een falend risicomanagement en compliance [1, 2, 3, 4, 5]. In de meeste ondernemingen is dit thema belegd als activiteit die losgekoppeld is van de primaire bedrijfsprocessen en het besluitvormingsproces [2]. Dit is ook niet verwonderlijk omdat de infrastructuur, processen en systemen voor risicomanagement en compliance onvoldoende ontwikkeld zijn, met als gevolg dat de meeste ondernemingen dit gefragmenteerd hebben ingericht. Vaak ontbreken daardoor echter essentiële schakels [1]. Dit is de toezichthouders inmiddels ook niet ontgaan. De toezichthouders zetten de lijnen uit en hebben tevens de taak de risico's niet te laten 'stapelen'. De kredietcrisis laat bijvoorbeeld zien dat het aan te houden kapitaal bij financiële instellingen niet overal even toereikend was. De rol van de toezichthouders is aan het veranderen. We gaan steeds meer naar een internationaal toezicht. De (internationale) toezichthouders van de banken buigen zich bijvoorbeeld momenteel over de governance, het herstellen van het vertrouwen, de transparantie en het aan te houden kapitaal. Ook de nationale overheden zullen daarin een rol van betekenis gaan spelen [5]. De overheid

tendeert richting verantwoordelijkheid en verantwoording. Op strategisch niveau is er in de meeste gevallen maar één verantwoordelijk. Degene die verantwoordelijk is zou daarom weer verantwoordelijk gehouden moeten worden voor de genomen beslissing. Op het tactisch niveau, meestal het senior management, moet men bekend zijn met de oorzaken en consequenties. Ze moeten een actieve rol bekleden in het risicobewust maken van de onderneming. Eigenaarschap van risico's en (implementatie van) beheersmaatregelen, naleven van wet- en regelgeving, delen van kennis en het naleven van afspraken zijn dan sleutelwoorden [6]. Op het operationele niveau vraagt de naleving van de regelgeving en controle op processen en activiteiten niet alleen een hoge vorm van risicobewustzijn van zowel medewerker als direct leidinggevende, ook het daadwerkelijk handelen speelt een grote rol [1, 3, 6]. Dit klinkt eenvoudiger dan het in werkelijkheid is. Ondernemingen zoeken continu naar nieuwe manieren om kennis en kunde op het gebied van risicomanagement en compliance te mobiliseren [9]. De trend is nu eenmaal, meer risicomanagement en meer compliance.

2. Assurance

Steeds meer ondernemingen zijn, mede door decentralisatie, druk vanuit de markt, meer focus op de kernactiviteiten, kostenoverwegingen en het sterk ontwikkelde internet, steeds beter in staat om hun services te outsourcen [9]. Met de toenemende globalisering zijn er bovendien uitstekende groeimogelijkheden bijgekomen in bijvoorbeeld opkomende economieën. Met name de bedrijfsprocessen die niet gemist kunnen worden maar geen directe bijdrage leveren aan de kernactiviteiten van het bedrijf worden geoutsourced. Met outsourcen bedoelen we hier het uitbesteden van één of meerdere activiteiten [10]. Voorbeelden hiervan zijn payrolling, (IT) helpdeskfuncties, het voeren van administraties en natuurlijk ook het outsourcen van (delen van) IT. Bij outsourcing denkt men tegenwoordig vaak direct aan de cloud. Er zijn echter vele vormen van outsourcing, het bespreken hiervan valt buiten de scope van dit essay [8, 10].

Het uitbesteden is niet zonder risico. Denk maar aan privacygevoelige informatie, verlies van belangrijke gegevens, het niet voldoen aan de wet- en regelgeving, verlies van kennis en kunde, financieel economische criminaliteit en de mogelijk slechte dienstverlening. Het uitbesteden roept vaak veel vragen op. Welke zaken kan ik uitbesteden? Welke regels zijn er? Hoe houd je grip op de zaken die uitbesteed zijn? Hoe blijf je bij outsourcing voldoen aan de wet- en regelgeving? Welke wet- en regelgeving is van toepassing als ik in de cloud zit? Waar ligt de juridische verantwoordelijkheid precies en wie

