RESEARCH IN IT-AUDITING

A MULTIDISCIPLINARY VIEW

IT-Audit, Compliance and Advisory Program

VU VRIJE UNIVERSITEIT AMSTERDAM
School of Business and Economics
EXECUTIVE EDUCATION

Prof.dr. Abbas Shahim RE

Prof.dr. Abbas Shahim RE is a full professor of IT Auditing and is the academic director of the IT Audit, Compliance and Advisory (ITACA) program at the Vrije Universiteit (VU) Amsterdam. He is active in conducting research, and manages a working group in the area of IT assurance and audit at International Federation for Information Processing (IFIP). Abbas pursuits a business career too and works as the global head of governance, risk and compliance at Atos Consulting where he is a member of the international leadership team.

Research in IT-Auditing:
A Multidisciplinary View

Omslagontwerp: Jan van Praat/Abbas Shahim
Omslagfoto: Vlag Vrije Universiteit, Hoofdgebouw

Eventuele op- en aanmerkingen over deze of andere uitgaven kunt u richten aan:
Vrije Universiteit Amsterdam
PGO IT Audit, Compliance & Advisory
De Boelelaan 1105
1081 HV Amsterdam
E-mail: edp.sbe@vu.nl

ISBN 978-90-828517-0-0
NUR123

Inhoudsopgave

Preface

Conducting scientific-oriented research in IT auditing was not a common practice in the past. It is a road less travelled as the academic relevance of this profession was challenged and discussed. In general, related publications pertain to the practical aspects with which IT auditors deal in the field while executing engagements. These practitioners, mostly passionate about the profession, documented challenges encountered, experiences gained, lessons learned, skills required, frameworks and approaches deployed, and standards applied to get the job done. This way of knowledge transfer has valuably helped IT auditing to get where it is now. Articles, books and other contributions have gratefully been used for years to keep in pace with developments and to expand insights. It has been an accepted way of working among professionals, and has proved to be useful for educative purposes too. And then, things started to change. The possibility emerged that enabled post-graduate programs at universities become a scientific education, after successfully passing an examination performed by the Accreditation Organization of the Netherlands and Flanders locally (referred to as NVAO). As it was decided to go for it, we began to strengthen research in our IT Auditing, Compliance and Advisory (ITACA) program as one of the activities initiated to move in the intended direction: Master of Science (MSc) accreditation. Among other improvements, the corresponding process is refined, the applicable documentation is updated accordingly, the team of mentors is expanded, our focus on methodological approach is enlarged, and personalized attention paid (tailor-made service) to students is increased. It is obviously necessary to keep enhancing the research component of our MSc program. Recently, the concept of the so-called 'House of IT Auditing' has been appended to demonstrate related domains of interest in a cohesive fashion, and to support the line of thinking of students who write a master thesis to specialize prior to their graduation.

Emergence of the book

In light of the above and to provide more concrete value to the profession, the idea of producing this book emerged in autumn 2017 and was immediately welcomed by the core staff of the ITACA program. For achieving this purpose, it was agreed collectively to form an editorial board to ensure that the book is what professionals operating in practice want to read. The installed board was therefore tasked to cooperate with the thesis coordinator on this mutual interest, and to thoroughly review the available theses. It identified only the work that discussed pertinent current subjects, was content-rich, and was realized in accordance with an inquiry-based and transparent process. The board informed the concerned authors, provided them with instructions, guided and monitored the shortening of their research documents, approved the outcomes, and compiled the book by assembling these collected results.

Rationale and contribution

The rationale behind this book is to capture the knowledge contained in the completed research-based theses, reflect it in a publication, and make this material available to practitioners. It is thus intended to make the researched, valued findings and conclusions accessible to a wider group of users than solely the scholars community. The selected multidisciplinary articles are incorporated in this book that we proudly present to the IT auditing profession as the primary and pertinent publication, if not the first one, characterized by a research-orientation. With this sincere initiative, we hope to actively encourage discussion, and tangibly contribute to the creation of another level of information sources involving informative as well as useful input. We consider it just an attempt to be more concrete and to the point with simultaneously varied and relevant themes, thereby generating a wider landscape of today's topics that can potentially sharpen the thoughts of readers, and suggests the focus areas underpinning future developments.

Overview of the content

The content of the book is diverse in nature and reflects a wide range of subjects that are described and discussed in the English as well as in Dutch language. It is provided by our graduated students who are active in IT auditing and related domains. An overview of the titles treated in this written work is presented in the figure below. It is noted here that some of them are abbreviated in order to fit into the illustration.

Research skills

It is worth mentioning that the process of making the book is not a one-time activity. This great experience is planned to become an annual recurring output of the ITACA program to stress the research orientation. It is our belief that the ability to execute a study is a necessary skill that practitioners should possess to be of more value in practice, and thus career ready. The fact of the matter is that we see many similarities between how a research, as a targeted, meaningful, scoped, planned, skilled, structured, documented, logically reasoned, cohesive and traceable way to answer a pre-defined question, is carried out and shared, and the way in which IT audit engagements are performed and reported.

Suggestions and comments

We would like to interact more frequently and engage more intensively with the profession. Any suggestion and feedback that you may have on this publication are welcomed and will surely support us to continuously improve and enrich its content going forward. Suggestions and comments can be provided via email at: edp.sbe@vu.nl. A session to jointly discuss and share views can be setup as well. We hope that you, as reader, will take the opportunity to read and enjoy this book. In so doing, you will make our efforts worthwhile.

Acknowledgements

I would like to acknowledge the active encouragement and involvement of my colleagues at the ITACA program with whom I gladly work: Aicha Rahali, Jan van Praat RE RA, Paul Harmzen RE RA, dr. Rene Matthijsse RE, Stef Schinagl MSc QSA CISA, drs. Kai Hang Ho RE RA, drs. Henk Hendriks RE CISA, and Paul Visser EMIA CISA. From the beginning, they were an enthusiastic supporter of the idea of producing this book, and provided me with valuable and constructive inputs, impressions, suggestions, and perspectives to move ahead. I am grateful to them as they show me dedication and teamwork, provide me advice, share with me their years of experience, and offer me their impressive insights. I also thank drs.ing. Ronald Koorn RE for his willingness to cooperate when he was approached by the editorial board to jointly select a Compact (a Dutch magazine issued by KPMG IT Advisory) article for inclusion in this book.

Thank you all. It has been and will always be a great pleasure to work with you.

Prof.dr. Abbas Shahim RE

Beheersing en DevOps

Veranderingen in de IV-voortbrengingsketen

Paul van Kemenade

Paul heeft ruime ervaring binnen informatiemanagement en IT. In 2001 is hij begonnen als informatie analist bij UWV waar hij o.a. heeft meegewerkt aan de nieuwbouw van het systeem voor re-integratie.

In 2006 is hij overgestapt naar Amersfoortse Verzekeringen waar hij is gaan werken als senior functioneel beheerder met als aandachtsgebied de verbetering van de kwaliteit van functioneel beheerprocessen. In 2011 heeft hij de overstap gemaakt naar de centrale ICT afdeling van ASR Nederland in Utrecht waar hij tot 2014 heeft gewerkt als IT consultant en daarna als IT riskmanager. Sinds 1 augustus 2017 werkt Paul als IT auditor binnen de interne audit afdeling van ASR Nederland.

Paul is in 2008 afgestudeerd aan de Hogeschool van Utrecht richting Management, Economie en Recht. In 2015 heeft hij de Post HBO opleiding internal auditing aan de Haagse Hogeschool afgerond. In 2016 is hij begonnen aan de masteropleiding IT Audit Compliance and Advisory aan de Vrije Universiteit van Amsterdam. Paul voert tijdens zijn masterfase onderzoek uit naar de invloed van agile/DevOps werken op de wijze van beheersing van IT risico's binnen een IV voortbrengingsketen.

1 Inleiding

1.1 Achtergrond

Stofberg [7] geeft een mooie schets van de huidige tijd waarin we leven en waar organisaties mee te maken hebben. We leven in tijden van grote veranderingen. Nieuwe technologieën bieden elke dag nieuwe mogelijkheden. De hoeveelheid data die elk jaar wordt vastgelegd verdubbelt en ook de mogelijkheden om daar bijzondere dingen mee te doen. Dankzij internet is de wereld een global village geworden, waarin iedereen iedereen kent en waarin iedereen met iedereen zaken kan doen. Er zijn dan ook voortdurend nieuwe ontwikkelingen. Hele markten veranderen ingrijpend en er komen steeds weer nieuwe producten en diensten bij, vaak ook nog eens heel erg disruptief (ontwrichtend). Ondernemingen hebben geen keus. Ze moeten enerzijds zichzelf blijven en anderzijds zichzelf voortdurend opnieuw uitvinden. Ondernemingen moeten steeds beter en steeds anders worden.
In het VINT-rapport van Sogeti wordt hierover het volgende gezegd. Dertig jaar investeren in informatietechnologie en digitale infrastructuren heeft nieuwe platformen en tal van nieuwe mogelijkheden opgeleverd. Er is voldoende reden om aan te nemen dat innovatie juist gemakkelijker wordt en niet moeilijker [1].
In een blog op de website van Accenture wordt aangegeven dat de opkomst van internet een belangrijke bijdrage heeft geleverd aan de versnelling van innovatie en daarmee verandering van businessmodellen voor bedrijven. In de afgelopen 20 jaar is de manier waarop we omgaan met internet meerdere keren getransformeerd. Daarbij kun je drie stadia onderscheiden [2]:

1 Digitaal competent: virtuele wereld binnen echte wereld en digitaal visitekaartje.
2 Digitaal ervaren: internet daadwerkelijk gebruiken voor toepassing bestaande businessmodellen (diensten en goederen via internet aanbieden).
3 Digitale transformatie: vanuit cloudgedreven bedrijven in staat te innoveren en aanbieden nieuwe producten en diensten vanuit de digital-first gedachte i.p.v. huidige businessmodellen vertalen in digitale producten en diensten (wendbaarder en schaalbaarder dan ooit).

Om te kunnen concurreren in de huidige markt moeten organisaties zich steeds veranderen en zich aanpassen aan de behoefte van klanten aan snellere diensten, verbeterde functionaliteit, kosten effectieve oplossingen etc. [9]. De business wil dus steeds sneller softwareproducten opgeleverd krijgen om invulling te kunnen geven aan deze behoefte. De IT-afdeling faciliteert hierin, zodat op elk moment goede, bruikbare software in gebruik genomen wordt. Marc Andreessen, een investeerder in Groupon en LinkedIn, verwoordde het in 2011 in een essay in de Wall Street Journal als volgt: software is eating the world. Elk bedrijf is ongeacht uit welke branche in wezen een softwarebedrijf.
Accenture onderzocht de verandering in diverse branches, als onderdeel van haar Technology Vision 2016. Een van de vragen in het onderzoek was: In welk tempo zal technologie veranderen in uw branche in de komende drie jaar? Resultaat van de enquête was dat 86% verwacht dat technologie in de komende drie jaar snel tot zeer snel verandert. Slechts 12% verwacht een langzame verandering in zijn of haar branche en de overige 2% verwacht dat de ontwikkelsnelheid van technologie niet sneller gaat of zelfs achteruit gaat [8]. Dit wordt in een onderzoek onder 250 global leaders surveyed in Harvard Business Review van de Analytic Services 2015 Bevestigd. 44 % van hen zegt te verwachten dat hun industrie in de komende 3 jaar serieus te maken krijgt met digitale disruptie. 22 % zegt dat dit al aan de gang is.
De uitdaging waar bedrijven in deze tijd voor staan werd al in het jaar 2000 treffend verwoord door voormalig CEO van General Electric Jack Welch. Hij zei: ‘If the rate of change on the outside exceeds the rate of change on the inside, the end is near.’ Hij bedoelde daarmee dat bedrijven in staat moeten zijn om mee te bewegen met de snel veranderende omgeving om te kunnen overleven. In deze context past de beweging die we zien naar een IV-voortbrengingsketen waarvan de inrichting gebaseerd is op Agile en DevOps. Deze concepten worden steeds meer omarmd door bedrijven om functionaliteit sneller en met minder frictie en overhead opgeleverd te krijgen waardoor beter voldaan kan worden aan de “always-on economie”.

Dat bedrijven steeds meer de beweging inzetten naar DevOps wordt bevestigd door het in mei 2016 uitgevoerde onderzoek van Gartner Enterprise DevOps Survey Study. Het onderzoek uitgevoerd binnen het Gartner-managed panel bestaande uit IT en business leiders blijkt dat 38 % van de enterprises al DevOps gebruikt en 50 % zal het eind 2016 actief gebruiken.
Maar er zijn natuurlijk ook al de bekende voorbeelden van bedrijven die al van DevOps gebruik maken. Veel aangehaalde voorbeelden zijn Google, Amazon, Spotify, Netflix en Walmart
(zie: http://techbeacon.com/10-companies-killing-it-DevOps).
Maar ook in Nederland zijn een aantal sprekende voorbeelden te vinden van bedrijven die DevOps al verregaand hebben geïmplementeerd. Voorbeelden van Nederlandse bedrijven zijn:

- hypotheekbeheerder Stater (https://www.ictmagazine.nl/achter-het-nieuws/eerste-grote-DevOps-implementatie-business-en-it-trekken-echt-samen-op/
- Bol.com (https://www.xebia.com/.../continuous-delivery-and-agile-transformations...
- ING (https://www.cxotalk.com/financial-services-digital-transformation-ron-van-kemenade-cio-ing-bank

1.2 Probleemstelling

De vraag die nu opkomt is waarom zo veel bedrijven hun IV-voortbrengingsketen aan het transformeren zijn naar DevOps. Sterker nog in het State of DevOps rapport 2016 [11] staat het als volgt verwoord: “Embrace DevOps, or get left behind’. De IT-organisaties die hun IV-voortbrengingsketen hebben georganiseerd op basis van de best practise modellen BiSL, ASL of ITIL en voor hun projectmanagement gebruik maakte van Prince2 hadden toch ook als doelstelling om betrouwbare en veilige systemen en infrastructuur op te leveren die voldoen aan de eisen van de business en binnen de tijd en budget opgeleverd worden.

Om antwoord te geven op deze laatste vraag is het goed om eens te kijken of de wijze van organiseren van de klassieke voortbrengingsketen wel past bij de noodzaak van snelle verandering.
Om hier een beeld van te krijgen wordt gebruik gemaakt van de organisatievormen die Mintzberg onderkent. Hij heeft een vijftal (later 7) organisatiestructuren onderscheiden die horen bij een verschillende groeifase van een organisatie maar belangrijker nog bij een verschillende omgeving waar deze organisatie in opereert. Uit zijn typologie worden twee organisatiestructuren genomen die passen bij de traditionele IV-voortbrengingsketen en de DevOps IV-voortbrengingsketen. De klassieke IV-voortbrengingsketen die gekenmerkt wordt door specialisten die georganiseerd zijn in groepen en gestandaardiseerde processen past bij de machine bureaucratie zoals Mintzberg die beschrijft.
In dit soort organisaties draait het om specialistische, routinematige werkzaamheden en procedures. Deze organisatievorm is weinig gevoelig voor veranderingen in de buitenwereld. In de machine bureaucratie is de technostructuur (wij zouden staf zeggen) het belangrijkste onderdeel en vindt coördinatie plaats door standaardisering van werkzaamheden.
De adhocratie of innovatieve organisatievorm past meer bij de DevOps ingerichte IV-voortbrengingsketen. Hierbij draait het om teams die in een wisselende verbanden samenwerken om op de ontwikkelingen in de markt in te spelen. Een innovatieve organisatie leent zich goed voor het snel in spelen op veranderingen in de markt en op specifieke vragen van klanten. Deze organisatievorm komt veel voor in turbulente markten. De uitvoerende kern en ondersteunende diensten zijn de belangrijkste onderdelen en is het belangrijkste coördinatiemechanisme de onderlinge afstemming.
Deze korte analyse laat zien dat de inrichting en coördinatiemechanisme van de klassieke voortbrengingsketen niet past bij de turbulente omgeving waarin de organisatie opereert.
Een beheersingssysteem dat gericht is op beheersing van de procesgang is namelijk van nature sterk bureaucratisch hetgeen ernstige negatieve bijeffecten kan hebben in een dynamische en veranderende omgeving. Merchant [13] noemt in dit kader een aantal operational delays die in een dergelijke omgeving vertragend werken. Hij noemt o.a. functiescheidingen, processtappen, budgetgames etc. Of zoals Patrick Debois [17] 1 van de founders van de DevOps movement het zegt:

“Despite all the great methodologies we have in IT, delivering a project to production still feels like going to war”.
Om tot een snellere levering van betrouwbare en hoge kwaliteit software te komen moet er een brug geslagen worden tussen development en Operations. De opdeling in Silo’s moet plaats maken voor intensieve samenwerking en communicatie tussen deze twee afdelingen. Een succesvolle implementatie van DevOps behelst een goede combinatie van mensen, cultuur, processen, tools en methodes die bijdragen aan de vermindering van de risico’s en kosten, die bijdraagt aan de snelheid van verandering van technologie die de snelheid van de business kan bijhouden en die de overall kwaliteit verbetert [9].

Zoals in de typologie van Mintzberg aangegeven moet er steeds intensiever samengewerkt gaan worden tussen de verschillende stakeholders binnen de IV-voortbrengingsketen. De businesseigenaren, development, operations en quality assurance moeten zodanig gaan samenwerken dat software continu geleverd kan worden en de business daardoor direct kan inspelen op kansen binnen de markt en eerder feedback van de klanten kunnen meenemen [14].
De veranderingen in de manier van werken binnen de IV-voortbrengingsketen - multidisciplinaire aanpak en automatisering binnen de OTAP straat hebben gevolgen voor de bestaande beheerskaders en beheersmaatregelen die nog uitgaan van handmatige overdrachten tussen de verschillende fases en processen binnen deze keten.
Hierin zal een verandering moeten plaatsvinden omdat dit niet meer past bij een integrale aanpak als DevOps.

1.3 Doel- en vraagstelling

De traditionele inrichting van de IV-voortbrengingsketen is het gevolg van een groeiproces gedurende decennia, waarbij in het verleden is geleerd hoe de risico’s bij wijziging en beheer van IT-diensten dusdanig beheerst kunnen worden dat betrouwbare en veilige diensten geleverd kunnen worden die voldoen aan de behoefte van de business. De continuïteit van de bedrijfsprocessen wordt daarmee gewaarborgd.
Het invoeren van DevOps binnen de IV-voortbrengingsketen is een drastische verandering ten opzichte van de traditionele inrichting en de wijze van beheersing. Daarbij is nog veel onduidelijkheid over wat er wordt afgedekt in de nieuwe wijze van beheersing en wat niet.
DevOps heeft mogelijk effect op de wijze van beheersing en verandert mogelijk de keuze in type beheersmaatregelen.
In dit onderzoek worden de oude en nieuwe wijze van beheersing bestudeerd om de veranderingen helder te maken. De inzichten die hiermee opgedaan worden, kunnen aanknopingspunten bieden voor de manier waarop de It auditor de beheersing kan onderzoeken in een DevOps ingerichte IV-voortbrengingsketen.
De centrale vraag die in dit onderzoek wordt beantwoord is wat de consequenties zijn van DevOps voor de wijze van beheersing binnen de IV-voortbrengingsketen wanneer deze keten in zijn geheel intern is georganiseerd.

Om deze centrale vraag te kunnen beantwoorden zijn drie deelvragen geformuleerd.

- Wat zijn kenmerken van de traditionele en DevOps georiënteerde inrichting van de IV-voortbrengingsketen en welke beheersmaatregelen zijn getroffen met betrekking tot het wijzigen en beheren van IT-diensten zodat deze (blijven) voldoen aan de requirements van de business.
- Welke verschillen in de wijze van beheersing zijn te vinden met betrekking tot het wijzigen en beheren van IT-diensten.
- Wat betekenen deze verschillen in beheersing voor de gevraagde snellere levering van flexibele, betrouwbare, veilige en kosten effectieve IT-diensten.

1.4 Afbakening van het onderzoek

Een eerste afbakening die in dit onderzoek wordt gemaakt zijn de IT domeinen die in de beschouwing over de IV voortbrengingsketen worden meegenomen. Dit zijn de twee domeinen ontwikkeling (development) en beheer (operations). De beschouwing over beheersing gaat over deze twee domeinen en de relatie daartussen. Er wordt niet dieper gekeken naar de processen of fases binnen deze domeinen.

Software ontwikkeling [30] is het proces van programmeren, documenteren, testen en bug fixing om te komen tot het creëren en onderhouden van een software product. Het bevat alles wat gedaan moet worden tot het begrip en ontwerp van tot het realiseren van de software.

Het doel van het andere domein operations of maintenance is volgens PWC [10] om er voor zorg te dragen dat de prestaties van de productiesystemen in lijn blijven met de beheersingsdoelstellingen van het management en dat performanceproblemen geïdentificeerd en accuraat opgelost worden.

Een tweede afbakening is dat niet de risico's worden meegenomen die gepaard gaan met de uitbesteding van IT-diensten. In dit onderzoek wordt er vanuit gegaan dat de ontwikkeling en onderhoud van applicaties en infrastructuur in zijn geheel plaatsvindt binnen de organisatie waar ook de business stakeholders deel van uitmaken. Uitbesteding van diensten brengt weer heel specifieke beheersingsuitdagingen met zich mee. Deze worden niet meegenomen in dit onderzoek.

1.5 Onderzoeksmethode

Om de centrale vraagstelling en geformuleerde deelvragen te kunnen beantwoorden is een literatuurstudie uitgevoerd. Hiervoor is gebruik gemaakt van artikelen op websites, onderzoeksrapporten, white papers van experts en wetenschappelijke literatuur.

Om de betrouwbaarheid van gebruikte literatuur te waarborgen is zo veel mogelijk gebruik gemaakt van erkende instituten (bijvoorbeeld ISACA) en schrijvers binnen het vakgebied. Echter niet alle informatie kon gevonden worden in wetenschappelijke literatuur. In dat geval zijn ook white papers en artikelen op websites gebruikt en hierbij is ingeschat of het toonaangevende instituten, auteurs of bedrijven zijn op dit gebied om deze informatie in dit onderzoek mee te kunnen nemen.

Belangrijk criterium hierbij was vooral of in de artikelen, rapporten of white papers gebruik is gemaakt van bronverwijzingen waarop de informatie is gebaseerd.

2 Beheersen van risico's en onzekerheden

2.1 Het begrip beheersing

Organisaties en projecten zijn samenwerkingsverbanden die bestaan omdat een groep van mensen een bepaald doel wil bereiken. Vaassen [3] geeft aan dat beheersing erop gericht is dat organisaties of projecten op een zo efficiënt mogelijke wijze de gestelde doelen kunnen realiseren. Beheersing zegt hij is dan het op koers houden van de organisatie of project in de richting van de gestelde doelen. Molenkamp [5] beschrijft het nog iets uitgebreider en benoemt de gebieden waar de beheersing betrekking op heeft. Beheersing is voor hem de manier waarop de organisatie als geheel, de organisatieonderdelen afzonderlijk, de verschillende kritieke succesfactoren en de complexe operationele en ondersteunende processen zodanig beheerst worden dat de geformuleerde doelstellingen kunnen worden bereikt. Dat betekent dus dat er verschillende objecten van beheersing kunnen zijn. Dit is in het kader van deze literatuurstudie van belang omdat de scope van een agile of DevOps team breder kan zijn dan alleen een systeem.

In de Engelse literatuur wordt voor de term beheersing het woord control gebruikt.

Beheersing bestaat volgens Vaassen [3] uit een aantal elementen:

- Een constituerend element wat het treffen van zodanige organisatorische maatregelen inhoudt dat afwijkingen van vastgestelde criteria – bijvoorbeeld standaarden of doelen - zo veel mogelijk worden voorkomen.
- Een terugkijkend element wat het afleggen van verantwoording, het detecteren van afwijkingen van gestelde criteria en het nemen van corrigerende maatregelen inhoudt.

- Een vooruitkijkend element wat het nemen van beslissingen inhoudt om afwijkingen van gestelde criteria tot een minimum te beperken.

Projecten en organisaties vinden echter plaats in een omgeving die van invloed is op het behalen van de gestelde doelen. Er vinden allerlei gebeurtenissen plaats zowel binnen als buiten het project of organisatie die aandacht verdienen omdat zij van invloed kunnen zijn op het bereiken van de gestelde doelen. De begrippen risico, dreiging als onzekerheid worden met deze gebeurtenissen in verband gebracht.
In dit onderzoek wordt bewust de term beheersing gebruikt. Beheersing omvat zowel het managen van risico's, dreigingen en onzekerheden omdat deze allemaal van invloed kunnen zijn op het bereiken van de gestelde doelen. Beheersing is dus gericht op het vergroten van de zekerheid dat doelen gehaald zullen worden. De begrippen hebben een wezenlijk andere betekenis in relatie tot beheersing. Daarom worden deze drie begrippen in de volgende paragraaf nader toegelicht.

2.2 Risico, dreiging en onzekerheid

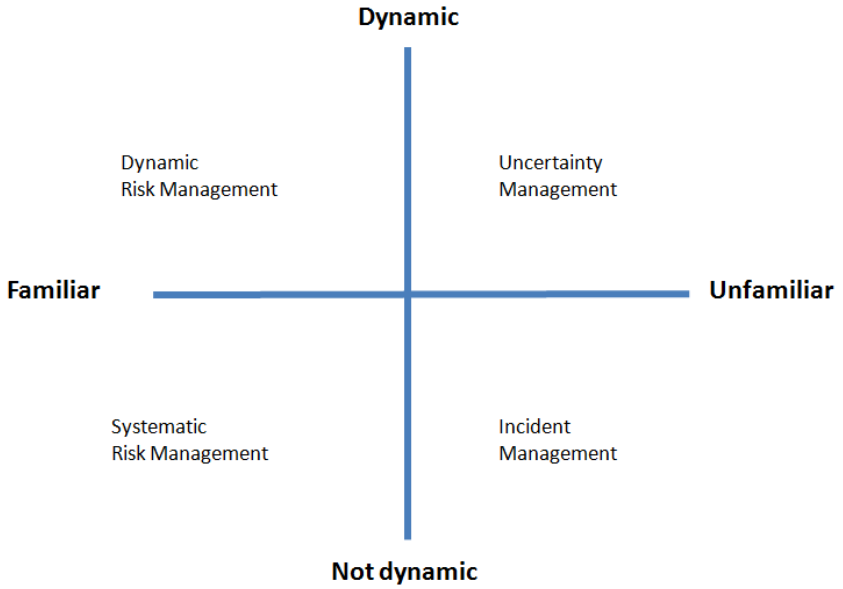
In deze paragraaf wordt dieper ingegaan op de begrippen risico, dreiging en onzekerheid omdat die een relatie hebben met beheersing en het vermogen van de organisatie/project om de doelstellingen te realiseren. Zoals Frijns in dit verband aangeeft [6] hebben programma's/projecten als doel om de gewenste veranderingen te realiseren terwijl de primaire processen gewoon zo veel mogelijk door moeten kunnen gaan zonder verstoringen. Dit lijkt gemakkelijk maar is het niet. Een wijziging brengt onzekerheden en risico's voor de omgeving met zich mee terwijl het primaire proces gebaat is bij stabiliteit. Maar ook de projecten brengen zelf onzekerheden en risico's met zich mee. Er is immers geen garantie dat de beoogde doelen ook daadwerkelijk gerealiseerd worden. Om te kunnen omgaan met deze onzekerheden en risico's worden beheersmaatregelen geïmplementeerd.
Het COSO/ERM-model [22] gebruikt daarbij de volgende definitie van een risico: de kans dat een ongewenste gebeurtenis met negatieve gevolgen (bedreiging) zich voordoet waardoor het realiseren van organisatiedoelstellingen in gevaar komt. Risicobeheersing volgens COSO/ERM is dan een binnen de gehele organisatie ingebed, proactief en continu proces, waarbij vanuit een gemeenschappelijk referentiekader op gestructureerde wijze wordt omgegaan met het beheersen van risico's in relatie tot organisatiedoelstellingen. Hier wordt er dus vanuit gegaan dat het onderkennen en beheersen van risico's continue aandacht moet hebben binnen organisaties. Dit blijkt ook uit de conclusie die Frijns trekt [6] n.a.v. een analyse van de aanbevelingen uit de gateway review op project met hoog risico. Hij trekt de conclusie dat wordt aanbevolen om risicomanagement meer te integreren in de aanpak van het project. Daarnaast moet er expliciete aandacht zijn voor de selectie en toepassing van geschikte preventieve en/of mitigerende maatregelen.
Deze benadering gaat ervan uit dat risico's vooraf allemaal onderkend kunnen worden. Maar in het onderzoek van Frijns [6] wordt door de deelnemers erkend dat het per definitie onmogelijk is om vooraf alle mogelijke onzekerheden en bedreigingen voor het project te identificeren en hier al op te anticiperen. De projecten veroorzaken immers zelf al enige turbulentie en worden uitgevoerd in een dynamische en turbulente omgeving. Het is paradoxaal genoeg een zekerheid dat een project te maken krijgt met onzekerheden, maar het is aan de andere kant onbekend welke onzekerheden dit zijn. Taleb [15] heeft hierover een duidelijke mening. Hij zegt dat risico's en waarschijnlijkheden van gebeurtenissen niet berekend kunnen worden ook al gebruiken we nog zo'n intelligente methodes. Risicomanagement zegt hij zoals het nu wordt uitgevoerd is de studie van een gebeurtenis die in de toekomst gaat plaatsvinden en alleen economen en andere dwazen beweren tegen beter weten in de gevolgen van deze gebeurtenissen te kunnen meten. De experts gebruiken volgens Taleb een model dat bestaat uit de "known-knowns" (de risico's waarvan we ons bewust zijn en die we adequaat geadresseerd hebben) of de "known-unknowns" (de risico's waarvan we ons bewust zijn maar die we niet adequaat geadresseerd hebben). Ze zijn echter overwegend blind voor de "unknown-unknown".

Frijns [6] komt in zijn onderzoek tot de conclusie dat ondanks deze kennis er toch vaak binnen projecten een systematische en procedurele aanpak van riskmanagement wordt gekozen die beter past bij een voorspelba-

re en maakbare wereld. De risicoanalyse wordt uitgevoerd bij de start en belangrijke mijlpalen in het project. Op die momenten worden de potentiële risico's geïdentificeerd en ingeschat en mogelijke maatregelen vastgesteld. Gedurende de uitvoering van het project wordt een risklog bijgehouden waarin de incidenten en mitigerende maatregelen worden bijgehouden voor de verantwoording.
Frijns [6] signaleert een paradox tussen de toepassing van systematisch risicomanagement en projecten die in een dynamische omgeving plaatsvinden waarbij meer het omgaan met onzekerheden en bedreigingen gevraagd wordt. In veel publicaties wordt ervoor gepleit om de dynamiek en onzekerheid de omarmen als onderdeel van een geïntegreerde risicobenadering.

2.3 Beheersingsstrategieën

Frijns beschrijft in zijn paper [5] dat er verschillende strategieën zijn van beheersing. Hij doet dat aan de hand van twee dimensies namelijk stabiel tegenover dynamisch en bekend tegenover onbekend. In onderstaande figuur zijn in de kwadranten de strategieën van beheersing geplaatst.



Figuur 1: Beheersing strategieën

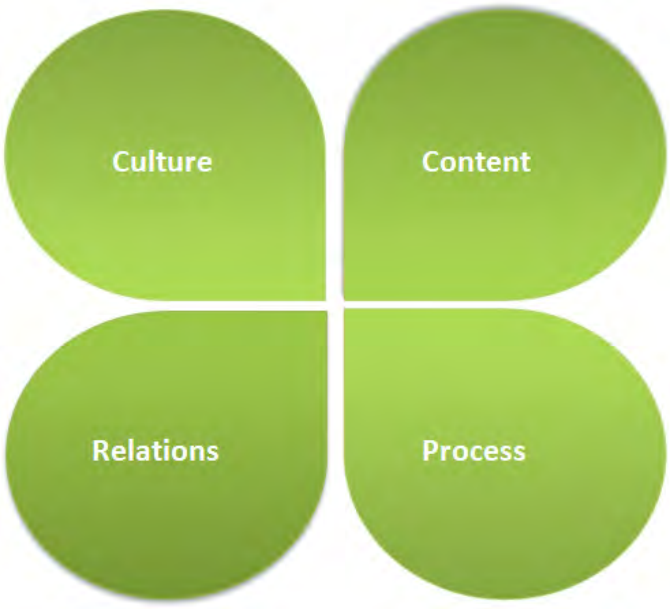
Deze strategieën van beheersing kunnen afgezet worden tegen de uitgangspunten waarop de traditionele en DevOps wijze van inrichting van de IV-voortbrengingsketen zijn gebaseerd. In onderstaande tabel zijn de uitgangspunten voor traditioneel en Agile tegenover elkaar gezet.

Uitgangspunten	Uitgangspunten
Traditioneel	Agile/DevOps
Stabiele omgeving	Dynamische en veranderende omgeving
Maakbaar en voorspelbaar	Omgaan met onzekerheden en bedreigingen.
Gericht op resultaat	Gericht op te bereiken doel
Lineair gericht proces met duidelijke producten en mijlpalen	Samenwerking tussen mensen

Een effectieve beheersing bevat een evenwichtige mix van de vier beheersingsstrategieën. In de traditionele benadering die uitgaat van een stabiele maakbare wereld zullen voornamelijk de strategieën uit de linker helft van het kwadrant gebruikt worden met de nadruk op systematisch risicomanagement. Onzekerheid wordt niet meegenomen omdat uit gegaan wordt van een planning vooraf die gevolgd moet worden waarbij alle informatie vooraf al bekend is. Omdat er minder aandacht is voor onzekerheid, zal dit opgevangen moeten worden met het afhandelen van incidenten.
Binnen DevOps zal naar verwachting ook de beheersstrategie uit het kwadrant rechtsboven meegenomen worden omdat er meer ingespeeld wordt op onzekerheid en verandering. Daardoor zouden er minder incidenten afgehandeld hoeven te worden.

2.4 Succes van een veranderingstraject

Frijns beschrijft in zijn paper [5] een viertal gebieden die van invloed zijn op de mate waarin de doelen van een programma/project gehaald worden. Dit is afhankelijk van wat men wil bereiken (inhoud) en hoe men dit denkt te bereiken (proces). Dit worden over het algemeen de “harde’ factoren genoemd. Een aantal studies heeft laten zien dat ook de zogenaamde “zachte” factoren voor een groot deel bepalen of de doelen van een programma/project gehaald worden. Dit heeft een relatie met de mate van samenwerking (relaties) en de omvang van de verandering, waarvoor mogelijk een nieuwe houding en gedrag nodig is (cultuur). De 4 gebieden vormen samen de blaadjes van het klavertje vier. In onderstaande figuur is dit schematisch weergegeven.



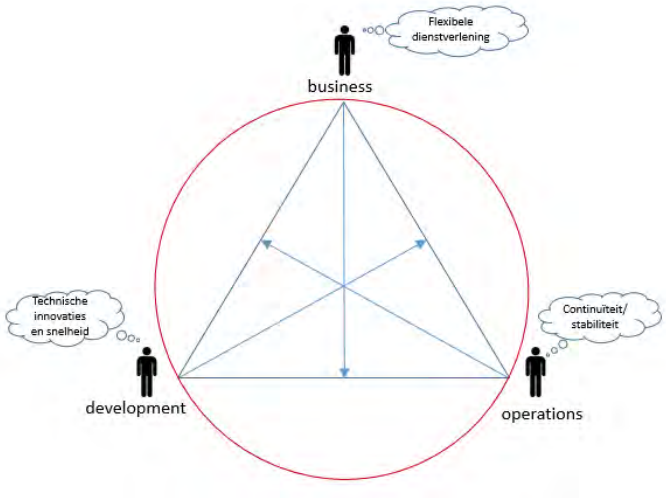
Figuur 2: Gebieden van invloed op succes behalen doelen

Uit zijn onderzoek blijkt dat de meeste beheersmaatregelen (70%) die aanbevolen worden voor beheersing van programma/projecten zich binnen het gebied Inhoud bevinden en als procedureel gekwalificeerd kunnen worden. Het laat een patroon zien van disbalans met de andere gebieden.
De nadruk bij het managen van programma’s/projecten ligt in grote organisaties vooral op het beheersen en besturen van taken zodat (onnodige) fouten kunnen worden voorkomen. Er worden veel procedurele en substantieve regelingen gebruikt en vaste patronen. Dit is in tegenspraak met de doorvoering van wijzigingen en het ontwikkelen van nieuwe producten en diensten. Innovatie en verandering vragen juist om nieuwe

(gedrags)patronen en methoden. Dit vraagt om het aanleren van “nieuw” gedrag en het afleren en niet meer laten zien van “oud” gedrag.

Deze constatering zou wel eens van belang kunnen zijn bij de analyse van de wijze van beheersing binnen de IV-voortbrengingsketen als hierin een meer traditionele of Agile/DevOps benadering gebruikt wordt. Immers Agile/DevOps gaat meer uit van een dynamische omgeving en samenwerking en communicatie tussen mensen. De traditionele benadering gaat meer uit van stabiliteit en planmatig werken.

Bij een IV-voortbrengingsketen zijn drie belangrijke stakeholders betrokken. Dit zijn naast de ontwikkelaars en de beheerders ook de vertegenwoordigers van de business (gebruikers).
Debois [17] beschrijft de verschillende belangen van de stakeholders. Hij geeft aan dat ontwikkeling de druk voelt om nieuwe features en functionaliteit zo snel mogelijk op te leveren aan de gebruikers terwijl beheer zo veel mogelijk wijzigingen probeert tegen te houden omdat ze weten dat wijzigingen een belangrijke oorzaak zijn van systeemuitval. Dit is weer frustrerend voor de gebruikers en de business die hierdoor niet in staat zijn om business value te leveren zoals verwacht en benodigd. Onderstaande figuur laat deze verschillende belangen van de stakeholders zien. Zij zijn daarbij continu op zoek naar de balans tussen belangen, omdat zij allemaal vanuit een ander perspectief bij de voortbrengingsketen betrokken zijn. De cirkel laat zien dat zij door hun verschillende belangen bij de verandering met elkaar verbonden zijn en afhankelijk zijn van elkaar.
In de verschillende fases van de SDLC cyclus zoeken de betrokken stakeholders steeds opnieuw naar de balans tussen deze belangen. De balans kan steeds anders zijn. De pijlen in de driehoek die wijzen naar de lijn tussen de stakeholders waar ze mee te maken hebben, laat deze spanning zien.



Figuur 3: Stakeholders met hun belangen

Het klavertje vier model en de onderkende gebieden worden in dit onderzoek samen met de onderkende beheersingsstrategieën gebruikt voor de analyse van de wijze van beheersing die gebruikt wordt binnen de traditionele en de DevOps georiënteerde inrichting van de IV-voortbrengingsketen. Door de beheersmaatregelen te beschrijven en daarna te plotten op 1 van de blaadjes van het klavertje vier wordt geanalyseerd hoe de beheersing van deze benaderingen eruit ziet.

Bovendien kan op die manier vastgesteld worden wat er in de wijze van beheersing binnen de IV-voortbrengingsketen wordt afgedekt en wat niet. Dit kan dan ook vastgesteld worden voor de wijze van beheersing binnen de DevOps IV-voortbrengingsketen.

3 Kenmerken van een traditionele en DevOps ingerichte IV-voortbrengingsketen

3.1 Inleiding

In dit hoofdstuk wordt de eerste deelvraag behandeld. Wat zijn de kenmerken van een traditioneel en DevOps ingerichte IV-voortbrengingsketen en welke beheersmaatregelen zijn te onderkennen met betrekking tot het wijzigen en beheren van IT-diensten zodat deze blijven voldoen aan de requirements van de business. Deze informatie wordt gebruikt in hoofdstuk 4 om de twee benaderingen met elkaar te kunnen vergelijken.

3.2 De traditioneel ingerichte IV-voortbrengingsketen

Om inzicht te krijgen in de wijze van inrichting van een traditionele IV-voortbrengingsketen en wat kenmerkend is voor een dergelijke inrichting wordt eerst aandacht besteed aan de achtergrond hiervan.
Schuyl en Nuijten [18] beschrijven dat de complexiteit van ICT componenten en de toename van de hoeveelheid koppeling daartussen de laatste decennia een flinke vlucht heeft genomen. Om dit te kunnen beheren was een verdere professionalisering van IT beheer noodzakelijk. Deze professionalisering werd verder gestuurd door de ontwikkeling van procesgerichte modellen zoals ITIL en Cobit. Hieraan zijn de procesmodellen BiSL voor informatiemanagement n ASL voor applicatie ontwikkeling nog toe te voegen. De implementatie van deze modellen gaat veelal gepaard met de introductie van nieuwe afdelingen, functies, onderlinge afhankelijkheden en wellicht bureaucratie in de ogen van de gebruikers.
Volgens Sharma en Coyne [14] wordt de traditionele IV-voortbrengingsketen gekenmerkt door ontwikkeling op basis van alleen wat de klant vraagt en handmatige processen. De betrokken teams.
zijn georganiseerd in afzonderlijke functionele afdelingen. De informatie die nodig is voor het plannen en herplannen is vaak gefragmenteerd aanwezig bij de verschillende teams en inconsistent. Als laatste wort feedback pas laat ontvangen waardoor het lastig is om het juiste niveau van kwaliteit te behalen.
Hartholt en Luistjes [26] beschrijven in hun onderzoek op basis van een literatuurstudie de kenmerken van een traditioneel ingerichte IV-voortbrengingsketen. Zij beschrijven dat teams worden ingericht op basis van hun verantwoordelijkheidsgebied. Dit worden silo's genoemd. Deze silo structuur werd begin van deze eeuw gezien als een beproefde methode voor het meten en verbeteren van het productieproces. Gedachte is dat organisaties functionele silo's gebruiken omdat dit zou leiden tot excellente performance en efficiënte processen. Tegenwoordig worden nog steeds deze silo's met specialisten gebruikt voor het managen van de IT-omgeving. Voorbeelden van silo's zijn dan een team gespecialiseerd in het coderen van software terwijl een ander team gespecialiseerd is in het testen van systemen. Een derde team zorgt er dan voor dat de ontwikkelde en geteste software naar productie gebracht wordt en is verantwoordelijk voor het beheer en onderhoud ervan. Elk team zorgt voor de invulling van zijn eigen requirements en stelt zijn eigen doelen die horen bij het soort werk dat ze uitvoeren. Op die wijze ontstaan er tegengestelde belangen zoals die tussen de ontwikkelaars die gericht zijn op snelheid en de beheerafdeling op stabiliteit.

3.3 Beheersing binnen de traditioneel ingerichte IV-voortbrengingsketen

Een systeemontwikkelmethode die past bij een traditioneel ingerichte IV voortbrengingsketen is de waterval methode. In deze aanpak komen de kenmerken van de traditioneel ingerichte IV-voortbrengingsketen naar voeren. Volgens Van Someren van PWC [20] is de watervalmethode een beheerste methode voor de ontwikkeling van nieuwe applicaties en functionaliteiten, waarbij
stap voor stap door verschillende functies gegaan wordt vanaf de originele specificaties, functioneel ontwerp, technisch ontwerp, datamodel, ontwikkelen, testen tot aan de inproductiename. Het resultaat van de voorgaande stap is de input voor de daaropvolgende stap, waarbij de oorspronkelijke specificaties als uitgangspunt worden gehanteerd voor

validatie van de juiste uitvoering van de processtappen. Dit maakt het watervalproces een goed beheersbaar en te controleren proces, waarbij de verschillende functionele expertises gescheiden van elkaar aan een deel van de totale eindoplossing werken. De communicatie tussen de verschillende functies binnen het totale ontwikkelproces is daarbij beperkt, en er zijn veel overdrachtsmomenten nodig voordat de functionaliteit in productie kan
worden genomen. De processen volgen elkaar dus sequentieel in een rechtlijnige beweging op.
Onderzoek van PWC [21] laat verder zien dat bij een dergelijke inrichting van een voortbrengingsketen een IT governance raamwerk noodzakelijk is waarbij de gedachte is dat als de IT governance verbetert dit een positieve bijdrage levert aan de verbetering van de productkwaliteit die opgeleverd wordt. Een dergelijk raamwerk bevat dan ook besluitvormingsprocessen, belanghebbenden, organisatiestructuren, verantwoordelijkheden en controls die nodig zijn om de toegevoegde waarde van IT te genereren en garanderen.

Een ander model dat past bij een traditioneel ingerichte IV-voortbrengingsketen is de projectmanagementmethode Prince2. Deze methode wordt veel gebruikt bij de uitvoering van projecten waarmee IT veranderingen worden doorgevoerd. Deze methode geeft inzicht in de wijze van beheersing zoals die veel wordt toegepast binnen de IV-voortbrengingsketen. Enkele belangrijke kenmerken [24] van Prince2 illustreren dit:

- Er is een continue focus op de zakelijke rechtvaardiging (Business Case) van het project.
- De organisatiestructuur voor het volledige projectmanagementteam is gedefinieerd.
- Niet alleen de taken en verantwoordelijkheden voor de Project Manager zijn beschreven, maar ook voor de Project Board. Hierdoor is betrokkenheid van management en belanghebbenden op de gewenste en vereiste momenten mogelijk.
- PRINCE2 hanteert Product-based planning als techniek; de planning richt zich primair op de beoogde resultaten (producten).
- Projectmanagement wordt beschreven als een proces, dat voor alle projecten soortgelijk is (rekening houdend met organisatiespecifieke en projectspecifieke kenmerken), ook al is ieder project op zich uniek qua resultaat, risico's, doelstellingen, stakeholders etc.
- De fasering van het project is niet star gedefinieerd (altijd dezelfde fasen), maar flexibel, gericht op een optimale bestuurbaarheid.
- Op basis van de Business Case (en de risico's) kan telkens besloten worden of het gerechtvaardigd en zinvol is om met het project door te gaan; dit noemen we de go/no-go beslissing per fase.

De kenmerken van de project aanpak Prince2 zijn een aanvulling op de watervalmethode zoals hiervoor beschreven en geven tezamen een goed beeld van de kenmerken van de inrichting van een traditioneel ingerichte IV voortbrengingsketen.

3.4 Wat is DevOps

In deze paragraaf worden de kenmerken van DevOps beschreven.
In het Agile Manifest [19] worden in de 4 uitgangspunten een aantal fundamentele verschillen beschreven tussen de traditionele benadering en de Agile/DevOps benadering. Dit zijn:

1 Mensen en hun onderlinge interactie boven processen and tools
2 Werkende software boven allesomvattende documentatie
3 Samenwerking met de klant boven contractonderhandelingen
4 Inspelen op verandering boven het volgen van een plan

In een Fins onderzoek [27] wordt aangegeven dat DevOps een fenomeen is waarvan gezegd wordt dat er nog geen echte duidelijke definitie is. Op basis van een literatuurstudie omschrijven zij DevOps als een mindset die de samenwerking over functionele gebieden heen in een software ontwikkelingsorganisatie aanmoedigt

(vooral ontwikkeling en beheer) om de ontwikkeling van weerbare systemen en versnelling van het doorvoeren van wijzigingen mogelijk te maken. Als aanvulling op deze definitie wordt in verschillende studies een aantal dimensies en karakteristieken genoemd zoals cultuur, delen, automatisering, samenwerking en meten.

DevOps is volgens Sharma en Coyne [14] een aanpak die gebaseerd is op principes uit lean en agile waarbij vertegenwoordigers van de business, development, operations en quality assurance samenwerken om continu nieuwe software op te leveren wat het voor de business in staat stelt om sneller in te spelen kansen op de markt en sneller gebruik kan maken van feedback van klanten. Ze geven verder aan dat de enterprise applicaties zo divers zijn en opgebouwd uit verschillende technologieën dat alleen een DevOps aanpak succesvol kan zijn bij het omgaan met de hiervoor beschreven complexiteit en onzekerheden. Ze hanteren daarbij een brede en holistische kijk op DevOps waarbij zij het zien als een business-gedreven software leveringsaanpak waarbij nieuwe functionaliteit door het gehele traject wordt gehaald van business idee tot oplevering in productie en direct waarde voor de business geleverd kan worden en direct bijgehouden kan worden wat de reactie van de klanten is.
Kim [28] geeft aan dat DevOps verwijst naar een opkomende professionele beweging waarin wordt gepleit voor een relatie tussen ontwikkeling en beheer gebaseerd op samenwerking die resulteert in een in een snelle doorstroming van gepland werk en tegelijkertijd de betrouwbaarheid, stabiliteit, weerbaarheid en veiligheid van de productieomgeving vergroot.
Het gaat vooral om ontwikkeling en beheer omdat zij belangrijk zijn in de waardestroom tussen de business waar de requirements worden gesteld en de klant waar de waardecreatie wordt geleverd. DevOps is ontstaan rond 2009 toen veel vergelijkbare en elkaar versterkende ontwikkelingen bij elkaar kwamen. Te noemen zijn de infrastructuur als code, lean startup beweging, continuous integration, de grote beschikbaarheid van cloud en platform as a service en de velocity beweging.
Samenvattend kunnen de volgende kenmerken van DevOps benoemd worden:

- Het is een samenvoeging van de woorden Development en Operations.
- Geen methode maar een filosofie of cultuur.
- Beweging met een set van practices dat de kloof tussen development en Operations probeert te overbruggen op de core activiteiten.
- Tegelijkertijd alle aspecten meeneemt die helpen bij het versnellen, optimaliseren en kwaliteitsverbetering bij de levering van software.
- Het probeert het agile denken in de gehele SDLC cyclus te brengen binnen de enterprise.
- DevOps bevat naast Development en Operations functies als governance, quality assurance (QA), testing, security and release management.
- DevOps is de combinatie van mensen, cultuur, processen, tools and methodes die zorgen voor het reduceren van risico's en kosten, het mogelijk maakt technologie meegaat in de snelheid van verandering van de business, en verbetert overall kwaliteit.