heeft welke verantwoordelijkheid? Wie is eigenaar van mijn (financiele) gegevens [8]? Om tegemoet te komen aan dit soort vragen wordt door de uitbestedende organisatie vaak een vorm van zekerheid (assurance) gevraagd aan de dienstverlenende organisatie.
De trend die we in het algemeen kunnen waarnemen is dat men elkaar niet meer vertrouwt op de blauwe ogen maar dat men steeds vaker het bewijs wil zien. Dit gebeurt steeds vaker met rapportages die de uitbesteder meer zekerheid moeten bieden. Voorbeelden hiervan zijn: het jaarverslag, auditrapportages, management letters, validatierapporten, ISAE 3402-verklaring, In Control Statement, XBRL rapportages, rapporten met betrekking tot de betrouwbaarheid van de financiële gegevens, milieueffecten rapportages, compliance rapportages en rapportages met betrekking tot de beveiliging van systemen en de data [4, 7, 8, 9, 10, 11, 13]. De gedachte is steeds vaker: vertrouwen is goed maar controle is beter. De gebruiker van de rapportages dient wel goed op te letten: welke zekerheid verkrijgt men bij welk rapport? Van wie krijgt men die zekerheid? Hoeveel zekerheid wilt u eigenlijk hebben? Honderd procent waterdicht is vaak niet wenselijk en zou bovendien erg kostbaar worden.

3: Business IT

Met business IT bedoelen wij hier de Informatie Technologie (IT), in de breedste zin van het woord, die de business van een onderneming ondersteunt en beheerst is. Wat is er aan de hand? We schetsen een eerste voorbeeld. Veel ondernemingen maken veelvuldig gebruik van Excel, Word en Powerpoint om bijvoorbeeld allerlei (financiële) rapportages te maken. De gegevens die veelal in de spreadsheets worden gezet, zijn afkomstig uit meerdere (verouderde) bronsystemen. Hierna vindt dan ook nog regelmatig een verrijking van gegevens plaats of worden bronnen met elkaar gecombineerd [8, 10, 13]. Hoe betrouwbaar zijn de uiteindelijke (financiële) rapportages eigenlijk nog [8]? Kunnen we de juiste gegevens nog wel administreren in de bronsystemen? Kunnen we de huidige systemen wel koppelen aan andere systemen? Hoe zit het met de betrouwbaarheid van de invoer, doorvoer en uitvoer van gegevens? Hoe zit het met het verplaatsen van de huidige softwarepakketten naar de cloud zoals de online boekhouding, tekstverwerking, spreadsheet verwerking, tijdsregistratie, enzovoort? Welke ontwikkelingen zien we nog meer? Een tweede voorbeeld: 'bring your own device'. Men kan een eigen apparaat meenemen naar de onderneming en dit vervolgens koppelen voor gegevenstoegang. Dit lijkt eenvoudig, maar u heeft direct te maken met beveiliging van gegevens en mogelijke verborgen kosten om al die apparaten onderling te verbinden. Ondernemingen zijn vaak niet voldoende in staat om de beveiliging

te waarborgen. Onze waarneming hierbij is dat de eindgebruiker steeds meer verantwoordelijk wordt gemaakt. Maar kan die deze verantwoordelijkheid eigenlijk wel dragen?

Innovatie van IT, platformen, systemen en (cloud) applicaties en de betrouwbaarheid daarvan is waarschijnlijk een van de belangrijkste middelen voor de verdere professionalisering van ondernemingen. Bij oude systemen blijven is zeer onwaarschijnlijk, gezien de snelle (technologische) ontwikkelingen die we doormaken. Zo is bijvoorbeeld het Internet niet meer weg te denken uit het huidige en toekomstige tijdsbeeld [1]. Veel ondernemingen bestempelen het Internet als 'key' in hun dienstverlening. Met de komst van het Internet worden grotere volumes sneller en efficiënter verwerkt door minder personeel, is er een betere bereikbaarheid, kan distributie goedkoper, zijn er uitgebreide contactmogelijkheden en is snelle verzending van informatie mogelijk [9, 13]. Maar ook de beveiliging van informatie speelt een steeds belangrijke rol. Veilige, effectieve en efficiënte gebruikmaking van business IT die tot tevredenheid leidt bij implementatie is volgens ons daarom één van de belangrijkste trends voor de verdere professionalisering van ondernemingen. De ontwikkeling van business IT gaat niet vanzelf in ondernemingen. Hiervoor dient men een nieuwe manier van denken te ontwikkelen. Hierbij dienen dan de aspecten als kernactiviteiten, klantfocus, producten, diensten, winstgevendheid, ontsluiting van diensten, compliance, risicomanagement en assurance centraal te staan.