3.5 Beheersing binnen een DevOps ingerichte IV-voortbrengingsketen

DevOps is geen uitgewerkte methode en zoals geconstateerd is er ook nog geen overeenstemming over een eenduidige definitie. Dat maakt de beschrijving van gebruikte beheersmaatregelen lastig. Toch zijn er een vijftal zogenaamde pilaren te onderscheiden waarop de DevOps filosofie of beweging berust. Voor een effectieve adoptie moet er een goede balans zijn tussen de 5 pilaren. Zo leidt een overfocus op automation tot een organisatie die overal fantastische tools voor heeft, maar waar geen enkele vorm van samenwerking, empathie of verbeterkracht aanwezig is.
De 5 pilaren cultuur, automatisering, lean, meten en delen (sharing) worden aangeduid met het acroniem CALMS. De beheersing binnen DevOps is wellicht nog het beste te beschrijven aan de hand van de aspecten van de 5 pilaren van CALMS. De beschrijving van de 5 pilaren is voornamelijk ontleend aan het Sogeti rapport [1] Design to disrupt.

C — Culture: systeemdenken en een cultuur van 'fail fast' omarmen
Belangrijk elementen binnen de cultuur van DevOps zijn het systeemdenken, feedback loops versterken en continu experimenteren en leren.
Systeemdenken zorgt ervoor dat mensen over de silo's en afdelingen heen gaan kijken en geconstateerde fouten niet doorschuiven naar andere afdelingen. Het resultaat van het hele systeem is het uitgangspunt, niet het behalen van de KPI's van de afdeling. Dit denken vanuit het geheel en de totaalprestatie creëert de basis om in multidisciplinaire teams te gaan samenwerken.
Een tweede belangrijke cultuurelement binnen DevOps zijn de feedback loops. Ze zijn nodig om een end-to-end overzicht te krijgen van wat interne en externe klanten gelukkig maakt om op basis hiervan bijstellingen te kunnen doen.
Het laatste belangrijke cultuurelement binnen DevOps is het voortdurend leren en experimenteren. Het gaat hier over het creëren van de juiste cultuur die openstaat voor het nemen van risico's en het leren van fouten. Dit is een van de belangrijkste veranderingen waar men bij de invoering van DevOps mee te maken krijgt. Veel organisaties hebben nu nog een zogenaamde "angstcultuur". Hiermee wordt bedoeld een cultuur waarin men angstig is om fouten te maken, te innoveren en uit de toon te vallen. Bij DevOps wordt dit juist aangemoedigd om te experimenteren en te leren en snel te falen zoals veel startups die kennen. Gedachte is dat je er beter snel achter kunt komen dat iets niet werkt dan later als er al veel tijd en geld is geïnvesteerd.

A — Automation: automatiseer de Automatisering
Automatisering is het meest eenvoudige en meest zichtbare deel van DevOps. Het doel is zo veel mogelijk van het softwareproces te automatiseren. Het idee achter 'automation' is dat alles wat kan worden geautomatiseerd, ook daadwerkelijk geautomatiseerd moet worden. Dit kan alle handelingen omvatten zoals het opzetten van een omgeving, het laden van datasets tot het uitvoeren van performancetests. Deze automatisering heeft een directe invloed op de snelheid en de kwaliteit van het software ontwikkelingsproces omdat handmatige handelingen die foutgevoelig zijn zo veel mogelijk uit het proces worden gehaald d.m.v. geautomatiseerde processen. Er zijn minder helden nodig die ad hoc moeten ingrijpen om problemen op te lossen. Waarschijnlijk kan in de praktijk niet alles worden geautomatiseerd, omdat er vaak nog menselijke checkpoints nodig zijn.
Er zijn veel tools die allemaal een bijdrage kunnen leveren aan de automatisering van een gedeelte van het software ontwikkelingsproces. Te noemen zijn versiebeheer, packaging en testautomatisering. Een specifieke tool die snel aan populariteit wint, is Docker, dat het gebruik van 'containers' mogelijk maakt. Het is een virtualisatie oplossing waarmee zeer eenvoudig applicaties kunnen worden verplaatst van de ene omgeving naar de andere, van de desktop naar de cloud of van de ene cloud naar de andere.

L — Lean: verspilling tegengaan met Lean
Bij lean in Dev-Ops gaat het net als in een Lean Startup vooral om 3 zaken. Allereerst moet de inspanning binnen de organisatie gericht zijn op verbetering van de innovatiekracht en het realiseren van de nieuwe of latente klantbehoeftes. Op de tweede plaats moet de organisatie bezig zijn met het meten en optimaliseren van de productiviteit in het hele systeem. Als laatste het feit dat binnen DevOps net als bij lean het gaat om succesvolle samenwerking binnen het systeem.
De obsessieve focus op de klantwaarde zorgt ervoor dat weinig tijd wordt verspild aan zaken die geen waarde toevoegen. De cultuur van snel falen hoort daarbij, net als de Minimum Viable Product-benadering. Al deze holistische elementen die we zagen in Lean Start up, zien we terug in DevOps. Dus ook de empowerment van de zelfsturende teams.

M — Measure: meten door de hele keten
Binnen deze pilaar ligt de nadruk op het meten van prestaties binnen het software ontwikkelingsproces. Hoeveel releases zijn er geweest afgelopen week? Waar ging het mis? Hoe reageerden de klanten erop en

welke verbeteringen hebben nu echt gewerkt? De automatisering van het operationele proces levert een schat aan informatie, die nu met DevOps ter beschikking komt in de hele keten. De ontwikkelaars worden geconfronteerd met de onvolkomenheden van de operatie en de mensen aan de kant van de operatie zien het effect op de klant. Waar voorheen wel werd gemeten werd dit gefragmenteerd gepresenteerd. Iedere afdeling of team zag alleen het stukje dat voor hen van belang was. Nu ziet het DevOps-team in 1 oogopslag informatie uit de gehele keten. De verantwoordelijkheid voor de benodigde verbeteringen ligt bij hetzelfde multidisciplinaire team. Maar wat nog veel belangrijker is, is de mogelijkheid die feedback loops bieden om businesshypotheses te toetsen die nieuwe innovaties kunnen opleveren.

S — Sharing: versneld leren door sharing
Het delen van kennis en ervaringen binnen en buiten teams is cruciaal voor het succes van DevOps. Sommigen noemen dit onderdeel van DevOps het realiseren van een 'open-source cultuur'. Het sharingprincipe gaat niet alleen op voor het werken binnen de DevOps-teams. Het gaat juist ook om het delen van tools, ervaringen, een architectuur of code tussen de teams. Hierdoor kunnen de leerervaringen in de diverse teams snel schalen.

Aanvullend op deze beschrijving van de 5 DevOps pilaren beschrijft Wright [25] in zijn vergelijking van de traditionele projectmanagementmethodes en SCRUM ook een aantal beheersingsmaatregelen van agile/DevOps. Dit zijn:
- Geen end to end plan maar alleen een korte sprint wordt gepland;
- project backlog die aan het einde van de sprint gereviewd wordt;
- Zo min mogelijk documentatie. Voornamelijk wat nodig is voor de gebruiker;
- Elke iteratie levert werkende software op.

Tenslotte wordt ook in het Agile manifest [19] in de onderliggende principes een aantal beheersmaatregelen genoemd. Te noemen zijn:
- Verwelkom veranderende behoeftes, zelfs laat in het ontwikkelproces. Agile processen benutten verandering tot concurrentievoordeel van de klant.
- tevredenstellen van de klant door het vroegtijdig en voortdurend opleveren van waardevolle software.
- Lever regelmatig werkende software op. Liefst iedere paar weken, hooguit iedere paar maanden.
- Mensen uit de business en ontwikkelaars moeten dagelijks samenwerken gedurende het gehele project.
- Bouw projecten rond gemotiveerde individuen. Geef hen de omgeving en ondersteuning die ze nodig hebben en vertrouw erop dat ze de klus klaren.
- De meest efficiënte en effectieve manier om informatie te delen in en met een ontwikkelteam is door met elkaar te praten.
- Werkende software is de belangrijkste maat voor voortgang.
- Agile processen bevorderen constante ontwikkeling. De opdrachtgevers, ontwikkelaars en gebruikers moeten een constant tempo eeuwig kunnen volhouden.
- Voortdurende aandacht voor een hoge technische kwaliteit en voor een goed ontwerp versterken agilty.
- Eenvoud, de kunst van het maximaliseren van het werk dat niet gedaan wordt, is essentieel.
- De beste architecturen, eisen en ontwerpen komen voort uit zelfsturende teams.
- Op vaste tijden, onderzoekt het team hoe het effectiever kan worden en past vervolgens zijn gedrag daarop aan.

In het volgende hoofdstuk worden de onderkende beheersmaatregelen geplot op de blaadjes van het klavertje vier en wordt de wijze van beheersing met elkaar vergeleken.

4 Vergelijking van de beheersing binnen de traditionele en DevOps ingerichte IV-voortbrengingsketen

4.1 Inleiding

In dit hoofdstuk wordt de tweede deelvraag behandeld. Welke verschillen in de wijze van beheersing zijn te vinden met betrekking tot het wijzigingen en beheren van IT-diensten.
Om deze vraag te kunnen beantwoorden, worden allereerst in paragraaf 4.2 en 4.3 de beheersmaatregelen die in het vorige hoofdstuk onderkend zijn binnen de traditionele en DevOps ingerichte IV-voortbrengingsketen geplot op de vier gebieden die van invloed zijn op het behalen van de doelen van een veranderingstraject. In paragraaf 4.4 worden de resultaten van de plotting met elkaar vergeleken en geanalyseerd waar overeenkomsten en verschillen zitten in de wijze van beheersing. Daarnaast kan vastgesteld worden waar eventuele tekortkomingen liggen in de wijze van beheersing met betrekking tot de gewenste balans tussen de aandachtsgebieden, de wijze van omgaan met verandering en onzekerheid en de aanwezigheid van voldoende dialoog over onzekerheden en bedreigingen. Als laatste wordt gekeken naar de betrokken stakeholders en de balans die gezocht wordt in de belangentegenstellingen waar zij mee te maken hebben zoals geïllustreerd in de driehoek in paragraaf 2.4.

4.2 Wijze van beheersing binnen de traditionele IV-voortbrengingsketen

De onderkende beheersmaatregelen van de traditioneel ingerichte IV-voortbrengingsketen zoals beschreven in paragraaf 3.3 zijn in onderstaande tabel geplot op de vier aandachtsgebieden die van invloed zijn op het behalen van de doelen van een veranderingstraject. Dit zijn de 4 blaadjes van het Klavertje vier.

Cultuur	Inhoud
Betrokkenheid stakeholders via geformaliseerde overlegstructuren (stuurgroep, change advisory board etc.)	Vooraf vastgestelde requirements Er is een continue focus op de zakelijke rechtvaardiging (Business Case) van het project Scope is vooraf gedefinieerd en kan tijdens de uitvoering alleen onder strikte beheersing gewijzigd worden Vooraf vastgestelde Acceptatie criteria) Resultaten vooraf bepaald
Relatie	**Proces**
Functionele expertises werken gescheiden van elkaar aan een deel van de totale eindoplossing met beperkte communicatie	Duidelijke fases met eindproduct Sequentieel/lineair doorlopen van fases Doorlopen stappen requirements, functioneel en technisch ontwerp, datamodel, coderen, testen productiename Start volgende fase bij validatie vorige fase Steeds hanteren van oorspronkelijke requirements bij beoordeling juistheid uitvoering fase overgangen Bij fouten of (scope) wijzigingen terug naar vorige fase voor analyse en impactbepaling Volgen vooraf opgezet plan Faseplanning (tijd, geld doorlooptijd, resources) Contract volgende fase Hiërarchische organisatiestructuur is gedefinieerd Gestandaardiseerde en herhaalbare processen over functionele gebieden heen Duidelijk omschreven taken, bevoegdheden en verantwoordelijkheden Systeemdocumentatie

4.3 Wijze van beheersing binnen DevOps

Net als in de vorige paragraaf voor de beheersmaatregelen van de traditionele IV-voortbrengingsketen is gedaan, worden in onderstaande tabel de in paragraaf 3.5 onderkende beheersmaatregelen van een DevOps ingerichte IV-voortbrengingsketen geplot op de 4 blaadjes van het Klavertje vier.

Cultuur	Inhoud
Delen van kennis en ervaringen binnen en buiten teams wat snel leren mogelijk maakt. Continu onderzoeken hoe effectiever gewerkt kan worden en aanpassing van gedrag. De beste architecturen, eisen en ontwerpen komen voort uit zelfsturende teams. Bouw projecten rond gemotiveerde individuen. Geef hen de omgeving en ondersteuning die ze nodig hebben en vertrouw erop dat ze de klus klaren. Systeemdeken waarbij over de eigen grens wordt gekeken en fouten zelf worden opgelost. Cultuur van continu leren en experimenteren. Focus op klantwaarde en alleen doen wat daarvoor nodig is. Aanpassen op basis van feedback loops en metingen. Continu toetsen van klanthypotheses.	Dynamische productbacklog Continue business planning op basis van klantfeedback verwelkom veranderende behoeftes, zelfs laat in het ontwikkelproces. Agile processen benutten verandering tot concurrentievoordeel van de klant.

Relatie	Proces
Vaste multidisciplinaire teams: alle specialismen vertegenwoordigd. Team verantwoordelijkheid voor behalen doelen. Continue betrokkenheid business owner. Continue samenwerking binnen team. De meest efficiënte en effectieve manier om informatie te delen in en met een ontwikkelteam is door met elkaar te praten.	Automatisering van (handmatige) processen. Continu testen en verbeteren van deployment processen. Regelmatige release kleine wijzigingen Korte iteraties waarin hele SDLC cyclus wordt doorlopen en werkende software wordt opgeleverd. shift-left concept: testen in een productie-like omgeving. Monitoring productie omgeving op basis van begrijpelijke en realtime informatie die directe bijstelling mogelijk maakt voor alle betrokken stakeholders. Samenwerking d.m.v. gebruik van een gemeenschappelijke set van practises en platforms. Continu integreren en testen van verschillende software componenten waardoor bekende en onbekende risico's onderkend worden.

4.4 Vergelijking van de wijze van beheersing

In deze paragraaf worden op basis van de twee tabellen uit de vorige paragraven de wijze van beheersing van de traditioneel en DevOps ingerichte IV-voortbrengingsketen met elkaar vergeleken. Als eerste wordt beschreven welke aspecten door de beheersing van beide benaderingen wordt afgedekt. Daarna wordt beschreven welke aspecten niet of onvoldoende worden afgedekt door de beheersing binnen de traditionele benadering maar wel binnen de DevOps benadering. Als laatste wordt beschreven welke aspecten niet of onvoldoende worden afgedekt door de beheersing binnen DevOps.

Aspecten afgedekt in beide benaderingen

Als eerste valt op dat de beheersing van beide benaderingen erop gericht is om de risico's te mitigeren met betrekking tot het kunnen garanderen van een betrouwbare, veilige en stabiele productie-omgeving. In de traditionele benadering worden hiervoor voornamelijk beheersmaatregelen gebruikt vanuit de gebieden inhoud en proces. Belangrijke beheersmaatregelen hierbij zijn het gebruik van gestandaardiseerde en herhaalbare processen, inrichting van een governancestructuur met besluitvormingsprocessen en beschrijving van taken, bevoegdheden en verantwoordelijkheden, en het sequentieel doorlopen van fases met duidelijke producten en kwaliteitschecks. De DevOps benadering gebruikt voor de beheersing van deze risico's andere beheersmaatregelen vanuit het gebied proces en relatie. Belangrijkste beheersing komt vanuit de continue samenwerking binnen multidisciplinaire teams die gezamenlijke verantwoordelijkheid dragen voor de te behalen doelen. Vanuit het procesgebied zijn hier nog aan toe te voegen de automatisering van (handmatige) processen, continu testen en verbeteren van deployment processen, regelmatige release van kleine wijzigingen, korte iteraties waarin hele SDLC cyclus wordt doorlopen en werkende software wordt opgeleverd.
Op de tweede plaats valt op dat ook de risico's van het opleveren van functionaliteit die niet voldoet aan de requirements van de business door beide benaderingen wordt afgedekt. In de traditionele benadering wordt dit gedaan door het vooraf met de business vaststellen van de requirements en hierop steeds teruggrijpen bij afsluiting van een doorlopen fase om te bezien of de tussenproducten nog steeds in lijn zijn met de vastgestelde requirements. Verder is de business betrokken via de Betrokkenheid van stakeholders in geformaliseerde overlegstructuren (stuurgroep, change advisory board etc.). In de DevOps benadering gaat dit via een continue betrokkenheid van de business binnen de vaste teams en de verantwoordelijkheid van de business

voor het beheer van de productbacklog en het prioriteren daarvan. Deze prioritering gebeurt ook op basis van de continu aanwezige klantfeedback. In zijn algemeenheid kan de conclusie getrokken worden dat de nadruk van de beheersing van deze aspecten bij de traditionele benadering meer ligt op de harde factoren binnen de gebieden inhoud en proces. Bij DevOps vindt een verschuiving plaats naar de gebieden relatie en cultuur. Processen worden niet losgelaten maar in hoge mate geautomatiseerd. Samenwerking en communicatie binnen en tussen teams wordt belangrijk binnen de beheersing.

Wat wordt niet of onvoldoende afgedekt in de traditionele benadering maar wel in DevOps

Als eerste valt op dat veranderende behoefte maar beperkt door de beheersing wordt afgedekt. De nadruk ligt op het volgen van de vooraf opgestelde planning met mijlpalen. Wijzigingen die zich tijdens de uitvoering van het veranderingstraject voordoen kunnen alleen onder strikte beheersing gewijzigd worden. Daarbij moet bij fouten of wijziging in de scope of requirements steeds terug gegaan worden naar vorige fasen impactbepaling van de wijziging. Een tweede aspect dat in mindere mate wordt afgedekt binnen de traditionele benadering is de behoefte van de business aan een steeds snellere oplevering van functionaliteit. Zoals aangegeven ligt de focus van de beheersing op het gecontroleerd doorvoeren van wijzigingen waarbij de productie-omgeving zo min mogelijk verstoord wordt. Hierbij horen duidelijke gestandaardiseerde processen, het doorlopen van fases met duidelijke tussenproducten en vooraf bepaalde mijlpalen en besluitvormingsmomenten. Als we kijken naar de driehoek van betrokken stakeholders en de belangentegenstellingen waarmee zij te maken hebben, dan lijkt er meer rekening gehouden te worden met het belang van de beheerders aan stabiliteit dan de belangen van de business en ontwikkelaars aan snelle en flexibele opleveringen.

Een laatste aspect wat nog genoemd moet worden dat onvoldoende wordt afgedekt binnen de traditionele benadering is het managen van onzekerheden. Zoals in hoofdstuk 2 aangegeven is hiervoor een continue dialoog en uitwisseling van informatie voor nodig tussen de stakeholders. De beheersmaatregelen die binnen de gebieden relatie en cultuur zijn gevonden, lijken dit niet te ondersteunen. Functionele expertises werken gescheiden van elkaar aan een deel van de totale eindoplossing met beperkte communicatie en de betrokkenheid van stakeholders verloopt voornamelijk via geformaliseerde overlegstructuren.

De hiervoor genoemde aspecten die in de traditionele benadering niet of onvoldoende worden afgedekt worden door de beheersing binnen de DevOps benadering wel afgedekt. Als we kijken naar het aspect verandering. Dan is een uitgangspunt van DevOps al dat verandering omarmd moet worden ook al vind deze laat in het veranderingstraject plaats. Dit gebeurt door beheersmaatregelen binnen het gebied inhoud. Agile en DevOps maken gebruik van een dynamische productbacklog en continue business planning op basis van klantfeedback. Er wordt niet gewerkt met een vooraf vastgestelde planning maar er wordt continu op basis van de dynamische backlog en de vastgestelde prioriteiten voorafgaand aan elke nieuwe iteratie bepaald wat er opgepakt gaat worden. Dit is mogelijk omdat de business owner onderdeel is of continu betrokken is bij het DevOps team. Ook voldoen aan de behoefte van steeds snelle opleveringen lijkt binnen de DevOps benadering beter afgedekt te worden. Hiervoor zijn beheersmaatregelen vanuit verschillende gebieden te noemen. Binnen DevOps is er een cultuur van continu leren en experimenteren. Daarbij onderzoekt het team op vaste tijden hoe effectiever gewerkt kan worden en past vervolgens zijn gedrag daarop aan. Daarbij ligt de focus op klantwaarde en alleen die dingen doen die waarde hebben voor de klant. Belangrijk binnen de cultuur van DevOps is het Delen van kennis en ervaringen binnen en buiten teams wat snel leren mogelijk maakt. Als laatste is hier van het procesgebied nog het continu testen en verbeteren van deployment processen te noemen waarbij het helpt dat in elke iteratie de gehele SDLC cyclus wordt doorlopen. Als laatste komen er uit de analyse ook beheersmaatregelen die bijdragen aan het beheersen van onzekerheid. Van het relatiegebied is het agile principe te noemen dat aangeeft dat de meest efficiënte en effectieve manier om informatie te delen in en met een ontwikkelteam is door met elkaar te praten. De vaste multidisciplinaire teams waarin ook de business is vertegenwoordigd of continu betrokken is schept hier de juiste context voor. Daarnaast draagt de beheersmaatregel van het procesgebied hier ook aan bij. Binnen DevOps worden softwarecomponenten continu geïntegreerd en geautomatiseerd getest waardoor bekende en onbekende risico's onderkend worden.

Wat wordt niet of onvoldoende afgedekt door DevOps
Een aspect dat door de traditionele benadering wel afgedekt lijkt te worden maar minder door DevOps is de behoefte van de business aan kosten effectieve oplossingen. Binnen de traditionele benadering zijn hiervoor verschillende beheersmaatregelen te noemen van verschillende gebieden. Van het inhoudsgebied is de beheersmaatregel te noemen dat er een continue focus op de zakelijke rechtvaardiging (Business Case) van het project is en dat bij elke fase overgang opnieuw gekeken wordt naar de oorspronkelijke requirements. Bij devOps lijken de maatregelen zich meer te richten op de belangen van snelle en flexibele dienstverlening en het garanderen van een stabiele omgeving. Er lijkt in de beheersing minder aandacht te zijn voor de kosten effectiviteit.

5 Consequenties voor de beheersing binnen de IV-voortbrengingsketen

5.1 Consequenties voor de beheersing binnen de IV-voortbrengingsketen

In deze paragraaf wordt de derde deelvraag behandeld. Op basis van de analyse uit het vorige hoofdstuk is het de vraag wat deze verschillen in de wijze van beheersing betekenen voor de gevraagde snellere levering van flexibele, betrouwbare, veilige en kosten effectieve IT-diensten.

Zoals in hoofdstuk 1 beschreven bevinden organisaties zich op dit moment in een zeer turbulente omgeving. Organisaties zijn gedwongen om mee te veranderen en tijdig in te spelen op de veranderende klantbehoeftes. Dit stelt hoge eisen aan de snelheid waarmee organisaties hun ondersteunende It-diensten kunnen aanpassen waarbij er geen afbreuk gedaan mag worden aan de stabiliteit, betrouwbaarheid en veiligheid van de productie omgeving. Daarbij vraagt de business om kosten effectieve oplossingen om concurrerend te kunnen zijn.

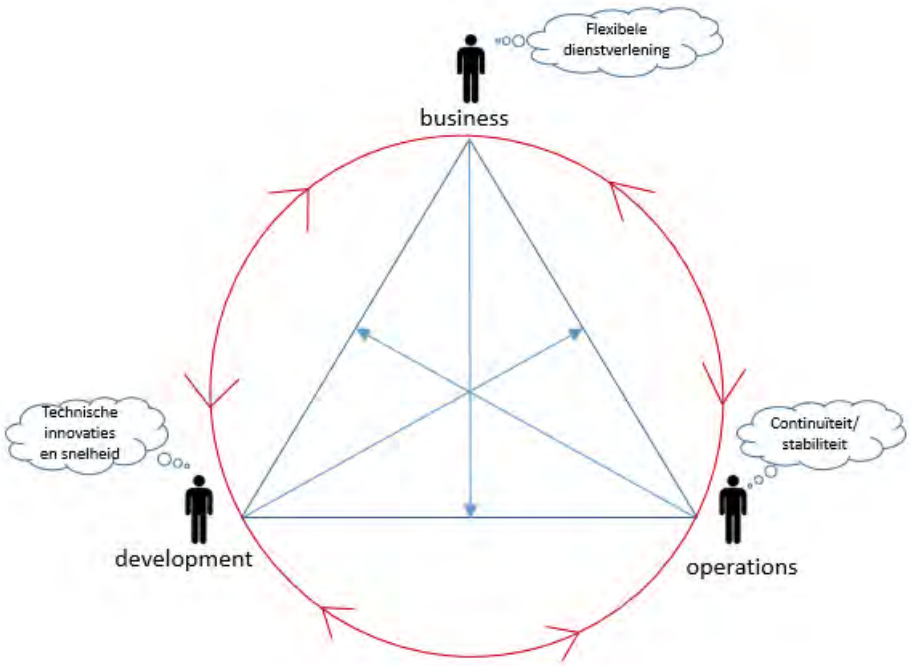
Uit de analyse in het vorige hoofdstuk kan de conclusie getrokken worden dat de beheersing van de traditionele benadering meer gericht is op garanderen van continuïteit van dienstverlening dan op het versnellen van levering of inspelen op verandering. Daarmee is deze benadering vooral effectief in een stabiele voorspelbare omgeving. Zoals Sharma en Coyne [14] aangeven past de beheersing binnen deze benadering meer bij de ontwikkeling en beheer van record systemen. Dit zijn systemen die een grote hoeveelheid data bevatten en transacties verwerken en ontworpen zijn voor een hoge mate van betrouwbaarheid en stabiliteit. Aangezien deze systemen niet veel wijzigen, hoeft voor het voldoen aan de requirements van de business maar een paar keer per jaar een wijziging opgeleverd te worden.

De beheersing binnen de traditionele benadering is onvoldoende om te kunnen omgaan met verandering en onzekerheid omdat uitgegaan wordt van een stabiele, voorspelbare en maakbare omgeving. Alles is van tevoren bekend op basis van volledige informatie en daardoor is een planning voor het hele traject te maken. Als echter gekeken wordt naar het kwadrant met de vier beheersingsstrategieën dan wordt het onzekerheidsmanagement in de beheersing niet meegenomen.
Frijns [6] concludeert dat er twee complementaire beheersingsstrategieën zijn die nodig zijn voor het kunnen managen en beheersen van dynamiek en onzekerheid. De essentie van de eerste strategie is het kunnen omgaan met de bekende risico's. Als ze zich voordoen worden ze in de risk log vastgelegd met als doel ze te kunnen beheren en regelmatig te reviewen om vast te kunnen stellen wat het effect is geweest van de getroffen maatregelen. De nadruk binnen de traditionele ingerichte voortbrengingsketen ligt op deze strategie.
De tweede strategie die Frijns beschrijft is gericht op de beheersing van onzekerheid. Deze strategie is erop gericht om een open dialoog en uitwisseling van informatie en waarnemingen te bevorderen. Er moet zo veel mogelijk en in een zo vroeg mogelijk stadium signalen worden opgepikt die een bedreiging kunnen vormen voor het behalen van de doelen, zodat tijdig aanpassingen doorgevoerd kunnen worden. Hij noemt dit de strategie dialoog.

In onderstaande figuur zijn deze strategieën toegevoegd aan de beheersingsstrategieën die in Hoofdstuk 2 gepresenteerd zijn.

Figuur 5: Strategieën voor de beheersing van dynamiek en onzekerheid

Binnen DevOps wordt de dialoog strategie ingevuld door het werken in vaste multidisciplinaire teams waardoor er tussen de stakeholders een continue communicatie en uitwisseling van informatie kan plaatsvinden. De cirkel in onderstaande figuur laat het team zien waarbinnen de stakeholders samenwerken. Iedere stakeholder doet dit vanuit het perspectief waarmee hij bij de verandering betrokken is. De verschillende betrokken rollen zijn complementair aan elkaar en er is een open communicatie op basis van gelijkwaardigheid. Hiërarchische lijnen spelen hier geen rol. Door de continue samenwerking en communicatie wordt omgegaan met onzekerheden zowel vanuit de omgeving als vanuit de techniek. Daarbij moeten de stakeholders steeds in hun afwegingen rekening houden met de verschillende belangen en daar een balans tussen zoeken. De pijlen op de cirkel in onderstaande figuur geven deze continue, open en gelijkwaardige communicatie aan. De pijlen wijze daarom twee kanten op. De loodlijnen binnen de driehoek laten de balans tussen de verschillende belangen zien waar de stakeholders mee te maken hebben.



Figuur 6: Communicatie binnen DevOps-teams

Niet alleen heeft de dynamische omgeving en kunnen omgaan met onzekerheid gevolgen voor de gebruikte beheersingsstrategieën en in te vullen randvoorwaarden om de samenwerking en continue communicatie tussen stakeholders te garanderen maar ook voor de gebruikte beheersmaatregelen die bij deze beheersing passen. In de beheersing zullen naast beheersmaatregelen binnen de gebieden inhoud en proces ook beheersmaatregelen meegenomen moet worden van de gebieden cultuur en relatie om met verandering en onzekerheid om te kunnen gaan. Zoals in hoofdstuk 4 is aangetoond worden er binnen de DevOps benadering meer beheersmaatregelen binnen het relatie- en cultuurgebied gebruikt dan in de traditionele benadering. Binnen DevOps wordt continu samengewerkt binnen multidisciplinaire teams die gezamenlijk eindverantwoordelijk zijn voor het behalen van de doelen. De benodigde cultuur verandering wordt bereikt door het bevorderen van leren en experimenteren waardoor continu verbeterd kan worden en innovaties tot stand kunnen komen. Hiermee wordt de randvoorwaarde ingevuld om snel te kunnen reageren op veranderingen binnen een dynamische omgeving met veel onzekerheid met tegelijkertijd de behoefte aan een hoge kwaliteit van geleverde IT/diensten.

5.2 Vervolgonderzoek

In dit onderzoek zijn de uitgangspunten en randvoorwaarden die ten grondslag liggen aan de beheersing binnen een DevOps ingerichte IV-voortbrengingsketen vanuit de theorie bestudeerd.
Daarnaast is vanuit de theorie bestudeerd hoe de randvoorwaarden en beheersmaatregelen zijn ingevuld.
DevOps is een concept en geen uitgewerkte methode. Daardoor kan de implementatie bij organisaties geheel anders zijn met een andere wijze van invulling van de wijze van beheersing.
Dit onderzoek is uitgevoerd op basis van een literatuurstudie waarbij vooral gekeken is naar de theorie. In vervolgonderzoek moeten de uitkomsten getoetst worden aan de praktijk om een beter beeld te krijgen van de consequenties voor de beheersing als DevOps wordt gebruikt binnen de IV voortbrengingsketen.

In het vervolgonderzoek zal onderzocht worden welke uitgangspunten in de praktijk ten grondslag liggen aan de inrichting van de beheersing binnen DevOps. Komen deze overeen met de uitgangspunten die in de theorie gevonden zijn, zijn ze een verdieping hierop of zijn er nog andere uitgangspunten te vinden die niet in de gevonden literatuur genoemd worden. Dit geeft een completer beeld van de uitgangspunten.
Dit zelfde kan gedaan worden voor de in te vullen randvoorwaarden. Zijn deze hetzelfde als die gevonden zijn in de theorie of zijn ze een verdere verdieping hierop of zijn er randvoorwaarden die in de theorie niet gevonden zijn. Ook dit kan een completer beeld opleveren als aanvulling op de huidige theorie.

6 Literatuurlijst

[1] S. Duivestein, J. Bloem, M. van Doorn, Thomas van Manen, DESIGN TO DISRUPT, Een executive introductie, 2015.

[2] H. Heinen, Schrik niet: Je bent een IT-bedrijf! Blog van 6 september 2016 op de website van Enrise https://enrise.com/2016/09/je-bent-een-it-bedrijf/

[3] E.H.J. Vaassen en R.H.G. Meuwissen, Hoofdlijnen bestuurlijke informatieverzorging, 2016.

[4] A.J.G Driessen en A. Molenkamp, Internal auditing, 2012.

[5] P. Frijns, F. van Leeuwen, R Bierwolf, publ Project management: A more balanced approach, 2016.

[6] P. Frijns en F. van Leeuwen, publ MSc Risk Log to Risk Dialogue, 2016.

[7] B. Stofberg, Iedereen kan innoveren Uitgeverij Haystack, 2016.

[8] Accenture Technology vision, 2016

[9] DevOps Overview - An ISACA DevOps Series White Paper, 2015.

[10] PwC audit Guide, 2016.

[11] State of DevOps Report presented by Puppet + DORA, 2016.

[12] M. Henry, Organisatiestructuren, 2013.

[13] K. A. Merchant, W. van der Stede, 1e druk Management control systems, 2007

[14] S. Sharma en B. Coyne, DevOps For Dummies, 2015.

[15] N. N. Taleb, Antifragile : things that gain from disorder, 2012.

[16] R. van der Pols, R. Donatz, F. van Outvorst, BiSL een Framework voor Functioneel Beheer en Informatiemanagement, 2005.

[17] Cutter IT Journal: The Journal of Information Technology Management, Vol. 24, No. 8 August 2011.

[18] J. Schuyl, A. Nuijten, Complexiteit en de inrichting van de ICT-beheerorganisatie 6de EDP-Auditor nummer 1, 2005.

[19] Manifest voor Agile Software Ontwikkeling, 2001.

[20] M. van Zomeren, PWC Spotlight, Interne beheersing en IT, 2015-2.

[21] P. Broshuis, PWC spotlight 2009-2 Optimale IT-inrichting: het IT Governance Raamwerk, 2009.

[22] COSO/ERM Nederlandse management samenvatting, 2004.

[23] S. S. Unnati, An excursion to software development life cycle models- an old to ever-growing models. Software Engineering Notes, 41, pp. 1-6., 2016.

[24] A.G. van den Akker Prince2 compact: methode voor projectmanagement derde druk LAGANT Management Consultants BV, 2006.

[25] C. Wright, Agile governance and audit IT governance publishing, 2014.

[26] B Hartholt, W. Luitjes Auditing DevOps in a financial statement audit

[27] L.E. Lwakatare, P. Kuvaja, M. Oivo, An Exploratory Study of DevOps: Extending the Dimensions of DevOps with Practices, 2016.

[28] G. Kim, top 11 things you need to know about DevOps

[29] ISACA whitepaper DevOps practitioner considerations, 2015.

[30] Wikipedia 02-06-2017 https://en.wikipedia.org/wiki/Software_development

Security Operations Center (SOC)

Modelleren en meten van effectiviteit

Stef Schinagl en Keith Schoon

Wij hebben 5 jaar gewerkt als IT-auditor bij Noordbeek. Omdat organisaties echt een behoefte hadden aan de meer theoretische invulling van een SOC, hebben wij de scriptie met plezier en overtuiging geschreven. In samenwerking met Ronald Paans heeft de scriptie geleidt tot een internationaal peer-reviewed paper: “A Framework for Designing a Security Operations Centre (SOC)” en is gepresenteerd op “ the Hawaii International Conference on System Sciences (HICSS)”. Keith vervolgt nu zijn IT-Audit carrière bij Zorg en Zekerheid. Stef is als Adviseur Informatiebeveiliging en Privacy werkzaam bij UWV. Hij combineert dit met een parttime aanstelling als docent bij de IT-audit opleiding aan de VU en een promotieonderzoek in de richting van Information Security Governance.

1 Introductie

Cyberaanvallen vormen een steeds ernstigere bedreiging voor de Nederlandse economie en de nationale veiligheid. De Algemene Inlichtingen en Veiligheid Dienst signaleert dat digitale aanvallen toenemen in aantal, complexiteit en impact [AIVD2012]. In een brief aan de Tweede Kamer op 5 april 2013 spreekt de Minister van Binnenlandse Zaken en Koninkrijksrelaties, R.H.A. Plasterk, zijn zorgen uit over de steeds grotere bedreiging van de nationale veiligheid, die is ontstaan door een toenemende mate van internationalisering en technologisering [BZK2013]. Daarin stelt de Minister dat bedrijven, overheden en burgers kwetsbaarder worden door een aantal trends en ontwikkelingen. Steeds meer informatie wordt namelijk door bedrijven, overheden en burgers digitaal opgeslagen, gekoppeld en via internetverbindingen en cloud computing (inter)nationaal gedeeld. De ICT-infrastructuur, maar ook de economie en de samenleving, wordt hierdoor kwetsbaarder voor aantastingen door zowel staten als criminele en extremistische groepen. De dreiging van Cyber-inbreuken op de nationale veiligheid manifesteert zich steeds nadrukkelijker.
De 'klassieke informatiebeveiliger' blijkt moeite te hebben het hoofd te bieden tegen de hedendaagse intensieve en geavanceerde cyberaanvallen. Generaal Dick Berlijn, Oud Commandant der Strijdkrachten, sprak op 30 oktober 2013 tijdens het seminar 'Fighting cybercrime' van de Vrije Universiteit Amsterdam, over oorlogsvoering binnen de cyberwereld. Menige Nederlander herinnert zich de cyberaanvallen waar onder meer de ING, Rabobank, ABN AMRO, KLM, DigID en Diginotar de afgelopen jaren mee hadden te kampen, welke resulteerden in een abrupte verstoring van hun bedrijfsvoering. Voor de gebruiker veroorzaakte dit een gevoel van onbehagen, mede door de onduidelijkheid over wanneer de dienstverlening zou worden hervat. Dit is ongewenst voor het bedrijfsleven, de overheid en alle betrokkenen. Voor de organisaties in kwestie resulteert dit onder andere in reputatieschade en financiële schade. Dit betekent dat deze organisaties meer geavanceerde middelen moeten ontwikkelen om zich te beschermen tegen cyberaanvallen en de weerbaarheid te verhogen.

1.1 Achtergrond

In het verleden werd het hacken van computers en computernetwerken veelal uitgevoerd door onschuldige hobbyisten. Deze wilden soms laten zien dat zij slimmer waren dan de technici die computers en netwerken moesten beveiligen. Opschepperij, aanzien en verveling waren de grootste drijfveren voor de hackers. Financieel gewin was tot dan toe nauwelijks het motief. Zo ontdekten hackers in de jaren 70 dat het Amerikaans telefoonsysteem werkte met bepaalde tonen. Het bleek mogelijk om
gratis te kunnen bellen door deze tonen met een fluit te imiteren. Om dit lek te demonstreren gingen zij gratis vanuit Amerika naar het Vaticaan bellen. Deze zogeheten 'prank calls' waren veelal onschuldig.
In de loop der tijd is het gebied van hacken verlegd van een onschuldige bezigheid naar een serieuze bedreiging die organisaties miljoenen kunnen kosten en zelfs de Nationale veiligheid in gevaar kunnen brengen. Vandaag de dag zijn inlichtingen- en veiligheidsdiensten bezig met de ontwikkeling van cyberwapens. Internationale criminele organisaties richten zich steeds meer op frauderen via het internet voor financieel gewin. Het NCSC stelt vast dat er gesproken kan worden van cybercrime-as-a-service [NCSC 2013]. Dit wordt gezien als een cyberdienstensector waarin hulpmiddelen commercieel beschikbaar worden gesteld. Cyberaanvallen worden enerzijds steeds professioneler en meer centraal georganiseerd, maar ook worden de middelen steeds laagdrempeliger beschikbaar gesteld aan de verschillende actoren.
Dick Berlijn vergelijkt het huidige internet met een oorlogsgebied. Hij neemt de cyberaanvallen heel serieus en stelt dat via cyberwapens een vitaal deel van de samenleving kan worden platgelegd. Stel dat de SCADA computers van de waterkeringen worden beïnvloed door hackers, criminelen of vijandige partijen, dan kan in theorie een deel van Nederland met natte voeten komen te staan. Hetzelfde geldt voor de SCADA computers binnen de energievoorziening. Zonder elektriciteit en benzine stagneert onze moderne maatschappij.

1.2 Probleemstelling

De overheid maakt zich zorgen omtrent het toenemend aantal beveiligingsaanvallen op de netwerken en websites van de overheid, de cyberdreigingen voor de vitale infrastructuur en het misbruik van financiële, privacygevoelige en vertrouwelijk gegevens. Dit heeft geleid tot de oprichting van het Nationale cyber Security Centrum (NCSC), de uitrol van de 'Baseline Informatiebeveiliging Rijksdienst' (BIR) en het inrichten van diverse samenwerkingsverbanden, zoals via het Centrum voor Informatiebeveiliging en Privacy (CIP).

De Rijksoverheid is gezien haar unieke taken een interessant aanvalsobject voor hackers, criminelen of vijandige partijen. Dit komt niet alleen door de vertrouwelijkheid van de informatie, tot en met Staatsgeheim Zeer Geheim, maar ook door de verwerking van enorme financiële geldstromen. De geldstroom door de Rijksoverheid is jaarlijks meer dan 250 miljard euro. Dit is een bedrag van € 250.000.000.000,-, uitgeschreven met het juiste aantal nullen voor de komma. Iedere crimineel droomt van het afromen van deze geldstroom, al is het maar met één procent. Daarnaast heeft het Rijk een reputatie hoog te houden wat het voor de actoren interessant maakt om hier schade aan toe te brengen.

Regelmatig vinden incidenten plaats, die door de media worden uitvergroot. Zo noopte een lek in programmeeromgeving Ruby on Rails overheidsorganisatie Logius ertoe om DigiD offline te halen [CW2013]. In 2011 is het systeem, waarmee SSL-certificaten voor overheidsdiensten als DigiD en de belastingdienst worden gemaakt, gekraakt [TW2011]. In 2012 besmette het Dorifel virus computers van tientallen gemeenten waardoor office-bestanden niet meer leesbaar waren [BB2012]. Dit soort incidenten prikkelt de politiek, die daarna druk uitoefent op senior management binnen de overheidsorganisaties. Veel bestuurders zijn hiermee overvallen, en missen persoonlijk de kennis en kunde om de juiste maatregelen te kunnen overzien. Hierdoor begint men vaak aan grote projecten om van alles te beveiligingen, zonder een helder doel voor ogen te hebben, en laat men zich overspoelen met toevallig aangeboden tooling. Het begrip cyberaanvallen blijft generiek en vaag, en het wordt niet concreet waartegen de organisaties zich moeten beschermen. Dit leidt tot inefficiënte investeringen.

In reactie op de toegenomen dreiging schieten Security Operations Center (SOC's) als paddenstoelen uit de grond. De realiteit leert ons echter dat er hiervoor weinig echt effectieve best practices zijn, zoals blijkt uit:

- European Network and Information Security Agency [ENISA2006] adviseert een team van specialisten met aanvullende competenties, maar wordt op dit punt niet concreet;
- Een Expert Groep van het PvIB concludeert dat er geen eenduidige inrichting mogelijk is voor een SOC. Er wordt gesteld dat de doelstelling en taken per organisatie te ver uiteenlopen om handvatten te kunnen geven aan de inrichtingen van een SOC [PvIB2011];
- Het CIP heeft een periodiek informatiebeveiligingoverleg (PIO) ingeregeld waarbij het inrichten en in stand houden van SOC's centraal staat. Hierbij is een bijeenkomst georganiseerd op 10 december 2013 waarna verschillende lessons learned naar voren zijn gekomen. Zo lijkt het inrichten van het SOC een lastige opgave door de complexiteit van een IT-omgeving.

De term SOC is binnen de overheid inmiddels een modewoord geworden. Allerlei organisaties die zich bedreigd voelen door cyberaanvallen en IT-misbruik denken dat het inrichten van een SOC de ultieme oplossing is. Zij zien het SOC dan als 'Haarlemmerolie'. Het ontbreekt echter vaak aan consistentie bij de inrichting van de SOC's, waarbij de optredende pluriformiteit geen garantie levert voor hun effectiviteit.

1.3 Beperking van de literatuur

De literatuur biedt geen eenduidig model voor een SOC. De beschrijvingen van de taken, verantwoordelijkheden en bevoegdheden van SOC's lopen in de literatuur sterk uiteen [PvIB2012]. Hierbij ontbreekt het aan een wetenschappelijke basis en consistentie. White papers van toonaangevende leveranciers gaan elk uit van hun eigen bedrijfsspecifieke inrichting, waarbij eenieder redeneert vanuit een eigen belang [HP2011] [IBM2013] [RSA2013] [McaFee2012]. Doordat er geen synergie bestaat voor de invulling

van een SOC, ontstaan op gefragmenteerde en bijna willekeurige wijze security taken die mogelijk wel of niet binnen een SOC kunnen worden ondergebracht. Er is sprake van een diffuus beeld van de term SOC. Derhalve zijn de auteurs van deze scriptie van mening dat er in de literatuur geen eenduidig model of voorbeeld voor de inrichting van een SOC voor komt. Deze absentie veroorzaakt verwarring. Deze verwarring belemmert de kennisuitwisseling en ontwikkeling van SOC's. Daarnaast bemoeilijkt dit ook de effectieve inrichting hiervan, terwijl het aantal organisaties die hier dringende behoefte aan heeft, gestaag blijft groeien.

2 Missie, doelstelling en scope van een SOC

Wij zijn naar een hoger abstractieniveau teruggegaan. Het doel hiervan is om te kijken waar het SOC mogelijk een rol kan spelen binnen de organisatie. Vanuit deze integrale aanpak komen wij uiteindelijk tot een definitie en missie van het SOC.

2.1 De taken van Informatiebeveiliging

Zoals John Hermans en Gerben Schreurs beschrijven in het artikel `Vijf denkfouten over cybersecurity [KPMG2012], is 100 % bescherming tegen cyberaanvallen en IT misbruik een illusie. Indien dit wordt onderkend kan vanuit een risicobenadering de juiste preventieve, detectieve en correctieve maatregelen worden opgesteld. Een denkfout welke hierbij wordt gemaakt is de oplossing te zoeken in de techniek. Hoewel de techniek essentieel is voor adequate beveiliging dient eerst een goed beleid, organisatie en procedures te worden ingericht. Techniek is pas de laatste stap. Hiervoor volgt de kenmerkende uitspraak: 'A Fool with Tool is still a Fool'. De mens is en blijft verantwoordelijk voor vele incidenten en zonder de juiste competenties blijft deze uitspraak gelden.
Cyberdreigingen zijn niet altijd zo geavanceerd als door de bestuurders wordt gedacht. Er wordt soms ten onrechte paniek gezaaid door de media. Er wordt gedacht dat de hackers extreem intelligente middelen hebben om hun aanvallen uit te voeren. Als dit het geval is, waarom doen organisaties dan nog moeite om ons te beschermen tegen deze aanvallen? De beste vraag die bestuurders zich hierbij moeten afvragen is, wat maakt ons nou zo interessant om aan te vallen oftewel wat zijn de waarden van de organisatie en op welke systemen hebben deze betrekking?
Cybersecurity is van iedereen binnen een organisatie. Er wordt in hetzelfde artikel gesteld dat cybersecurity vaak wordt belegd bij een groep experts maar dat de uitdaging juist ligt bij het integreren in de gehele organisatie.
Zoals wordt gesteld in de visie van KPMG zal effectieve informatiebeveiliging invloed moeten hebben op een samenhangend stelsel van preventieve, detectieve, correctieve en repressieve maatregelen. Het SOC kan een rol spelen binnen deze aandachtsgebieden. Het SOC is daarbij onderdeel van de totale informatiebeveiliging van de organisatie.
Er zijn drie hoofdtaken te onderscheiden bij de uitvoering van het bovengenoemde stelsel van maatregelen, namelijk sturing binnen het voortbrengingsproces, bewaking binnen de operationele omgeving en het ingrijpen in de bedrijfsprocessen.

Preventieve en detectieve maatregelen

Men moet zorgen dat zowel de voordeur als de achterdeur goed op slot zitten. Indien dit niet het geval is ontstaat het 'dweilen met de kraan open' effect. Hiertoe wordt getracht het voortbrengingsproces veilig te maken door het in voeren van Security by Design, namelijk Secure Service Development (SSD). SSD omvat onder andere betrokkenheid van consultants en architecten bij de BIA, de risicoanalyses, de Privacy Impact Analyses (PIA's), het bijhouden van de architectuur voor informatiebeveiliging en de Attack Patterns, het participeren bij het vaststellen van specifieke beveiligingseisen, het toezien op code reviews, pentesten en scans etc.

Het onderwerp Security by Design is verder uitgewerkt in het boek 'Grip op secure software development (SSD)' van het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) [CIP2014].
Binnen de infrastructuur voert men ook pentesten uit, naast observeren, continuous monitoring en scans. Daarnaast worden technische hulpmiddelen geïnstalleerd, zoals endpoint protection, IDS/IPS, firewalls, DMZ, PKI, certificaten en cryptografie. De doelstelling is de gegevens via een veilige applicatie te verwerken binnen een veilige infrastructuur en die veiligheid actief te bewaken. Het bewaken van de operationele omgeving van de IT is onderdeel van het SOC. Hiertoe beschikt het SOC over analisten, hulpmiddelen voor het observeren en analyseren, en kan pentesters inzetten. De primaire taak is de dreigingen tijdig te identificeren en daarop gepaste actie te ondernemen.