Tot slot

Meer dan te voren moeten we er rekening mee houden dat het risicoprofiel van elke onderneming buitengewoon snel kan veranderen. De veranderende wet- en regelgeving zal daarbij een dominante rol gaan vervullen binnen een mondiaal systeem. Succesvol opereren kan in de nabije toekomst daarom wellicht alleen nog binnen een internationaal raamwerk van samenwerking. De vak- en onderwijsgebieden Risk, Assurance & Business IT zullen hierbij een essentiële rol spelen maar worden nog vaak vanuit silo's benaderd. In de nabije toekomst zal dit een meer integraal geheel moeten worden. Ondernemingen, overheden, toezichthouders en onderwijsinstellingen zullen een nieuwe manier van denken, manier van werken, manier van modelleren en manier van managen aan moeten leren. Die nieuwe manier van denken verbindt dan vanuit fundamentele principes het risicomanagement & compliance, assurance en Business IT met de gehele onderneming. Het implementeren hiervan kost tijd. Enerzijds moet men wennen aan deze nieuwe manieren. Anderzijds moeten

door het doen van onderzoek, criteria, meetinstrumenten en lesmaterialen aangepast worden. Kortom: we staan aan de vooravond van een ingrijpend veranderproces dat vraagt om een nieuwe aanpak op het gebied van risicomanagement, assurance & business IT. ■

Referenties

[1] Grinsven, van. Jürgen H. M., Ros, Gert-Jan., Lessen en uitdagingen in het financiële systeem. In Bank en Effectenbedrijf, October 2009, pp. 18-21.

[2] Buith, Jacques., Grinsven, van. Jürgen. Governance Risk en Compliance. In Financieel Management, Issue 8, December 2009, pp. 57.

[3] Grinsven, van. Jürgen H. M., Ons overkomt dat niet: Integraal risicomanagement & compliance nog niet vanzelfsprekend, in Bank en effectenbedrijf, pp. 4-6, March 2008.

[4] De Nederlandsche Bank. www.toezicht.dnb.nl

[5] De Nederlandse Overheid. www.overheid.nl

[6] Pauw, Wim. Van Macht naar Kracht. In IT Auditor, pp. 36-39, nr. 1, 2013.

[7] Meijs, Koert and Grinsven, van. Jürgen. The Influence of Anchoring and Framing on Audit Quality. Research paper presented at the Network for AIS research (NAIS) Conference, november 2013.

[8] Panman, Niels., Grinsven, van. Jürgen H. M. en Maarten Mennen. Interne beheersing en financiële data. In controllers magazine, September 2013.

[9] Janssen, Marijn, Grinsven, van. Jürgen. en Joha, Anton. Operational Risk Management as Shared Service Center of Exellence. In Finance Bundeling and Finance Transformation, pp. 363-378. ISBN: 978-3-658-00372-2 (Print). Springer 2013.

[10] Damen, Johan., Grinsven, van. Jürgen., De toegevoegde waarde van een ISAE 3402-verklaring. In Tijdschrift Controlling, pp. 26-30. Oktober 2012.

[11] Grinsven, van. Jürgen H. M., Tien bouwstenen van het In Control Statement. In Finance & Control (Kluwer), April 2011 pp. 41-44.

[12] Grinsven, van. Jürgen H. M., Toet, Maurits., Implementatie van een in control statement. In controllers magazine, Oktober 2010. pp.20-23.

[13] Grinsven, van. Jürgen H. M., Rabou, Joop., Een beter inkoopbeleid van uw bancaire diensten en kredieten. In Tijdschrift Controlling, pp. 28-31, Juni 2012. Eerder al verschenen in Finance & Control, april 2012.