Correctieve en repressieve maatregelen
Bij een inbreuk op de informatiebeveiliging zijn niet alleen technische herstelmaatregelen nodig van beheerders, maar moet soms ook worden ingegrepen bij de gebruikers, zowel intern als extern. Hierbij kan worden gedacht aan integriteitskwesties zoals bekijken van ongewenst beeldmateriaal of aan identiteitsfraude bij de belastingdienst. Om deze reden ligt er een relatie tussen informatiebeveiliging binnen de eigen organisatie en beveiligingsfunctionarissen op de werkvloer, een Bureau Integriteit en Veiligheid, Beveiligingsambtenaren en functionarissen van het Openbaar Ministerie of Openbare Orde en Veiligheid, veiligheidsdiensten etc. Deze functionarissen hebben de taak elders in te grijpen en schade te beperken of te herstellen.

2.2 Definitie SOC
Conform de visie van KPMG stellen wij hiertoe dat het SOC integraal deel uit maakt van informatiebeveiliging. Hierbij hanteren wij de volgende definitie:

> *Een SOC is een groep competente medewerkers welke vanuit een integraal stelsel van maatregelen, gewenste bescherming biedt tegen cyberdreigingen en IT-misbruik.*

Hiertoe biedt het SOC diensten, informatie, advies en ondersteuning aan de gebruikersorganisaties en beheerorganisaties. Hierbij voeren zij een drietal hoofdtaken uit: sturing binnen het voortbrengingsproces, bewaking binnen de operationele omgeving en het ingrijpen in de bedrijfsprocessen.

3 De Meetmethode

De expertbrief van het PvIB over SOC's [PvIB2012] stelt dat taken van het SOC sterk uiteen kunnen lopen. In deze expertbrief wordt geen eenduidig takenpakket gedefinieerd. Iedere medeauteur aan dit stuk geeft een eigen definitie van taken, die naar zijn of haar mening de potentie hebben binnen het SOC te vallen. Daarbij ontstaan op gefragmenteerde wijze security taken, die mogelijk, al dan niet virtueel, binnen een SOC kunnen worden ondergebracht.
KPMG volgt een andere aanpak, namelijk een integrale benadering van informatiebeveiliging waar het SOC een logisch onderdeel van uitmaakt [KPMG 2012], [CBP 2013]. KPMG gaat uit van een samenhangend stelsel van preventieve, detectieve, correctieve en repressieve maatregelen. Deze kunnen bij diverse organisatieonderdelen worden belegd, maar moeten wel een samenhangende structuur blijven behouden.
Uit ons literatuuronderzoek blijkt dat er geen eenduidig beeld bestaat van een SOC. Iedere auteur beschrijft een eigen variant, soms vanuit een integraal perspectief, of soms als een geïsoleerde entiteit. Ook de taakverdeling varieert heel sterk.

> *In het kader van deze scriptie hebben wij de integrale benadering gevolgd, namelijk door het gehele stelsel als uitgangspunt te nemen. Hiervan is een deelverzameling van het stelsel relevant voor het SOC, waarbij een deel van die deelbenadering door het SOC zelf wordt uitgevoerd en de rest van deze deelverzameling kan worden gezien als randvoorwaardelijk en faciliterend. De grens tussen deze twee delen kan variëren.*

De naar onze mening relevante groepen van maatregelen die zijn gerelateerd aan een SOC hebben wij verdeeld over vier domeinen, die voor onze modelvorming van belang zijn. Dit zijn:

- Secure Service Development: De maatregelen die nodig zijn om een veilige (web)applicatie te verkrijgen;
- Continuous Monitoring: De maatregelen die nodig zijn om aanvallen vroegtijdig te ontdekken en snel actie te kunnen nemen;
- Schadebeperking: De maatregelen die nodig zijn om een aanval te stoppen en de schade zoveel mogelijk te beperken;
- Kennisdeling: De maatregelen die nodig zijn om alle betrokkenen te laten samenwerken.

Deze relevante groepen maatregelen hebben wij als assen afgebeeld in een spider diagram. Iedere as moet zijn ingevuld door de organisatie, anders kan een SOC niet effectief opereren. Een ketting is zo sterk als zijn zwakste schakel. Dit houdt niet in dat iedere as binnen het SOC valt. Maar de as moet wel ergens binnen de organisatie zijn belegd, anders vallen er gaten in de verdedigingslinie. De voor het model van belang zijnde assen zijn zichtbaar in figuur 1:

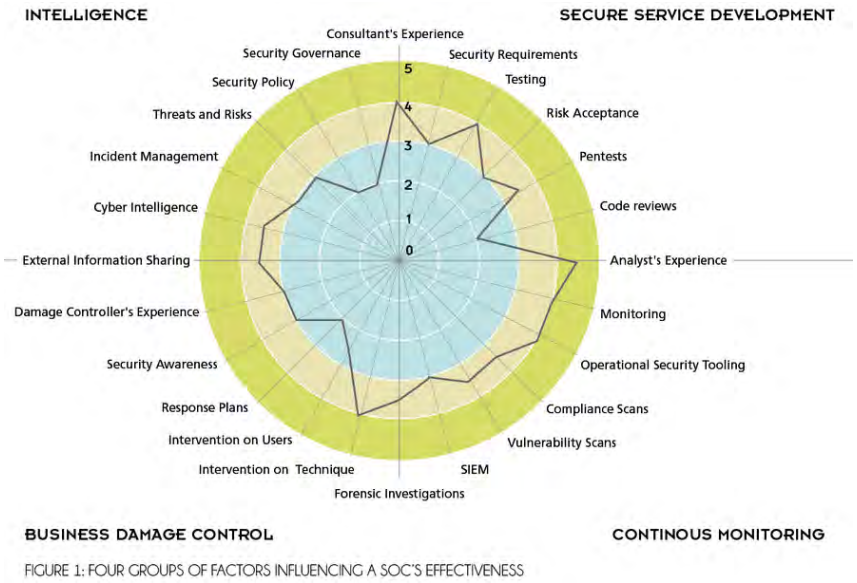


FIGURE 1: FOUR GROUPS OF FACTORS INFLUENCING A SOC'S EFFECTIVENESS

Iedere as representeert een groep van maatregelen en geeft hun volwassenheidsniveau aan. Hierbij is de waarde:

- Niveau 5: Gewenste situatie. Hier moet men niet de ideale situatie onder verstaan, maar het ambitieniveau van senior management gebaseerd op hun afweging van het accepteren van risico's versus de kosten van mitigerende maatregelen;
- Niveau 4: Voldoende;
- Niveau 3: Suboptimaal. Het functioneert wel, maar niet met de gewenste effectiviteit;
- Niveau 2: Zorgelijk;
- Niveau 1: Hoog risico of niet aanwezig.

3.1 Bij het veldonderzoek onderkende verschijningsvormen van SOC's

SOC's zijn vrijwel altijd gepositioneerd binnen een technische IT-afdeling van een organisatie. Gezien de sterk technisch gerichte werkzaamheden is dit een voor de hand liggende positionering. Zoals beschreven

in het voorgaande hoofdstuk, is het van belang dat een SOC invloed kan uitoefenen op het gehele stelsel van preventieve, detectieve, correctieve en repressieve maatregelen gerelateerd aan het werkgebied van het SOC.
Tijdens het veldonderzoek zijn er grofweg vier verschijningsvormen van SOC's naar voren gekomen. Individule resultaten worden in dit artikel niet openbaar gemaakt. Figuur 1 is een voorbeeld:

Integraal SOC:
Een 'integraal SOC' is een kenniscentrum, bestaande uit een aantal competente en gedreven medewerkers, die zich met zowel het voortbrengingsproces als met beheer, infrastructuur en schadebeperking bezighoudt. Dit type SOC is geplaatst binnen de IT-organisatie en voelt zich integraal verantwoordelijk voor veel zaken die betrekking hebben op informatiebeveiliging;

Technisch gericht SOC:
Vaak zijn SOC's dichtbij of binnen het beheergedeelte van de IT-organisatie gepositioneerd en hebben daarbij voornamelijk interactie met de functionele en technische beheerders. Dit type SOC heet in onze indeling een 'technisch gericht SOC'. Zij worden niet betrokken bij het voortbrengingsproces en hebben een beperkte, veelal ad hoc relatie met de schadebeperkers die actief zijn in de business;

Intelligence SOC:
Er zijn SOC's die het analysewerk en de pentesten in eigen beheer uitvoeren en de monitoring (deels) uitbesteden aan een andere interne afdeling of een marktpartij. Zo een 'Intelligence SOC' komt bijvoorbeeld voor in situaties waarbij de infrastructuur, servers, besturingssystemen en middleware zijn uitbesteed. Hierbij is het de bedoeling van de opdrachtgever dat de leverancier de monitoring, filtering en selectie verzorgt en samen met de opdrachtgever de serieuze alerts en events meer diepgaand analyseert.

In de lijn geïntegreerde SOC-functie:
Soms is er wel deels SOC-functionaliteit, maar is deze niet benoemd als een entiteit. Dan wordt security niet dedicated belegd, maar is er bijvoorbeeld voor gekozen om security taken binnen de bestaande lijn te beleggen. Er zijn geen aparte security functies. Het uitgangspunt is dat alle medewerkers bewust bezig zijn met security. Er zijn wel specialisten bijvoorbeeld op het gebied van netwerken welke een sterkte security achtergrond hebben, maar zij voeren hun taken uit vanuit een netwerkbeheerders functie. De tooling zorgt op de achtergrond voor signalen welke in de lijn van incidenten wordt afgehandeld.

3.2 Analyse verschijningsvormen

De meetmethode bevindt zich nog in een experimenteel stadium. Wij hebben deze methode ontwikkeld, gebruikt tijdens de interviews om een beeld te krijgen van de sterke en zwakke punten van ieder verschijningsvorm van een SOC, en de assen iteratief verbeterd op basis van voortschrijdend inzicht.
De indeling van de assen in vier kwadranten blijkt nuttig te zijn om snel een visueel beeld te krijgen over de verschijningsvorm van het SOC en hun focus.
Bij de metingen in de praktijk herkenden wij snel de verschijningsvormen van de bezochte SOC's, met elk specifieke sterke en zwakke punten binnen een kwadrant. Echter is de waarde van de assen binnen deze verschijningsvormen fluctuerend. De fluctuaties geven aan dat er andere bepalende factoren zijn binnen een SOC, die de volledigheid van het takenpakket sterk beïnvloeden.
Dit leidde tot nader onderzoek, namelijk het uitvoeren van een decompositie van de elementaire basisfuncties binnen een SOC. Dit zijn in feite de bouwblokken waaruit het SOC is opgebouwd. In het volgende hoofdstuk gaan wij in op deze analyse.

4 De typologie van een SOC: de elementaire basisfuncties

Dit hoofdstuk beschrijft het model voor een SOC, bestaande uit vijf elementaire basisfuncties. Deze decompositie is van belang om mogelijk samenwerkingsverbanden per basisfunctie uit te kunnen werken.
Een SOC functioneert alleen binnen een bepaalde context. De vereiste bovenliggende structuur is op de onderstaande figuur weergegeven als 'Governance & Control', met de CISO, IB-beleid etc., en Security by Design.

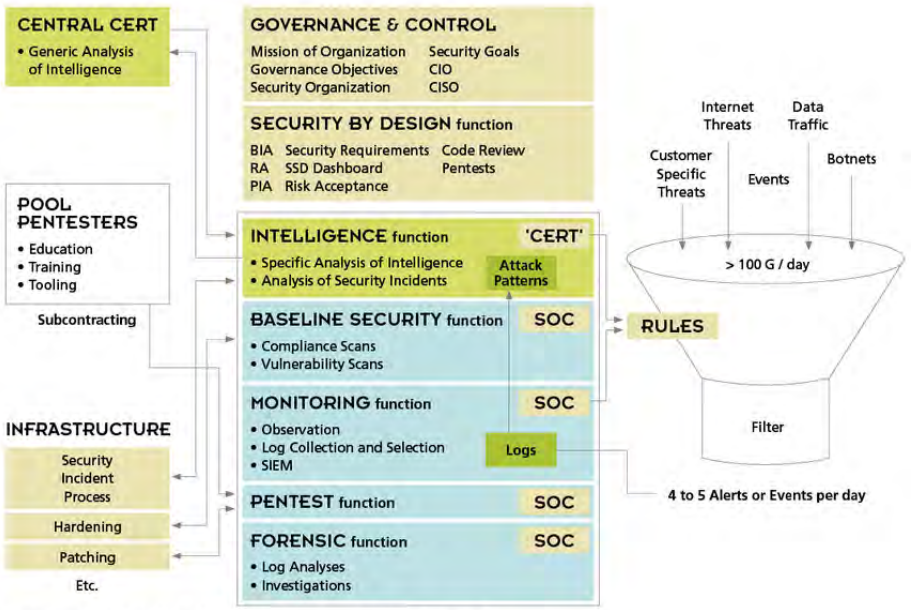


FIGURE 2: FRAMEWORK FOR DESIGNING AND IMPLEMENTING A SOC

De vijf basisfuncties van het SOC zijn hieronder uitgewerkt.

4.1 Intelligence-functie

Een SOC heeft een kern van ervaren analisten nodig, die zich richten op de specifieke dreigingen en beveiligingsincidenten die relevant zijn voor de gebruikersorganisatie. Zij analyseren en geven richtlijnen aan de andere functies binnen het SOC, aan de beheerders, aan de schadebeperkers binnen de gebruikersorganisaties en aan degenen die werkzaam zijn binnen het voortbrengingsproces. Tevens bepalen deze analisten hoe de rules van de SIEM moeten worden ingesteld, welke scans moeten worden gedraaid, welke pentesten moeten worden uitgevoerd etc. [SIEM2012]
De Intelligence-functie is de kern van het SOC. De opzet van deze functie vertoont overeenkomsten met een Computer Emergency Response Team (CERT), dat zich ook bezighoudt met dreigingen en het analyseren van incidenten. De naam CERT kan echter niet formeel worden gehanteerd, omdat dit een gedeponeerd handelsmerk is van het CERT/CC van de Carnegie Mellon University.

4.2 Baseline Security-functie

Een SOC ziet toe op de technische aspecten van de uitrol policy zoals de BIR, het proces van hardening van de technische componenten, het proces voor het aanbrengen van patches en de onderhoudsniveaus. Hiertoe worden naast preventieve instructies aan beheerders scans uitgevoerd om de compliance en kwetsbaarheden vast te stellen.

Het SOC draagt bij aan het opstellen van de Baseline Security, namelijk het stelsel van maatregelen voor informatiebeveiliging en privacybescherming. Deze Baseline Security is afgeleid van de security architectuur van de organisatie en de classificatie voor BIV voor de systemen en gegevens, die volgt uit de BIA. Via risicoanalyses en PIA's wordt bepaald welke maatregelen absoluut van belang zijn. Nadat die maatregelen door de beheerders zijn geïmplementeerd, worden deze met scans gecontroleerd. Afwijkingen worden gerapporteerd aan de beheerders en aan de Intelligence-functie. Deze ziet er op toe dat de afwijkingen worden opgelost.

4.3 Monitoring-functie

Een SOC bewaakt de verkeersstromen en probeert anomalieën te detecteren. Hierbij worden de grote volumes aan signalen verzameld en geanalyseerd via filtering en het leggen van correlaties, met het doel de werkelijk relevante signalen te kunnen herkennen.
Dagelijks genereren de netwerken en systemen grote volumes aan loggegevens, waarbij volumes van 100 tot 200 Gigabyte niet ongebruikelijk zijn. Het kernprobleem bij het gebruik van een SIEM is de rulesets zo in te regelen dat de werkelijk belangrijke alerts of events worden gefilterd uit deze omvangrijke stroom. Slechts enkele alerts of events per dag zijn kandidaat voor het initiëren van een verder onderzoek.
Op dit vlak hebben de onderzoekers in de private sector voorbeelden gezien waarbij SOC's meer grip hebben gekregen op het proces van selecteren en filteren. De effectiviteit van dit proces wordt grotendeels bepaald door de competenties en gedrevenheid van de betrokken analisten, oftewel dit is mensenwerk waarvoor (zeer) goede mensen nodig zijn. Die goede analisten zijn schaars.

4.4 Pentest-functie

Zowel in de productieomgeving als bij het voortbrengingsproces worden pentesten uitgevoerd, met name gericht op de door de Intelligence-functie aangegeven aandachtspunten. Het doel is robuustheid te creëren.
De pentesten in de productieomgeving zijn bedoeld als een noodzakelijk aanvulling op de Baseline Security en de scans. Via de scans worden maatregelen routinematig nagelopen en afwijkingen op de instellingen gesignaleerd, maar kan men geen sluipwegen ontdekken. Via de pentesten wordt gecontroleerd of er omwegen zijn naar belangrijke functionaliteit of gegevens, die door kwaadwillende kunnen worden misbruikt. Populair gesproken, via de scan wordt gekeken of de voordeur dicht is, bij de pentest wordt er flink aan gerammeld om te kijken of hij niet uit de schoot springt bij een flinke schop en of men niet via de regenpijp naar een open raam kan klimmen [PINE2013].
Pentesten hebben enige verwantschap met technische IT-audits, waarbij technisch geschoolde IT-auditors diep in de infrastructuur speuren naar technische zwakheden.

4.5 Forensische functie

Het SOC assisteert forensische onderzoekers bij het verzamelen en analyseren van bewijsmateriaal.
Veelal ligt de leiding van dit soort onderzoeken bij functionarissen die een formele opsporingsbevoegdheid hebben. De medewerkers van het SOC zijn uitvoerend op het technische vlak. Hieronder vallen bijvoorbeeld activiteiten zoals het veilig stellen van computers en storage, en het analyseren van harde schijven, log bestanden, mail etc., waarbij veel aandacht nodig is voor een zorgvuldige 'chain of custody' voor het bewijsmateriaal.
Bij de meeste SOC's is het forensische werk een parttime nevenfunctie, die wordt uitgevoerd door medewerkers die binnen de andere basisfuncties werkzaam zijn.

4.6 Andere varianten

Deze vijf basisfuncties vormen de typologie van het SOC. Voor iedere basisfunctie gelden specifieke randvoorwaarden, die invloed hebben op mogelijke of vereiste samenwerkingsverbanden met andere betrokken partijen.

Naast de bovenstaande basisfuncties wordt een SOC soms uitgebreid met andere taken zoals het:

- Bewaken van de beveiliging van SCADA computers en Industrial Controls Systems (ICS) voor procesautomatisering. Hierbij is ook een relatie met de vitale infrastructuur, zoals energievoorziening, bruggen sluizen etc. [TREN2013];
- Controleren op te 'hoge bevoegdheden';
- Adviseren over IB-vraagstukken;
- Beheren van het ontheffingsproces voor baselines;
- Beheren van endpoint protection, PKI, certificaten en cryptografie etc.;
- Beoordelen van wijzigingsverzoeken.

De diversiteit aan functies die binnen de verschillende SOC's worden opgenomen maakt een vergelijking van de bestaande SOC's gecompliceerd. Met name ter bevordering van de vergelijkbaarheid van SOC's is in dit rapport een standaardmodel ontwikkeld voor de basisfuncties.

5 Suggesties vervolgonderzoek en aandachtspunten

Doordat het SOC wordt opgebouwd per basisfunctie, kan de aanpak modulair verlopen en kan tevens het SOC zo worden ingericht dat meerdere gebruikersorganisaties met hun eigen bedrijfsprocessen, en meerdere beheerorganisaties met hun eigen infrastructuren kunnen worden bediend. Binnen de Rijksoverheid kan men hierbij denken aan een (Multi)Departementaal SOC of een Ketengericht SOC dat voor een of meer Ministeries zorgt voor cybersecurity en het voorkomen van IT-misbruik. Wij adviseren dit als vervolgonderzoek op te pakken.
Het meetmodel wordt vooralsnog door vakgenoten gezien als een beschrijvend model en biedt nog niet de mogelijkheid kwantitatief de effectiviteit van een SOC te meten of uit te drukken. Het advies is om een diepgaande analyse te doen en mogelijke KPI's af te leiden voor de bestaande assen. Als een SOC meetbaar wordt gemaakt kan er vanuit de organisatie sturing plaatsvinden. Via deze KPI's kan concreet worden vastgesteld of het SOC daadwerkelijk effectief opereert. De onderzoekers zien dit als een nuttige uitbreiding en stellen voor dit op te pakken als een mogelijke vervolgstudie.

5.1 Aandachtpunten voor de inrichting van een effectief SOC.

Tijdens het onderzoek hebben wij een aantal ervaringen opgedaan, die mogelijk nuttig zijn om als randvoorwaarden mee te nemen bij een ontwerp of optimalisatie van een SOC:

<u>De analisten:</u>
Een cyberaanval is mensenwerk, en het verdedigen daartegen is ook mensenwerk. Daarom is de kwaliteit en de ervaring van de individuele analisten van vitaal belang voor de doeltreffendheid van een SOC, met name voor de Intelligence-functie. De vereiste vaardigheden zijn echter nog (zeer) schaars. De verwachting is dat er onvoldoende analisten op de markt zijn om alle momenteel voorziene decentrale SOC's adequaat te kunnen bemensen. Deze schaarsheid is een van de argumenten om te pleiten voor een meer gecentraliseerde aanpak van SOC's binnen de overheid;

<u>Tooling:</u>
Meetinstrumenten zijn van essentieel belang, want 'meten is weten'. Goede meetinstrumenten zijn echter kostbaar. Door de huidige versnippering van programmatuur en licenties voor endpoint protection, scans en monitoring geeft de overheid nodeloos veel geld uit. Door trage lokale besluitvorming zijn er ook licenties waarvoor wel wordt betaald, maar die (nog) niet worden gebruikt of met een forse vertraging in gebruik zijn genomen. Standaardisatie kan tot een aanzienlijke reductie in kosten voor licenties en menskracht leiden voor de overheid;

SIEM:
Continuous Monitoring vereist het verzamelen van veel log-informatie, het selecteren en analyseren, en vooral het correleren van events. Hiervoor is een Security Information and Event Manager (SIEM) nodig. Wij komen tot de conclusie dat de juiste instrumenten en technieken hiervoor nog niet breed beschikbaar zijn, en het opzetten van de juiste rulesets nog steeds niet lukt. Op het gebied van scans en preventie zijn enkele succesvolle voorbeelden, maar bij geen enkele van de door ons bezochte organisaties is men er tot nu toe in geslaagd een doeltreffende SIEM op te zetten. Het ontwerpen van een goede methode voor een SIEM is iets wat centraal moet worden opgepakt binnen de overheid;

Informatiebeveiliging:
Een SOC is alleen effectief als een aantal essentiële onderdelen van informatiebeveiliging op orde is binnen de overheidsinstantie, zoals de governance voor informatiebeveiliging en privacybescherming, grip op het voortbrengingsproces, grip op de beheerprocessen en grip op de beheerprocessen, zoals voor hardening en patches. Het SOC is onderdeel van een groter geheel, en dat grotere geheel moet wel bestaan en werken, bij voorkeur conform de BIR;

Management Commitment:
Een belangrijke randvoorwaarde is de attitude van lokaal senior management. Worden er daadwerkelijk budgetten en menskracht beschikbaar gesteld, krijgen informatiebeveiliging en het SOC de formele status die daarvoor nodig is, of werkt men volgens 'BIR in Name Only (BiNO)'? Deze attitude verschilt per bezochte instantie.
Met betrekking tot het laatste punt geldt, dat als lokaal senior management geen prioriteit geeft aan het inrichten en financieren van een SOC, men er niet aan moet beginnen. Het opbouwen van een SOC heeft alleen zin als het SOC over een lange periode daadwerkelijk wordt gebruikt, mede gezien de forse investering en alle energie die gaat zitten in het opleiden en trainen van de expertise. Wij zien in de praktijk dat alleen de wat oudere SOC's stap voor stap effectief worden, door de daar opgebouwde ervaring, expertise en contactennetwerk. Het effectief krijgen van een SOC is een groeipad.

6 Conclusies

Het woord SOC is een modewoord. Allerlei organisaties die zich bedreigd voelen door cyberaanvallen en IT-misbruik denken dat het inrichten van een SOC de ultieme oplossing is. Zij zien het SOC dan als 'Haarlemmerolie', namelijk een oplossing voor alles, en zoeken die oplossing veelal in de techniek. Men schaft te snel dure meetinstrumenten aan, zoekt er wat mensen bij die er enig verstand van lijken te hebben, en verklaart het SOC voor geopend en operationeel actief. Het probleem van deze organisaties is dat de literatuur geen eenduidig model biedt van een SOC. White papers van toonaangevende leveranciers zoals HP, RSA, McAfee IBM gaan elk uit van hun eigen specifieke inrichting, die allemaal totaal verschillend zijn. Doordat er geen synergie bestaat over de invulling van een SOC, ontstaan op gefragmenteerde en bijna willekeurige wijze security taken die mogelijk binnen een SOC kunnen worden ondergebracht.
Er is sprake van een diffuus beeld van de term SOC. Aan de hand van ons veldonderzoek hebben wij hier invulling aangegeven en hebben wij vastgesteld welke taken in feite bij iedere vorm van een SOC zouden moeten worden uitgevoerd om de gewenste doelstelling te kunnen behalen, namelijk het realiseren van meer cyberrobuustheid. Als een organisatie een nieuw SOC wil inrichten, helpt deze decompositie. Iedere basisfunctie kan nu separaat worden ingevuld en worden gekoppeld om de daarbij benodigde verankering te realiseren. De organisatie kan het inrichten nu veel efficiënter uitvoeren, door voor iedere basisfunctie doelstellingen te formuleren en die op een wijze te gaan invullen die voor hun eigen context het meest geschikt is. Deze standaardisatie helpt tevens bij het optimaliseren van een bestaand SOC. Daarnaast kunnen nu best practices worden ontwikkeld per basisfunctie, zonder dat men een verwarrende discussie krijgt over wat een SOC nu precies inhoudt en hoe dit moet worden gepositioneerd.

7 Literatuur

[AIVD2012] Algemene Inlichtingen- en Veiligheidsdienst, (2012). Jaarverslag.

[BIG2013] Kwaliteitsinstituut Nederlandse Gemeente, (2013). Tactisch Baseline Informatiebeveiliging Nederlandse Gemeente.

[BIR2012] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2012). Baseline Informatiebeveiliging Rijksdienst: Tactische Normenkader.

[BZK2013] Plasterk, R.H.A., (2013). Brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, Nr 51.

[CBP2013] College Bescherming Persoonsgegevens, (2013). Beveiliging van persoonsgegevens.

[CIP2014] Reuijl, A., Koers, M., Paans, R., Veer van der, R., Roukens, R., Kok, C., Breeman, J., (2014). Centrum Informatiebeveiliging en Privacybescherming: Grip op Secure Software Development.

[CW2013] Redactie Computerworld, (2013). 38 grote IT-incidenten in 2013: http://computerworld.nl/beveiliging/78462-38-grote-it-incidenten-in-2013-deel-1.

[ENISA2006] European Union Agency for Network and Information Security, (2006). Een stapsgewijze aanpak voor het samenstellen van een CSIRT.

[GOV2010] GOVCERT.NL, Fox-IT, (2010). Pentesten doe je zo: Een Handleiding voor opdrachtgevers.

[GvIB2006] Tolido, R., Borsoi, P., Bronk, H., Elsinga, B., Greuter, R., Haftkamp, W., … Reijers, R. (2006). Genootschap van Informatie Beveiligers [GvIB]: CERT in de organisatie.

[HP2011] Hewlett- Packard Development Company, (2011). Building A Successful Security Operations Center: ESP-BWP014-052809-09.

[IBM2013] International Business Machines Corporation, (2013). Strategy considerations for building a security operations center: Optimize your security intelligence to better safeguard your business from threats.

[ITIG2006] IT Governance Institute, (2006). Information Security Governance: Guidance for Boards of Directors and Executive Management 2nd Edition.

[KPMG2013] Hermans, J., Schreurs, G. [KPMG] (2013). Vijf denkfouten over cybersecurity: Een bestuurdersperspectief op cybersecurity.

[McAfee2011] McAfee Creating and Maintaining a SOC, (2011): The details behind successful Security Operations Centers.

[NCSC2012] Nationaal Cyber Security Centrum, (2013). Cyber securitybeeld Nederland: CSBN-3.

[NCSC2013] Nationaal Cyber Security Centrum (2013). De aanhouder wint: De wereld van Advanced Persistent Threats. Factsheet FS-2013-02C.

[NIST2011] Dempsey, K., Chawla, N.S., Johnson, A., Jonston, R., Jones, A.C., Orebaugh, A., Stine, K. (2011). National Institute of Standards and Technology [NIST]: Information Security. 800-137.

[PINE2013] Pinewood, (2013). Datasheet Penetratietest.

[PvIB2011] Rorive, K., Beerends, M., Bordewijk, L., Breedijk, F., Cimen, H., Cornelisse, J., Smulders, A., (2011). Platform voor Informatie Beveiliging, Expertbrief Security Operations Center: Een inrichtingsadvies. ISSN 1872-4876, Jaargang 7 - Nr3.

[RSA2013] RSA Technical Brief, (2013). Building an intelligence driven security operations center.

[SIEM2012] Dorigo, S., (2012). Radboud University Nijmegen: Security Information and Event Management.

[Trend2012] Trend Labs, (2012). You have one new friend request: A guide to threats on Social Media.

[Trend2013] Wilhoit, K., (2013). Trend Micro: Who's really attacking your ICS Equipment?.

[TW2011] Wokke, A., (2011). http://tweakers.net/nieuws/76558/overheid-mogelijk-digid-inloggegevens-gestolen-door-hack.html;

Blockchain Maturity Model

Raoul van der Voort
Hardwin Spenkelink

	
Hardwin Spenkelink first got interested in cryptocurrencies and distributed ledgers in 2013 when he started mining his own cryptocurrencies. In 2014 he graduated with a masters degree at the University of Twente on the topic of the adoption of cryptocurrencies. In the same year he started working at KPMG IT Advisory as a consultant and has kept very active in the distributed ledger space. Last year (2016) he joined the newly formed global KPMG Distributed Ledger Services team as a Senior consultant.	In 2014 Raoul van der Voort graduated with a master degree at the Rotterdam School of Management (RSM) Erasmus university on the topic of cloud adoption and maturity within organizations. In 2014, Raoul started working at KPMG IT Advisory as a consultant within the financial services department. In 2017 he started at Rabobank as IT Risk Manager and is helping the organization with (IT) risks related to new technologies such as Distributed Ledger Technology (blockchain) and Cloud Computing

1 Introduction

In the past few years we have witnessed the quick rise of Distributed Ledger Technology (DLT, also known as blockchain). At the moment it seems as almost all financial institutions are involved with DLT pilots. However the use cases for DLT are far more widespread than only the financial sector, also sectors as the public sector, healthcare, supply chain, logistics and the music industry are looking at the use of this new technology. The current popularity of DLT and the enormous amount of media attention for this topic has lead Gartner to declare 2016 the 'year of the blockchain hype'. However, this does not mean that Gartner dismisses the potential of blockchain, on the contrary:

> *"As a portent for the rise of the programmable economy, the potential of this technology to radically transform economic interactions should raise critical questions for society, governments and enterprises, for which there are no clear answers today." (Gartner, 2016)*

This leads to the question what is it that DLT has to offer that is supposed to have such a profound impact on the way we do business in many industries. The key element of a distributed ledger is that it enables multiple parties to work together efficiently by offering a single source of truth, removing the need for trusted third parties and constant reconciliation between data that is siloed between organizations. This enables the automation of trust, combining this with advanced features such as 'smart contracts' enables the creation of completely automated transactions in a provably secure fashion.

According to prominent actors such as the European Central Bank (ECB), Banks of England (BoE), the Financial Stability Board (FSB), and the World economic forum (WEF), DLT will change existing business models for example; payment/transaction, trade and settlement infrastructures . In order to understand what DLT means for organizations and to fully understand its profound impact, we need to take a step back and look what happened over the past several years across various industries where the pace of technological innovation drastically increased. Over the past several years within almost every sector a shift took place from existing more traditional business models towards more new evolving business models which pose a threat to the incumbents. Due to technological improvements over the years (boundless storage, networking and infinite computing power) it resulted in an evolving and expanding array of new technologies and business models, which opened the door for new entrants. On top of that most industries must become more efficient in order to increase revenues and decrease investments and costs.

But if DLT is the "Holy Grail" that copes with these challenges organizations are facing; becoming more efficient in order to increase revenues and decrease investments and costs, why is distributed ledger technology still not adopted? In order address these questions within this paper we try to answer all these questions. We found that there have been many (academic) publications looking at theoretical use cases for DLT and benefits it would provide, however to the authors knowledge there is no literature looking at DLT implementation from an IT Risk perspective. Past studies and academic research on IT risks associated with DLT mainly have focused on theoretical aspects. In addition, most existing studies on IT risk assessments are abstract and there are no in-depth empirical analyses that determine which maturity level the organization holds on these risks.

Accordingly, this paper will attempt to fill this literature gap by developing a testable research framework and by building a self-assessment framework to measure the organizations IT maturity on IT risk associated with the use of DLT. In order to do so, an in-depth empirical analysis was conducted to develop an understanding on IT risks associated with the adoption and implementation of DLT.
In addition to the developed Maturity model, this paper enlarges to a better theoretical understanding of DLT. It contributes to our understanding on DLT and its related IT risks. In addition, this paper will gather

empirical evidence to understand DLT in practice, and contributes in supporting existing DLT literature and definitions. However, before DLT could be adopted and implemented within organizations, IT risks still remain. Therefore this paper will be relevant both practically and academically. Practically the main relevance for this research will be mainly for organizations looking at implementing a DLT and DLT providers. This paper will provide them with a framework of IT risks associated with the use of DLT. All the IT risks of DLT will be aligned with a framework, in order to assess the maturity level and the trade-off when using DLT.

As already mentioned earlier, the approach used for this paper is a design oriented research approach which has a hybrid methodology of qualitative research and case study to test if the developed maturity model is correct and useful for organizations. This approach was considered as appropriate because it provides valuable insights which could not be achieved otherwise with other research approaches.

2 Distributed Ledger Technology

In this section we give an overview of our literature research and the resulting research model. We start with describing Distributed ledger technology (DLT), in which the basics of Bitcoin, mining, blockchain and DLT is covered. In the second paragraph a comparison of different DLT protocols of both public and private blockchains is given. Finally we have analyzed earlier academic research around the topic of IT risks in the context of DLT implementations. This knowledge combined led to the creation of a DLT maturity model.

2.1 Definition of DLT

In order to be able to build a risk management framework for DLT we first need to determine how DLT can be defined. Corporations and governments all over the world are talking about blockchain and every respectable bank seems to be in a blockchain consortium. This culminated in Gartner calling 2016 the year of blockchain hype. It declared that blockchain was at the peak of its famous hype cycle and is suffering from 'inflated expectations' (see figure below). Interestingly though this does not mean that Gartner dismisses the potential of Blockchain, on the contrary:

'As a portent for the rise of the programmable economy, the potential of this technology to radically transform economic interactions should raise critical questions for society, governments and enterprises, for which there are no clear answers today.' (Gartner, 2016)

Figure 1: Gartner Hype cycle for blockchain (Gartner, 2016)

Seeing that blockchain is a hyped topic, we also see that this has led to many corporates and individuals to start building their own blockchain solution, which might be more or less based on the original blockchain as created in 2008 by Satoshi Nakamoto: Bitcoin (Nakamoto, S., 2008).

2.2 The basics

In this section we will start by describing bitcoin as a basis in order for the reader to be able to understand the mindset and way of thinking of blockchain. After describing bitcoin we will dive into other blockchains (or distributed ledgers). We will describe the basics of hashing, digital signatures, merkle roots and consensus mechanisms. These rather technical topics are the underpinnings of what is blockchain and differentiate the blockchains from one another. After discussing the aspects of different blockchains we will continue with an overview of the most prominent risks of each type of blockchain.

Blockchain generics

The key element of a distributed ledger is that it enables multiple parties to work together efficiently by offering a single source of truth, removing the need for trusted third parties and constant reconciliation between data that is siloed between organizations. This enables the automation of trust, combining this with advanced features such as 'smart contracts' enables the creation of completely automated transactions in a provably secure fashion (Spenkelink & Hough, 2017)

The Bitcoin blockchain

Bitcoin is a digital, decentralized and pseudo-anonymous currency and is the most prominent example of a 'cryptocurrency'. The main idea behind the currency is to provide a fast way to transfer funds globally, with minimal transaction costs, with a certain amount of privacy and without the need for a trusted third party (Trautman, 2016) In order to facilitate this cryptocurrency, a system is needed to keep track of who is the legitimate owner of the currency and to prevent one from spending the same money twice (a so called "double spending attack") (Nakamoto, 2008). This system is what is known as the blockchain. In 2008 the anonymous author under the name of Satoshi Nakamoto published a whitepaper describing the working of the Bitcoin blockchain. The main idea of this blockchain is to have all transactions publicly announced and sorted in blocks, with each block cryptographically chained to the previous block in order to achieve tamper resistance (Nakamoto, 2008).

Blockchain architecture

Figure 3 shows the architecture of the Bitcoin blockchain. We are looking at a chain of three blocks, block 10 to block 12. What can be seen is that each block contains four items, namely all transactions (tx_root), a timestamp to prove when a block was mined, a nonce (random value used in the mining process) and most notably: the hash value of the previous block. By including the hash value of the previous block a link is created, because block 12 will link to block 11, but then block 11 also links back to block 10, and so on. Because all blocks link to each other if one is sure that the last block in the chain is to be trusted, then one can be sure that all transactions included in previous blocks are correct as well. This gives blockchain its powerful immutability. (Nakamoto, S., 2008)

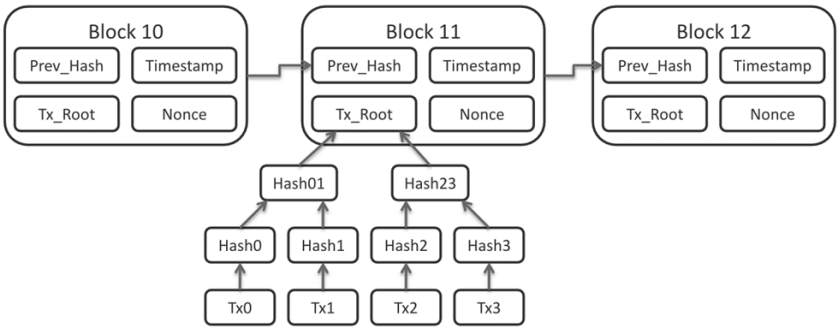


Figure 2: Bitcoin Blockchain

Mining

So called "miners" are users that are building the blocks in the blockchain described in the section above. By solving a computationally hard problem, they "prove" that they processed the transaction and that it is legitimate (Babaioff, Dobzinski, Oren, & Zohar, 2012). This problem is called a "proof of work" and it is constructed in such a way that it is difficult to solve, meaning costly or time-consuming, however trivial to check by others to see if the miner actually put in the required effort.

This concept of "Proof-of-Work" is essential to cryptocurrencies because it guarantees the integrity of the block chain. Proof of Work is a type of consensus mechanism, this system is used to reach a consensus among the nodes in the network that these transactions are valid and are stored in a block. It is interesting to note that Proof of Work is simply one of many different consensus mechanisms and it is one of the defining factors of Bitcoin. We will discuss other consensus mechanisms in the next section of this thesis.

By having Proof of Work in place an attacker cannot simply change one transaction in a block, he would have to change the entire blockchain from the point this transaction occurred and thus do all the work again. If the processing power of the network increases, so does the difficulty of finding a block. Therefore the more processing power the network has, the more difficult it is for a malicious actor to disrupt the network. (Gervais et al., 2016)

Because of this reliance on "miners" they are rewarded for their computational efforts. Every time a miner is first in "creating" a block in the blockchain, a predetermined amount of Bitcoins are created which he owns. (Nakamoto, 2008)

Since no Bitcoins are issued by a central authority this is the only way in which Bitcoins enter circulation. This does not mean that there is an infinite number of Bitcoins to be mined. Due to the specification of the Bitcoin protocol there is an exponentially decreasing number of Bitcoins to be earned per mined block, leading to a maximum of 21 million bitcoins in circulation. Each of these 21 million bitcoins is however divisible into 100 million units leading to a nearly infinite amount of pieces of bitcoin.

Distributed ledger technology

DLT can be seen as the overarching name for a combination of Distributed Ledger products, including Public Permissionless Distributed Ledgers such as the Blockchain and Private Distributed ledgers, such as IBM's Hyperledger or R3's Corda.

Bitcoin is the quintessential example of a public distributed ledger. In such an open distributed network, transactions are transparent and every user can join or leave the network at any time. These properties make it suitable for a large number of widely distributed parties to work together and create value. The fact that transactions are transparent, the network access is unrestricted and the code is open source means that anybody can check transactions or build applications on top of the distributed ledger.

A public distributed ledger has at its basis a cryptocurrency, this provides the ledger with a built-in economic incentive for participants since currency is earned for participating in the network, for instance by providing processing power. This is in contrast to a private distributed ledger where the incentive for participation is not built into the system but contractually organized. Examples of public distributed ledgers are: Bitcoin (currency), Ethereum (smart contract platform) and Steem (social networking).
Although transactional privacy is the main concern due to their architecture other differences between public and private ledgers exist. The main ones are summed up in figure 3. (Spenkelink & Hough, 2017)

	Public blockchain	Private blockchain
Participation in network	Open	Closed
Transactional privacy	Not prioritized except for so-called anon-coins	Adjustable to the wishes of the participants
Economic incentive for participation	Built-in	Contractually organized
Transaction volume supported	Low	High
Commonly used for	Payments, remittances, prediction markets, distributed storage, paid social networking	Asset servicing, FX (Foreign eXchange), provenance tracking, trade finance, health care

Figure 3: Public versus Private ledgers (Spenkelink & Hough, 2017)

The distinction between public and private ledgers becomes more granular based on the anticipated need from different industries for both public and private distributed ledgers to come in permissioned versions. Meaning participation in the network can be open or closed based irrespective of whether the transactions in the distributed ledger are public or private. Figure 4 illustrates this continuum.

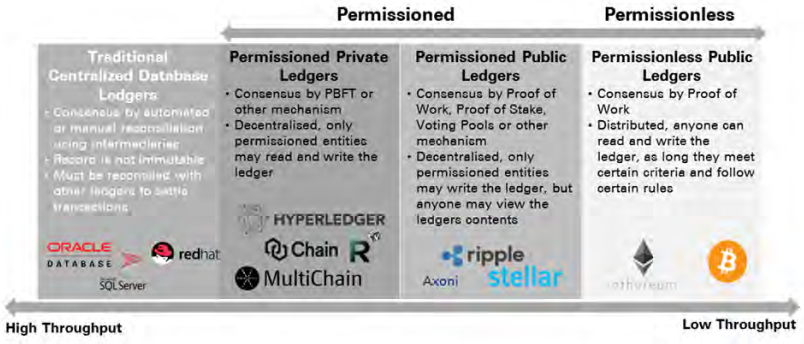
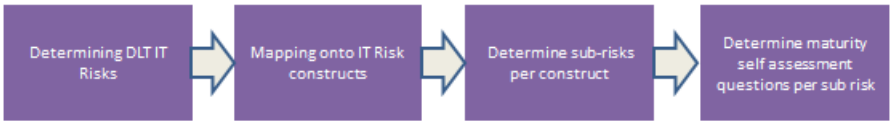


Figure 4: Distributed Ledger landscape (Spenkelink & Hough, 2017)

What we see happening in the market is that many solutions in the middle of the spectrum are starting to form, which are comprised of elements of blockchain, being decentralized and based on cryptography, however they are also private. Taking for example the R3CEV consortium: this is a consortium of more than 80 of the biggest financial services institutions worldwide (including ING and ABN AMRO). Together they have built the Distributed Ledger system Corda. Corda enables the banks to work together and share information and transactions, however this is done in a private manner by only allowing the banks involved in a transaction to see the contents (Acheson, 2017; Groenfeldt, 2017) .

3 Creating a Distributed Ledger Maturity model.

In the previous paragraph the basic concept of DLT is defined. In the second paragraph the underlying theory of DLT was studied. In this paragraph we describe how we have come to our maturity model. In order to create the maturity model, in the next subparagraphs we outline the steps to arrive at the maturity model;



3.1 Determining DLT IT risks

The concept of DLT in particular its use cases (e.g. bitcoin blockchain, Ethereum blockchain) and benefits has extensively been studied. In this literature review an attempt was made to cover most prominent studies, and enlarge to a better theoretical understanding. The concept of IT Risks in relation to DLT is a new concept that has not been studied and explored a lot (Berke, 2017; Lansiti, Marco; Lakhani, 2017).

The outcome of this study on risks associated with DLT is a list of constructs (IT risks) related to DLT implementation. These risk constructs were used to build an IT risk maturity model in relation to the implementation of DLT. This IT risk maturity model is a self-assessments for organizations that want to implement DLT within their organization. By using the model, organizations are able to determine what their IT risk maturity level is on each risk dimension.

Concept of IT risk

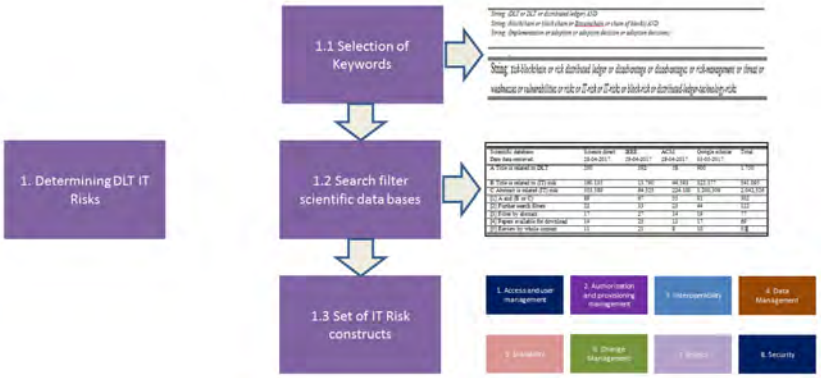
All industries show interest in adopting DLT within their organization. Although IT risks related challenges and concerns appears as one of the main impediments for adopting and implementing this technology (Hogan, n.d.; Lageschulte et al., 2016; Walch, 2015; Zheng, 2016). Different studies use different definitions of IT risk in the context of implementation and adoption of DLT (Lageschulte et al., 2016; Walch, 2015; Zheng, 2016), in order to use the best IT risk definition for this paper we used the definition by ISACA as leading:

ISACA, uses a broader meaning of IT Risks, in which it encompasses not just the negative impact of (business) operations but also looks at the benefit value trade-off enabling risk associated to missing opportunities (Stoneburner, Goguen, & Feringa, 2002)(Détienne et al., 2013).

IT Risk is defined as:
"The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise"

Generating a pool of IT risks items

In order to generate an initial pool if IT risk items that represent the constructs, a structured literature review was conducted to develop the content domain for this study. According to Vom brocke et al. (2009), validity of study constructs can be reached by performing a comprehensive literature study and literature study process (Vom Brocke, Simons, Niehaves, Niehaves, & Reimer, 2009). To do so, it involves the selection of scientific databases, keywords on the papers topics and journals. We conducted this literature review by focusing on the research outcomes described and applied in the analyzed articles. The process of generating a pool of IT Risk items was as follows:



The goal for this part of the literature review was to integrate current IT risk items into the research. All items found were summarized into a neutral perspective, interpreted as subjective and with an overall coverage as possible. Because of the scope of this research, and uses of certain scientific databases we tried to cover the availably literature for this study as much as possible. In order to merge related IT risk items together, the results of the literature study were organized and arranged conceptually based on focus area.

3.2 Mapping on IT risk constructs

We found that most recent literature on risks related to DLT is focused on IT risks related to: data (in the context of privacy and integrity), change management, security, interoperability, regulatory, user access and provision risks. The aforementioned studies related to IT risks were used in combination with existing literature to make the IT risk construct for this study complete. Investing in DLT technologies exposes an organization to several IT risk factors. Certain IT risks found related to blockchain implementation within organizations are diverse and comparable with risks from IT outsourcing and cloud computing. The most frequently mentioned risks in previous studies include data management, inter-operability, scalability and security. However IT risks related to DLT span a broader spectrum than the more standard IT risks for technologies. For example, risks associated with compliance (privacy), user access management (within a distributed environments) and change management risks due to fragmented implementation were found to impact organizations. Furthermore can the distributed nature of DLT lead to accountability risks; since there is no owner of the network? Below all eight risks constructs found in the literature review are described in more detail. The most mentioned IT risks in previous studies have been grouped below:

User access management

User access management across organizations is a relatively new concept, where no best practices and standards have been found and set for so far. Blockchain uses unique addresses which are assigned to each participant in the network. This address is used for transactions (sending and receiving) and enable participants to authenticate themselves and these transactions by using a public key.

The provisioning process of these key-pairs (unique identifier) and assigning access rights is different for each DLT implementation. Due to the fact that DLT heavily relies on digital identity means that adequate management and security around the process of providing and storing the cryptographic keys is of great importance. In addition, users from multiple organizations, with user access authorizations are difficult to manage because the network is distributed, at this moment there is no oversights/supervisory body which checks on valid access rights

This results in risks of unauthorized access of participants (organizations) and users due to the lack of an overall supervision/oversight that manages access for user and participants

Authorization
In current blockchain concepts there is no system that adequately prevents violations in segregation of duties, uses a role-based access model and restricts access. Every organization has its own users, and user authority which will be difficult to segregate and manage all role and authorizations.

This results in risks such as: incorrect authorizations, abuse of high privileged or over authorized users.

Interoperability
Just like all other new technologies, blockchain is facing issues integrating with (legacy) IT platforms. This could result in potentiality costly operational challenges, for example the conversion of data models and business processes, the incorporation of new authentication and communication protocols/systems.

The main IT risk there is focusses on the failure to fully integrate the two "worlds" (IT legacy and blockchain technology) which result in weak internal control mechanisms, for example authorization or security processes which are not covering the whole organization/network.

Data Management (Integrity, availability and governance)
Using DLT results in a growing chain of transactions and volume. The risk for financial services lies within the data used for transactions. The presence of corporate data that is stored outside the organizations network, and the use of metadata that is not part of the blockchain transaction leads to risks that are similar to outsourcing.

Within the construct data management we made a distinction in three risks related to data (data management)

Data confidentiality
Data confidentiality, is focused on the risk that data is available to unauthorized parties. Because financial services have sensitive data (on personal or business level), confidentiality considerations needs to be made how to cope with these risks.

Data availability
Data availability means that data needed for blockchain transactions is accessible to authorized user. Availability is related to integrity because the data within the blockchain is needed to achieve a consensus when transactions are performed. For the transaction process, it is critical that data is always available

Data integrity
Data integrity is about persevering the accuracy, consistency and validity of data. This should be done by maintaining the integrity of data through protecting it from invalid modification, insertion or deletion.

Change Management
Because of the nature of DLT (a distributed network of participants), changes made to the platform require agreement and implementation of all participants. Current initiatives within financial services where a consensus has to be found for technology standards/industry adoption have a lead time between 6 months and 2 years.

The risks exists that the blockchain will be fragmented with multiple versions/rollouts leading to forks in the blockchain. Furthermore, it may decrease the velocity in which new functionalities and features can be introduced.

Privacy
Privacy in DLT systems is a very complex risk. Due to the fact that DLT systems are append only, data can never be removed from the blockchain. Therefore one has to be very careful which data is placed in the blockchain and which data is kept elsewhere. The fact that data in a DLT system is shared and stored across multiple locations makes managing this risk even more difficult.

Scalability & Performance
Current blockchain concepts/platforms have not come up with proof of concepts (PoCs) that prove and show that they can handle high-volume transactions. Blockchains will become interesting for financial services if blockchains can replace high volume transactions like payment/clearing processes which are typical for financial services environments.

This results in IT risks of potential system failure (through processing speed), scalability issues (upscaling capacity by adding more nodes).

Security
Although, blockchain tackle a lot of security concerns existing technology are facing, through its distributed characteristics there are still some (IT) security risks blockchain technology is facing.

The first IT security risks focusses on network architecture, within this study we focus on permissioned blockchains used by financial services. One of most important requirement within financial services for technology is continuity and integrity of its (IT) processes and services.

Blockchain achieve consensus on their ledger, this is done through communication, and communication is required to write and approve new transactions.

Risk: Consensus and integrity risk caused by insufficient security (control) mechanism or violation of node restrictions caused by nodes maintained/operate by (un/wrong) authorized participants.

3.3 Determine sub-risks per risk construct and

In the previous paragraph the eight risk constructs found in literature were described in detail. We found that all these risk factors are associated with using and implementing DLT. In the section below further details of these 8 risks of DLT were described and self-assessment questions were derived from existing literature. All the risks in a given construct affect the objective of the corresponding overall dimension of IT maturity.

Access and user management.
As already mentioned earlier, implementing DLT, and participating in a network results in access and user management which is difficult to manage because it is a distributed environment with no centrally managed body that check on valid access rights and has a policy wide approach (Berke, 2017; Lageschulte et al., 2016; Walch, 2015). Base on the literature review performed, we found three types of risks associated with access and user management related to DLT.

1 Unauthorized access of participants: Within Permissioned DLTs network the risk of unauthorized access still exist. Because at this moment every participant can grant new members access to the network, it is

possible that unauthorized/untrusted parties will gain access (Berke, 2017; Lageschulte et al., 2016; Walch, 2015);

2 Users are not uniquely identifiable: DLT uses unique addresses which are assigned to each participant in the network. This address is used for transactions (sending and receiving) and enable participants to authenticate themselves and these transactions by using a public key. The provisioning process of these key-pairs (unique identifier) and assigning access rights is different for each DLT implementation. Due to the fact that DLT heavily relies on digital identity means that adequate management and security around the process of providing and storing the cryptographic keys is of great importance (Berke, 2017; Lageschulte et al., 2016; Walch, 2015);

3 Authentication mechanisms are not working: The DLT mechanism relies on unique addresses that are assigned to each member, which are used for sending/receiving and authenticating transactions via a PKI infrastructure. Inadequate authentication mechanisms could results in authentication risks. The process of proving the counterparty identities and the existence of assets via private public keys (Berke, 2017; Lageschulte et al., 2016; Walch, 2015).

Authorization and provisioning management

As indicated in the previous paragraph, within distributed ledger concepts there is no system that adequately prevents violations in segregation of duties, uses a role-based access model and restricts access. Every organization has its own users, and user authority system instead of network-wide systems used by all participant, which will be difficult to segregate and manage all role and authorizations (Hogan, n.d.; Lageschulte et al., 2016; Lindman et al., 2017)(Vukoli, 2017). Based on the literature review performed we found two risk types related to DLT:

1 Incorrect authorizations: Authorization management is the first defense line for organizations to have control over activities performed within the organization. Because DLT nature as decentralized network with multiple participants it's difficult to manage all these authorizations network-wide. First, there must be a consensus how it should be arranged between all organizations. Due to the lack of a centrally managed systems and oversight body around authorization management, there is a risk that participant (organizational level) or users have incorrect authorizations such as over authorized users, or incomplete insight into what roles/authorizations users and participants has. (Hogan, n.d.; Lageschulte et al., 2016; Lindman et al., 2017)(Vukoli, 2017)

2 Abuse of high privilege users: Within distributed ledger networks high privilege users occur on every level within the network (participant/organizational, user and oversight authorities). The function of high privilege users is for example to deploy changes to production (nodes) within the network, or as a holder of the private key (e.g. organizational level) to sign transaction batches. The risk exists that if there are no procedures, system enforced controls and monitoring activities in place, activities of high privilege users could be unauthorized and traceable (Hogan, n.d.; Lageschulte et al., 2016; Lindman et al., 2017)(Vukoli, 2017)

Interoperability

Although most distributed ledger initiatives are open-sourced, DLT is facing issues with the integration of both "worlds". Integrating this new technology with legacy IT platform, could result in potentiality costly operational challenges. According to SWIFT (Europe's biggest FMIs intermediary (Kech & Markets, 2016) and ENISA (ENISA, 2016), the main interoperability challenges for financial services that adopt DLT will be the conversion of data models, business processes, incorporation of new authentication and communication protocols and systems. Based on the literature review performed (ENISA, 2016; Kech & Markets, 2016;

Lageschulte et al., 2016; Mclean & Deane-johns, 2016; Seibold & Samman, 2016) we found two risk dimensions related to DLT:

1 Current security mechanisms in place do not cover all risks within the new (DLT/DLT) environment. Integrating DLT with legacy IT platforms is a potentially costly operational challenge. Participants will need to convert data models and business processes and incorporate new authentication and communication protocols.

2 Continuity issues in data processing between systems (legacy vs DLT) leading to inconsistencies. If for some reason a discrepancy occurs between the data in the DLT and data in legacy systems this can lead to complex problems. As data in the DLT cannot be changed it is hard to correct inconsistencies.

Data management

Over the last couple of years, data management have become more important. Data management allows organizations to response better to sudden changes in business models (e.g. new products), regulatory requirements (e.g. BCBS 239) and is the most important strategic source of information about clients and markets. For DLT, data and data management is important because it is the foundation for block chains to work. Without the integrity and availability of data, DLT is not able work. In order to work, all underlying mechanisms and infrastructure, such as consensus mechanisms (nodes), block technology and transaction throughput. Based on the literature review performed we found that the risk for financial services lies within data used for transactions. The presence of corporate data that is stored outside the organizations network, and the use of metadata that is not part of the block chain transaction leads to risks that are similar to outsourcing. We found three types of risks related to data management:

1 Data used within the DLT is invalid or not accurate and/ or data is modified, inserted or deleted inappropriately: As with more traditional IT systems data integrity is of high importance. DLT offers to advantage that modifying of data is in most cases hard or even impossible. However this still means that the data that is put in the DLT has to be of high quality. Data quality checks have to be in place. When onboarding real world objects into the block chain, this connection has to be made by a trusted party to ensure that one can rely on the contents.

2 Data is unavailable for the system: The risk for data availability is when a DLT either loses connection with the underlying data sources that might be used, or when a check pointing system is not available and data gets unwillingly erased.

3 Data is visible for non-authorized parties: Since a DLT is focused towards sharing data with all participants in the network, a risk is that data is shared with and visible to parties that are not authorized to view this.

Scalability and performance

One of the main open questions about block chain and DLT is the questions if it can handle high volume transactions. As already mentioned earlier, current block chain concepts have not come up with proof of concepts (PoCs). Though, permissioned distributed ledgers on the other hand could overcome this challenge by setting up and configuration the infrastructure in a certain way. Based on the literature review performed we found that scalability and performance risks can be classified into two risk dimensions; scalability issues of the platform resulting in not enough performance and a lack of pre-defined arrangement between participants that result in slowing down the network by executing large transactions. Both risks found are described in more detail below:

1 The platform is not scalable enough to deliver the performance needed: DLT scalability is reverse from 'regular' IT scalability. When adding more nodes to the network, this results in longer processing times

due to the fact that consensus has to be reached among the participating nodes. This means that a risk is that the network does not scale well when adding more nodes.

2 Network participants slow down the entire network with large transactions: The DLT network runs the risk of participants clogging the network with an extreme amount of large transactions or transactions with a high smart contract complexity leading to excessive resource consumption

Change management

Blockchain and DLT initiatives have been struggling for a while now how change management and changes related to the network in particular should be addressed. Because the complex infrastructure DLT uses it is difficult to roll-out changes within the entire network all at once. At the time of writing, the most known distributed ledger "bitcoin" shows how difficult it is to setup change management and mitigate the risks (Hertig, 2017). Due to a lack of consensus regarding changes and how changes should be deployed, in case of the bitcoin blockchain it led to a (soft) fork of the network. In order to determine which risks related to change management organizations are facing, we performed a literature review (Kaivanto & Prince, 2017) and found two risk dimensions;

1 Unauthorized changes are put into production. Since the DLT network is a distributed system one runs the risk that when unauthorized changes are put into production that all network participants are affected (Kaivanto & Prince, 2017).

2 DLT forking due to incorrect change management. If the different participants in the DLT network do not upgrade their platforms simultaneously a DLT fork could occur leading to a split in the DLT (Kaivanto & Prince, 2017).

Privacy

Another, major issue DLT is facing is about the privacy of its users. As tempting as DLT advantages are, neither organizations, individuals nor governments are keen on publishing all of their information onto a shared network that could be read by other participants without any restrictions. Compared to permission less distributed ledgers, permissioned distributed ledgers have the ability to set restrictions on which information is shared and/or visible for other participants within the network. So far, most solutions used within current existing distributed ledgers regarding privacy are not satisfying enough to be used within financial services. Therefore it is much harder to find and create a "holy grail" solution for DLT that allows users to do absolutely everything they can do right now with current existing financial products, but with complete privacy. The main goal for DLT developers will be to find the best solution in which they are forced to contend with partial solutions, heuristics and mechanisms that are designed to bring privacy to the distributed ledger solution provided. In order to determine which risks related to privacy organizations within financial services are facing, we performed a literature review (Berke, 2017; Buterin, 2016; Deloitte, 2016; European Parlament, 2016; Lansiti, Marco; Lakhani, 2017; Li & Sforzin, 2017; Perez-Sola, Christina; Joancomarti, 2016) and found two risk dimensions;

1 Non-compliance with data privacy regulation (GDPR): Privacy in DLT systems is a very complex risk. Due to the fact that DLT systems are append only, data can never be removed from the DLT. Therefore one has to be very careful which data is placed in the DLT and which data is kept elsewhere (Berke, 2017; Buterin, 2016; Deloitte, 2016; European Parlament, 2016).
2 Data is visible for non-authorized parties: Since data in a DLT is shared with network participants, a risk is that certain transactional data is visible to parties that should not have access to this data. elsewhere (Berke, 2017; Buterin, 2016; Deloitte, 2016; European Parlament, 2016).

Security

(Cyber) Security and DLT go hand in hand with each other on both sides; advantages and disadvantage of using DLT. DLT tackles a lot of existing security concerns current technologies are facing. Currently each financial organization is working on protecting itself against external (cyber) attacks on the infrastructure. Due to distributed ledger's nature as a distributed infrastructure technology which is shared with all participants of the network most (cyber) security issues of current technologies are mitigated. However, through its distributed characteristics there are still some (IT) security risks DLT is facing (Berke, 2017; Lansiti, Marco; Lakhani, 2017)

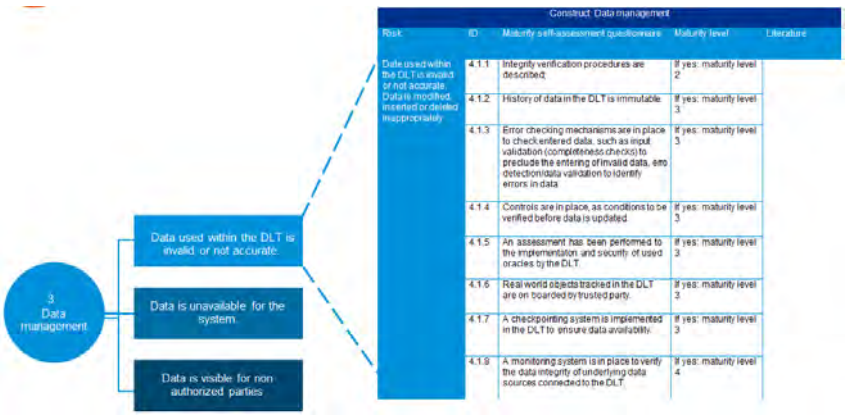
This study focusses on permissioned distributed ledger used by financial services. Therefore in our literature review we focused on potential security risks associated with these two variables. Based on one of most important requirements within financial services for technology "continuity and integrity" of its (IT) processes and services we found that the nodes performing the consensus check within the network is considered as main security issue for financial services. Distributed ledgers achieve consensus on their ledger through communication, and communication is required to write and approve new transactions, if we look to most recent attacks the DAO incident (del Castillo, 2016), and the Bitfinex breach (Baldwin & Reuters, 2016) we conclude that further steps need to be taken in the field of security.

Based on the literature review performed (Berke, 2017; Gervais et al., 2016; Karame & Ghassan, 2016; Lansiti, Marco; Lakhani, 2017)we found one risk dimension which is the most relevant security risks for financial services; Consensus and integrity risk caused by insufficient security (control) mechanism or violation of node restrictions caused by nodes maintained/operate by (un/wrong) authorized participants. Resulting in the following risk construct:

1 A node within the network is compromised. The risk is that when a node in the DLT network is compromised, incorrect or corrupt data might be added to the DLT.

3.4 Determine self-assessment maturity questions

In the previous steps we build up the maturity model up to sub-risk. In the last step we translated each of these sub-risks into maturity self-assessment questions. In order to keep this paper brief we have included a small part of the maturity model in the section below.



Construct: Data management

Risk	ID	Maturity self-assessment questionnaire	Maturity level	Literature
Data used within the DLT is invalid or not accurate. Data is modified, inserted or deleted inappropriately	4.1.1	Integrity verification procedures are described.	If yes: maturity level 2	
	4.1.2	History of data in the DLT is immutable.	If yes: maturity level 3	
	4.1.3	Error checking mechanisms are in place to check entered data, such as input validation (completeness checks) to preclude the entering of invalid data, error detection/data validation to identify errors in data.	If yes: maturity level 3	
	4.1.4	Controls are in place, as conditions to be verified before data is updated.	If yes: maturity level 3	
	4.1.5	An assessment has been performed to the implementation and security of used oracles by the DLT.	If yes: maturity level 3	
	4.1.6	Real world objects tracked in the DLT are on boarded by trusted party.	If yes: maturity level 3	
	4.1.7	A checkpointing system is implemented in the DLT to ensure data availability.	If yes: maturity level 3	
	4.1.8	A monitoring system is in place to verify the data integrity of underlying data sources connected to the DLT.	If yes: maturity level 4	

4 Distributed ledger technology maturity model in practice

Case study

This chapter presents a business case, describing DLT (DLT) for a Top 20 Bank in Europe. The aim is to address the question whether DLT is suited, and whether this Bank adequately addressed the IT risks when adopting DLT. Apart from the solution, the case is interesting in that it shows which maturity level this big bank holds on its route to the adoption of DLT.

This top 20 Bank is a universal banking group, with headquarters in the Netherlands. It operates in several market segments, embracing different business contexts mainly focused on wholesale, rural and retail in the agri-food sector. Furthermore, it offers a full range of retail (commercial and SME), private and business products.

Background
Just like all financial services, this bank is also pushed in becoming more efficient in order to increase revenues and decrease investments and costs. That is one of the reasons why they started exploring the possibilities of DLT. To support these challenges, they started developing distributed ledger concepts alone and together with other banks in a consortium to gain knowledge and come up with new products and opportunities.

In this case study we evaluated the DLT IT risk framework by assessing the "the DLT initiative in which they participate. The DLT initiative is an international project, run with 6 other European banks. To quote:

> *"A group of seven banks has agreed in principle to develop a ground-breaking shared platform that aims to make domestic and cross-border commerce easier for European small and medium-size (SME) businesses by harnessing the power of DLT.*
>
> *This new product will simplify trade finance processes for SMEs by addressing the challenge of managing, tracking and securing domestic and international trade transactions. Larger companies use documentary credit as a way of reducing the risks involved in doing business, but documentary credit is not always suitable for SMEs or for companies that prefer open account solutions." (Top 20 bank 2017).*

Use case DLT initiative
The DLT initiative is a blockchain-based digital platform for managing and tracking domestic and cross-border Open Account trade transactions securely. The aim of the platform is to make domestic and cross-border commerce easier for European small and medium-size (SME) businesses by harnessing the power of digital DLT.

It will enable authorized customers to initiate transactions on a paperless but secure basis, and track the transaction at each stage of transaction lifecycle, through to the point of settlement/payment.

By maintaining secure records on a digital distributed ledger, this DLT initiative has the potential to accelerate the order-to-settlement process, and significantly decrease administrative paperwork.

5 Conclusion

We started this paper with the question if Distributed Ledger Technology is "the technology" that will help organizations innovate, reach their objectives, and support them in becoming more efficient, increase their revenues and decrease the cost of investment. Before we answer this question, we need to understand, the challenge of innovation in an increasingly digitized business world that requires a clear understanding about the role of information technologies like Distributed Ledger Technology and how they can be used to shape

new business models. Addressing the impact DLT is likely to require significant change on the part of both organizations and individuals, and significant change is something that many (if not most) of us often find hard to do.

The impact of new complex technologies, such as DLT can often be difficult to grasp. With this paper we have aimed to discuss and present the main challenges in the context of IT risks DLT is facing. By taking these challenges into account, we tried to make it easier for organizations to implement DLT.

By making use of the case study, we have found that some IT risks both within Banks (please see the results of our use case) and other sectors as well need to be further developed, agreements and standards need to be defined and new and or other controls need to be introduced.

In addition, by looking at the developed IT maturity self-assessment and use the results of the case study to determine if the self-assessment is working and fulfils the requirements set; making IT risks transparent, act as control mechanism and guide organizations in their maturity.

5.1 Analysis

The use case studied is a very interesting example of how blockchain or Distributed Ledgers can be used in practice. We see that at the moment almost every organization is looking at DLT and is performing the first experiments. While many of these experiments are of a very simple nature and could possibly be performed by hosting a central system, already a trend is showing. DLT is forcing companies to have a look at their entire value chain and to think in terms of networks and working together rather than developing your own internal IT system and trying to gain a competitive advantage out of that. Without a doubt we will see much more DLT pilots the coming months and years and possibly the first usages of blockchains in a production environment will start to occur.

Just as with the rise of the internet, and for instance, payment systems such as a debit or credit card consumers do not need to know how exactly a DLT system works. As long as a DLT enables companies to deliver the same services, but faster or cheaper this benefits the consumer and one could say that its goal is reached. With this point in mind, we also look at the question that concerns the whole sector: *"can DLT replace banks and especially the underlying infrastructure, such as FMIs."*.

During our literature review on IT risks associated with the use and implementation of DLT by financial services, we found that there are several IT risks that have an impact on the use of DLT, please see chapter 2 for the complete list of IT risk constructs found. In order to assess the actual impact of these IT risks, we have made these risks measurable, which helps to gain insight into how mature an organization is that uses or wants to use DLT in the context of IT risks. The maturity self-assessment on IT risks we performed for the use case, showed that from an IT risk perspective, DLT offers a lot of new challenges. As we have discovered when creating this DLT maturity assessment, there are many different facets in which a DLT system is different from a more traditional IT system. The fact that a DLT system cannot be viewed as a standalone system, but rather is just one actor in a network, capable of making transactions that are irreversible and broadcasted to all relevant parties leads to a whole new range of IT risks on many different levels.

Overall we can conclude that most IT risks associated with DLT need a different approach than more "traditional" IT risks. Based on our results, we can state that IT risks have an impact on the use and implementation of DLT. The challenge for organizations that want to use DLT is therefore to convert these IT risks into mitigating procedures that eliminate these risks.

5.2 Conclusion

Following the results of the literature review; a list of IT risks constructs that impact the use and implementation of DLT, we came to the conclusion that these constructs need to be measured in order to provide insight into the maturity of the organization. In order to determine the level of impact of the risk constructs found, we built and developed an IT maturity self-assessment with as objective to give organizations more insight and guidance into how mature they are on these themes. By looking at the developed IT maturity self-assessment and use the results of the case study to determine if the self-assessment is working and fulfilling the requirements set; making IT risks transparent, act as control mechanism and guide organizations in their maturity.

After evaluating the use case we can conclude that we think that for most organizations improvement can be made on the topics of interoperability, scalability and change management. Authorization and provisioning management and security.

What we have found is that the focus is on getting the DLT solution up and running as quickly as possible, leads to the areas of access and user management, data management and privacy getting a lot of attention. Area's that do not dictate immediate attention are left to be resolved at a later time.

During the interviews held with stakeholders and SMEs we noted that many of our maturity indicators were steps that organizations were thinking of implementing, but that were not actually implemented at that moment in time. For example with regards to change management of the use case studied, concrete policies and procedures on how to manage this were still under development. At the moment most organizations only have the traditional IT change management policies in effect, however there seems to be a gap between this policy and the reality of using a DLT system.

5.3 Will this maturity model help?

A DLT enables multiple parties in a value chain to work together and share data and processes very efficiently. This reduces administrative work, reduces the risk of fraud by creating an audit trail of transactions and enables the automation of common business processes with the use of smart contracts. However, due to the nature of a DLT system, implementation also introduces new and specific risks that do not exist in current financial transaction processing systems. This is because a DLT system is an interconnected system in which multiple parties cooperate and share data, combined with the fact that all transactions logged on this system are irreversible.

The literature study shows that most IT risks associated with DLT need a different approach than more "traditional" IT risks. The challenge for financial services firms that want to use DLT is therefore to convert these IT risks into mitigating procedures that eliminate these risks. In addition, it is concluded that the necessary steps must be taken before DLT can replace existing technologies.

By combining an IT risk maturity model with DLT specific risks as found in the current literature, a maturity model can be created to measure DLT IT risk maturity. This enables the user of the framework to assess maturity and give specific and prioritized recommendations tailored to the situation.

The case study shows the value of having a DLT maturity assessment as it can help not only by giving an impression of the current state but it also helps to create a well-founded and prioritized action plan to improve maturity levels. The overall conclusion is that DLT is still a very immature technology and more research will have to be performed about keeping control over a DLT system and making sure that all IT risks are properly dealt with.

6 References

(NIACAP), N. I. A. C. and A. P. (2000). Certification and Accreditation Process (NIACAP). Security, (1000).

Acheson, N. (2017). Consensus 2017: Blockchain Consortia in A Rapidly Changing Market - CoinDesk. Retrieved September 3, 2017, from https://www.coindesk.com/consensus-2017-blockchain-consortia-rapidly-changing-market/

Babaioff, M., Dobzinski, S., Oren, S., & Zohar, A. (2012). On bitcoin and red balloons. In Proceedings of the 13th ACM Conference on Electronic Commerce (pp. 56–73).

Baldwin, C., & Reuters. (2016). Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong. Retrieved September 18, 2017, from https://www.reuters.com/article/us-bitfinex-hacked-hongkong/bitcoin-worth-72-million-stolen-from-bitfinex-exchange-in-hong-kong-idUSKCN10E0KP

Becker, J., Niehaves, B., Pöppelbuß, J., & Simons, A. (2010). Maturity Models in IS Research. Retrieved from http://aisel.aisnet.org/ecis2010/42/

Berke, A. (2017). How Safe Are Blockchains? It Depends. Retrieved August 6, 2017, from https://hbr.org/2017/03/how-safe-are-blockchains-it-depends

Bis. (2012). Financial Markets Infrastructure.

BIS. (2017). Principles for Financial Market Infrastructures (PFMI). Retrieved September 3, 2017, from http://www.bis.org/cpmi/info_pfmi.htm

BoE. (2017). FinTech Accelerator Proof of Concept Distributed Ledger Technology The Proof of Concept. Retrieved from http://www.bankofengland.co.uk/Documents/fintech/fintechpocdlt.pdf

Brown, R., Carlyle, J., Grigg, I., & Hearn, M. (2016). Corda: An Introduction. R3 CEV, August. Retrieved from https://www.researchgate.net/profile/Ian_Grigg/publication/308636477_Corda_An_Introduction/links/57e994ed08aed0a291304412.pdf

Bruin, D., Rosemann, M., & de Bruin, T. (2005). TOWARDS A BUSINESS PROCESS MANGEMENT MATURITY MODEL, 26–28. Retrieved from https://eprints.qut.edu.au/25194/1/25194_rosemann_2006001488.pdf

Buterin, V. (2016). Privacy on the Blockchain - Ethereum Blog. Retrieved August 20, 2017, from https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

Cermeño, J. S. (2016). Blockchain in financial services : Regulatory landscape and future challenges for its commercial application, (December).

Coindesk. (2016). The DAO Attacked: Code Issue Leads to $60 Million Ether Theft. Retrieved April 26, 2017, from http://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/

Cpss-iosco. (2012). Committee on Payment and Settlement Systems Principles for financial market infrastructures. Retrieved from http://www.bis.org/cpmi/publ/d101a.pdf

CPSS-IOSCO. (2017). Press release: CPSS-IOSCO principles for financial market infrastructures. Retrieved September 3, 2017, from http://www.bis.org/press/p110310.htm

Crawford, M. (2017). Risk Management – The Insurance Implications of Blockchain. Retrieved September 16, 2017, from http://www.rmmagazine.com/2017/03/01/the-insurance-implications-of-blockchain/

Cross, N. (2001). Designerly Ways of Knowing: Design Discipline Versus Design Science. Design Issues, 17(3), 49–55. https://doi.org/10.1162/074793601750357196

CSD. (2017). IOSCO Principles - Central Securities Depository. Retrieved September 16, 2017, from https://www.csd.com.gh/market-info/iosco-principles.html

del Castillo, M. (2016). The DAO Attacked: Code Issue Leads to $60 Million Ether Theft - CoinDesk. Retrieved September 18, 2017, from https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/

Deloitte. (2016). The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services, (August).

Dermine, J. (2016). Digital Banking and Market Disruption: a Sense of Déjà Vu? Financial Stability Review - Banque de France, 20(April), 17–24.

Détienne, F., Rouet, J.-F., Burkhardt, J.-M., Deleuze-Dordron, C., Kumar, R., Khan, S. A., … Jabar, M. (2013). Risk Management Guide for Information Technology Systems : Recommendations of the National Institute of Standards and Technology. Journal of Systems and Software, 30(4), 1–22. https://doi.org/10.1111/j.1745-6622.2008.00202.x

ECB. (2016). 2016 Distributed Ledger Technology. Retrieved September 16, 2017, from https://www.ecb.europa.eu/pub/annual/special-features/2016/html/index.en.html

ECSDA. (2011). European Central Securities Depositories Association. Retrieved from http://www.fsb.org/wp-content/uploads/c_110909x.pdf

EMSA. (2016). The Distributed Ledger Technology Applied to Securities Markets. European Securties and Markets Authority. https://doi.org/10.1016/j.yexmp.2014.03.001

ENISA. (2016). Distributed Ledger Technology & Cybersecurity - Improving information security in the financial sector. https://doi.org/10.2824/80997

European Parlament. (2016). Distributed ledger technology and financial markets, (November).

Exchanges, W. F. of. (2016). Financial Market Infrastructures and Distributed Ledger Technology. World Federation of Exchanges, (August).

fca. (2017). DP17/3: Discussion Paper on distributed ledger technology. Retrieved from https://www.fca.org.uk/publication/discussion/dp17-03.pdf

FD. (2017). ECB vindt blockchain nog niet veilig genoeg | Het Financieele Dagblad. Retrieved September 16, 2017, from https://fd.nl/economie-politiek/1197187/ecb-vindt-blockchain-nog-niet-veilig-genoeg

From, A. R., Financial, T. H. E., & Regulatory, I. (2017). Distributed Ledger Technology : Implications of Blockchain for the Securities Industry 1, (January), 1–22.

Froystad, P., & Holm, J. (2015). Blockchain: Powering the Internet of Value. Evry Labs, 50.

Gartner. (2016). Gartner's 2016 Hype Cycle. Retrieved April 26, 2017, from http://www.gartner.com/newsroom/id/3412017

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the Security and Performance of Proof of Work Blockchains. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16, 3–16. https://doi.org/10.1145/2976749.2978341

Goodspeed, I. (2017). Financial market infrastructures. Retrieved July 17, 2017, from http://financialmarketsjournal.co.za/oldsite/18thedition/printedarticles/marketinfrastructures.html

Greenspan, G. (2015). MultiChain Private Blockchain — White Paper. Retrieved from https://www.multichain.com/download/MultiChain-White-Paper.pdf

Groenfeldt, T. (2017). 7 European Banks Form Blockchain Consortium For SMEs. Retrieved September 3, 2017, from https://www.forbes.com/sites/tomgroenfeldt/2017/06/28/7-european-banks-form-blockchain-consortium-for-smes/#1324784d3818

Guegan, D. (2017). Public Blockchain versus Private blockhain Centre d ' Economie de la Sorbonne Documents de Travail du Public Blockchain versus Private blockhain.

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. Financial Innovation, 2(1), 24. https://doi.org/10.1186/s40854-016-0034-9

Hardy, G., Heschl, J., & Clinch, J. (2008). Aliging COBIT, ITIL V3 and ISO/ICE 270002. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf

Hertig, A. (2017). Bitcoin Cash: Why It's Forking the Blockchain And What That Means - CoinDesk. Retrieved August 6, 2017, from https://www.coindesk.com/coindesk-explainer-bitcoin-cash-forking-blockchain/

Hogan, B. (n.d.). Three risks to assess as your company considers blockchain, 27.

Howard, L. (2016). Whitepaper On Distributed Ledger Technology, 98.

Hyperledger. (2017a). Hyperledger – Blockchain Technologies for Business. Retrieved April 26, 2017, from https://www.hyperledger.org/

Hyperledger. (2017b). Hyperledger Fabric 1.0 is Released. Retrieved August 29, 2017, from https://www.hyperledger.org/blog/2017/07/11/hyperledger-fabric-1-0-is-released

ISACA. (2017). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Retrieved from http://www.isaca.org/cobit/pages/default.aspx

ISO/IEC 27005. (2008). Information technology - security techniques - Information security risk management.

ITIL. (2013). ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls. Retrieved from https://www.iso.org/standard/54533.html

Kaivanto, K., & Prince, D. (2017). Risks and Transaction Costs of Distributed-Ledger Fintech: Boundary Effects and Consequences, 44(0), 1–12. Retrieved from http://arxiv.org/abs/1702.08478

Kakavand, H., & Kost De Sevres, N. (2016). The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies.

Karame, G., & Ghassan. (2016). On the Security and Scalability of Bitcoin's Blockchain. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16, 1861–1862. https://doi.org/10.1145/2976749.2976756

Kech, A., & Markets, S. (2016). Distributed Ledger Technologies What are Distributed Ledger Technologies How do they work.

KPMG. (2010). From Hype to Future. Retrieved from https://www.kpmg.com/ES/es/ActualidadyNovedades/ArticulosyPublicaciones/Documents/2010-Cloud-Computing-Survey.pdf

Lageschulte, P., Krajecki, M., Sokalski, M., & Nagaraj, K. (2016). Missing link - navigating the disruption risks of blockchain.

Lansiti, Marco; Lakhani, K. (2017). The Truth About Blockchain. Retrieved August 6, 2017, from https://hbr.org/2017/01/the-truth-about-blockchain

Li, W., & Sforzin, A. (2017). Towards Scalable and Private Industrial Blockchains, 9–14. https://doi.org/10.1145/3055518.3055531

Lindman, J., Tuunainen, V. K., & Rossi, M. (2017). Opportunities and Risks of Blockchain Technologies - {A} Research Agenda. Hicss, 1533–1542.

Maguire, Eamonn; Nagaraj, K. (2017). Securing the Blockchain | KPMG | US. Retrieved from https://home.kpmg.com/us/en/home/insights/2017/05/securing-the-blockchain-fs.html

Mainelli, M., & Smith, M. (2015). Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology). The Journal of Financial Perspectives, 3(3 Winter), 38–69. Retrieved from https://www.gfsi.ey.com/the-journal-x.php?pid=18&id=110

Manning, Mark; Sutton, Maxwell; Zhu, J. (2016). DISTRIBUTED LEDGER TECHNOLOGY: in securities clearing and settlement: Some issues - ProQuest. JASSA, 3, 30–36. Retrieved from https://search-proquest-com.vu-nl.idm.oclc.org/docview/1833242432?pq-origsite=gscholar

Mclean, B. S., & Deane-johns, S. (2016). Demystifying Blockchain and Distributed Ledger Technology – Hype or Hero ?, (April), 1–8.

Morabito, V. (2017). Business Innovation Through Blockchain. https://doi.org/10.1007/978-3-319-48478-5

Mougayar, W. (n.d.). The business blockchain : promise, practice, and application of the next Internet technology. Retrieved from https://books.google.nl/books?hl=nl&lr=&id=X8oXDAAAQBAJ&oi=fnd&pg=PR9&dq=Risks+blockchain+implementation&ots=jd0WzYVN1z&sig=97gwR4nrM-_wLAffTSBH6B4-3co#v=onepage&q=Risks blockchain implementation&f=false

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from www.bitcoin.org

NIST. (2016). NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations JOINT TASK FORCE TRANSFORMATION INITIATIVE. https://doi.org/10.6028/NIST.SP.800-53r4

on Payments, C., & Infrastructures, M. (2017). Committee on Payments and Market Infrastructures Distributed ledger technology in payment, clearing and settlement An analytical framework. Retrieved from https://www.bis.org/cpmi/publ/d157.pdf

Oost, Henize; Markenhof, A. (2010). Een onderzoek voorbereiden. Retrieved from https://www.managementboek.nl/boek/9789006978131/een-onderzoek-voorbereiden-heinze-oost

Overnance, C. D. I. G. (2017). DISTRIBUTED GOVERNANCE Carla L. Reyes, * Nizan Packin, ** and Benjamin P. Edwards ***, (forthcoming), 1–18.

OWASP. (2008). OWASP TESTING GUIDE. Retrieved from https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

Perez-Sola, Christina; Joancomarti, J. (2016). Privacy in Bitcoin Transactions: New Challenges from Blockchain Scalability Solutions, 4617, 318–329. https://doi.org/10.1007/978-3-540-73729-2

Peters, G. W., & Panayi, E. (2015). Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. arXiv Preprint arXiv:1511.05740, 1–33. https://doi.org/10.2139/ssrn.2692487

Pirrong, C. (2011). The Economics of Central Clearing : Theory and Practice. ISDA Discussion Papers Series, (May), 1–44.

Platt, C. (2016a). Blockchains as Financial Market Infrastructures (FMIs). Retrieved July 16, 2017, from https://medium.com/@colin_/blockchains-as-financial-market-infrastructures-fmis-8a6d02e13212

Platt, C. (2016b). Blockchains as Financial Market Infrastructures (FMIs).

Pohl, M., Freitag, S., & European Association for Banking History. (1994). Handbook on the history of European banks. E. Elgar.

R3CEV. (2016). Introducing R3 CordaPTMP: A Distributed Ledger Designed for Financial Services — R3. Retrieved April 26, 2017, from http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services

Rabobank. (n.d.). Over Rabobank - Rabobank. Retrieved from https://www.rabobank.nl/particulieren/over-rabobank

Rabobank. (2017). Seven banks plan blockchain platform to help European SMEs increase trade. Retrieved August 11, 2017, from https://www.rabobank.com/en/press/search/2017/20170116-banks-platform-dtc-blockchain.html

Reserve Bank of Australia. (2014). Sources and Management of Systemic Risk | Submission to the Financial System Inquiry – March 2014 | Financial Sector | Submissions | RBA. Retrieved July 16, 2017, from http://www.rba.gov.au/publications/submissions/financial-sector/financial-system-inquiry-2014-03/sources-and-management-of-systemic-risk.html

Rights, M. (2017). Broby , Daniel and Paul , Greig (2017) Blockchain and its use in financial settlements and transactions . The Journal of the Chartered Institute for Securities and Investment (Review of Financial Markets). ISSN 1357-7069 (In Press) , This version is, 7069.

Rizzo, P. (2017). ECB DLT Lead: Central Banks Won't Compete on Blockchain Tech - CoinDesk. Retrieved September 16, 2017, from https://www.coindesk.com/ecb-fintech-lead-central-banks-wont-compete-blockchain-tech/

Robeco: Jeroen van Oerle &, & Lemmens, P. (2016). Distributed ledger technology for the financial industry. Blockchain Administration 3.0, (May). Retrieved from https://www.robeco.com/images/201605-distributed-ledger-technology-for-the-financial-industry.pdf

Rosemann, M., & Bruin, T. (2005). Towards a Business Process Managment Maturity Model. ECIS 2005 Proceedings. Retrieved from http://aisel.aisnet.org/ecis2005/37

Rossi, M., & Sein, M. (2003). Design research workshop: a proactive research approach. Presentation Delivered at IRIS.

Saunders, A., & Cornett, M. M. (n.d.). Financial markets and institutions.

Seibold, S., & Samman, G. (2016). Consensus - Immutable agreement for the internet of value. Retrieved from https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf

Shrier, D., Iarossi, J., Sharma, D., & Pentland, A. (2016). Blockchain & Transactions, Markets and Marketplaces. Connection Science & Engineering Massachusetts Institute of Technology, (May), 19.

Spenkelink, H., & Hough, G. (2017). Blockchain: from hype to realistic expectations. Compact, 6. Retrieved from https://www.compact.nl/pdf/C-2016-4-Spenkelink.pdf

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). SP 800-30. Risk Management Guide for Information Technology Systems. Retrieved from http://dl.acm.org/citation.cfm?id=2206240

Swan, M. (2015). Blockchain: Blueprint for a new economy. Retrieved from https://books.google.nl/books?hl=nl&lr=&id=RHJmBgAAQBAJ&oi=fnd&pg=PR3&dq=financial+market+infrastructure+blockchain&ots=XQqAD1_Sk3&sig=Jzmhh9-5VQ7DlAINXVJsvUO5vKk

Tasca, P., Aste, T., Pelizzon, L., & Perony Editors, N. (n.d.). New Economic Windows Banking Beyond Banks and Money A Guide to Banking Services in the Twenty-First Century. Retrieved from http://download.springer.com.vu-nl.idm.oclc.org/static/pdf/116/bok%253A978-3-319-42448-4.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fbook%2F10.1007%2F978-3-319-42448-4&token2=exp=1492162659~acl=%2Fstatic%2Fpdf%2F116%2Fbok%25253A978-3-319-42448-4.pdf%3F

The Distributed Ledger Technology Applied to Securities Markets. (2016). Retrieved from https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf

Trautman, L. J. (2016). Is Disruptive Blockchain Technology the Future of Financial Services? Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2786186

Verschuren, P., & Hartog, R. (2005). Evaluation in Design-Oriented Research. Quality & Quantity, 39, 733–762. https://doi.org/10.1007/s11135-005-3150-6

Vom Brocke, J., Simons, A., Niehaves, B., Niehaves, B., & Reimer, K. (2009). Association for Information Systems AIS Electronic Library (AISeL) RECONSTRUCTING THE GIANT: ON THE IMPORTANCE OF RIGOUR IN DOCUMENTING THE LITERATURE SEARCH PROCESS. Retrieved from http://aisel.aisnet.org/ecis2009

Vukoli, M. (2017). Rethinking Permissioned Blockchains, 3–7. https://doi.org/10.1145/3055518.3055526

Walch, A. (n.d.). THE BITCOIN BLOCKCHAIN AS FINANCIAL MARKET INFRASTRUCTURE: A CONSIDERATION OF OPERATIONAL RISK. Retrieved from http://media.bizj.us/view/img/8744032/blockchain-technology-academic-research.pdf

Walch, A. (2015). The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk. Legislation and Public Policy, 18, 837–894. Retrieved from https://www.academia.edu/18602560/The_Bitcoin_Blockchain_as_Financial_Market_Infrastructure_A_Consideration_of_Operational_Risk

White, W. (1998). The coming transformation of continental european banking? Retrieved September 3, 2017, from http://www.bis.org/publ/work54.htm

Winter, R. (2008). Design science research in Europe. European Journal of Information Systems, 17(5), 470–475. https://doi.org/10.1057/ejis.2008.44

Winter, R., & Gericke. (2008). Design science research in Europe. European Journal of Information Systems, 17(5), 470–475. https://doi.org/10.1057/ejis.2008.44

World Economic Forum. (2017). Realizing the Potential of Blockchain | World Economic Forum. Retrieved from https://www.weforum.org/whitepapers/realizing-the-potential-of-blockchain

Xu, J. J. (2016). Are blockchains immune to all malicious attacks? Financial Innovation, 2(1), 25. https://doi.org/10.1186/s40854-016-0046-5

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on Blockchain technology? - A systematic review. PLoS ONE, 11(10), 1–27. https://doi.org/10.1371/journal.pone.0163477

Zheng, Z. (2016). Blockchain Challenges and Opportunities : A Survey Shaoan Xie Hong-Ning Dai Huaimin Wang, 1–24.

A DDoS Security Control Framework

Lars Drost

Lars Drost kick-started his IT career by obtaining a Bachelor degree in Business Informatics from Inholland University and a Master degree in Information Sciences at the VU University.

After finishing both degrees, Lars started working at Ernst & Young (EY) were he was part of EY's IT Risk and Assurance team. At EY Lars advised Financial Services Organisations about a large variety of IT Risk related topics. During his time at EY Lars graduated from the Executive Master IT Audit, Compliance & Advisory at the VU University and was seconded to the Dutch Central Bank (*De Nederlandsche bank, DNB*).

Lars currently holds the position of Security and Privacy Manager at Pon were he is responsible for the security and privacy programs of Pon's bicycle and heavy machinery businesses, which all in itself consist of a large number of legal entities.

1 Introduction

This document contains a summary of the master thesis “A DDoS Security Control Framework”. The research described in both the thesis and this summary was conducted a part of the Post graduate IT Audit degree of the Vrije Universiteit Amsterdam (VU). In addition to this introduction, this thesis summary sets out in short (i) the theoretical background of the research; (ii) the risks of DDoS; (iii) the DDoS Security Control Framework itself and (iv) the verification and validation of the Framework.

1.1 Problem definition

The internet hype which skyrocketed as of 1997 made companies and organizations eager to make use of all the opportunities internet had to offer them. The commercial use of the internet has dramatically changed the way organizations do business. There are e-businesses that solely focus on business on the internet and there are organizations that use the internet as one of their primary sales and/or service channels. By embracing the internet, organizations did not only take advance of the opportunities internet had to offer them, they also became dependent on the internet and their IT systems (Smits, 2011) and this dependence makes their business vulnerable for security threats such DDoS attacks.

The significant impact DDoS attacks may have on the continuity of their business makes it important for organizations to protect their network against such attacks. Especially since DDoS attacks are become more complex, larger in scale, cheaper and easier to buy (Goncharov, 2012) (Arbor Networks, 2013), more lucrative and far less risky than for example illegal drug trafficking which makes DDoS attacks attractive for criminals (Symantec, 2009). It no longer is a question whether a company will become a victim of a DDoS attack, but when it will become a victim of such an attack.

Even though the online survey conducted by Verisign (Verisign, 2012) that more than half of the respondents (53 percent) experienced web infrastructure downtime in the past year or which one third (33 percent) is accountable to DDoS attacks, a surprising 15 percent of the 76 percent of respondents with an e-commerce platform, reported having no DDoS solution in place, while 33 percent reported they have experienced three DDoS attacks in the past 12 months that lasted 7 hours on average.

Taking into account the high risk that an organization will become or will (again) be a target of a DDoS attack makes it essential for organizations to implement security controls and (counter) measures to defect and m minimize the impact of a DDoS attack as it can severely compromise the availability of their business and will lead to customer impact, employee productivity impact and revenue loss (Verisign, 2012).

1.2 Research Scope

The aim of the research was to develop a ‘building block’ which specifically focuses on DDoS which can be implemented in the existing IT control framework of organization. The DDoS Security Control Framework is based on the assumption that an IT control framework is already in place and that this IT control framework contains the fundamental organizational, procedural and technical controls based on a well-known and accepted framework, for example COBIT. Due to the aforementioned aim and assumption, the research and the security control framework itself only focus on DDoS measures and not on any other (cyber-)security related issues.

2 Theoretical background

2.1 The ISO Model

The Open System Interconnection Reference Model, or OSI model in short, forms the basis of the theoretical background section. This model was chosen because the OSI model is a commonly accepted standard, well-known and most referred to network model (Fitzgerald & Dennis, 2009), which made this thesis, and also this summary, easier to read since most people will be familiar with this model.

The model consists of seven different layers (Tanenbaum, 2002) (Blank, 2004) (Fitzgerald & Dennis, 2009):

1 Physical layer: This layer determines how bits of data that are send and received are moved along the network. Examples are Ethernet and FDDI.
2 Data Link layer: In this layer the data is prepared for delivery to the network. The layer consists of a LLC sublayer and a MAC sublayer. The LLC layer is the interface between the network layer protocols and the media access method such as a token or Ethernet. The MAC sublayer is in charge of the connection to the physical media such as the coaxial cabling. Examples are PPP and IEEE 802.5/802.2.
3 Network layer: Routing is performed by the network layer. In this layer it is determined to which computer the message should be send next to make it follow the best route possible through the network. Examples are IP and IPX.
4 Transport layer: The end-to-end issues are dealt with by the transport layer. Logical connections for the transport of data between the place of origin and the final destination are established, maintained and terminated by this layer. It controls the flow of data to ensure that no system is overflowing with data it receives. Examples of the transport layer are TCP and SPX.
5 Session layer: Managing and structuring all sessions is the responsibility of the session layer. Sessions can be the performance of a security check but also transferring files from one application to another. Examples of the session layer are SQL and RPC.
6 Presentation layer: The formatting of the data for presentation to the user is done by the presentation layer. The main task of this layer is to make sure that the data exchanged is exchanged in a form that is understood by the receiving system. Examples are JPEG and GIF.
7 Application layer: This layer provides network access to the end-user. Furthermore, this is the layer of the model in which the applications requests for and receives data. Examples are HTTP and FTP.

The basic principle to OSI layering is that each layer provides added-value to services provided by the layers below that particular layer. Based on this principle the highest layer constitutes the set of services which are needed for the distribution of applications (Saxena, 2014).

2.2 What is a DDoS attack?

A DDoS attack, also known by its full name 'distributed denial-of –service' attack, is a "large-scale, coordinated attack on the availability of services on a victim's system or network resources, launched indirectly through many compromised computers on the Internet" (EC-Council, 2010). An attack generally consists of four steps:

1 The DDoS attacker writes a virus that will send ping packets to a target network or a website;
2 Infect as many systems as possible and make them into so-called 'zombies'.
3 Launch the attack by waking up the zombie systems; and
4 The zombie systems attack the target website or network until it is disinfected (EC-Council, 2010) (McDowell, 2013).

2.3 Types of DDoS attacks

The basic idea behind a DDoS attack is to identify a weakness and create a mass-exploit in an effort to compromise the system. Per layer of the OSI model different types of DDoS attacks can be identified. The National Cybersecurity and Communications Integration Center of the U.S. Department of Homeland Security published a DDoS Quick Guide (National Cybersecurity and Communications Integration Center, 2014). The DDoS Quick Guide provides an overview of the types of DDoS attacks per OSI layer.

ISO Layer	Description of attack	Examples
Physical layer	Attacks on the physical layer are attacks that result in physical destruction, obstruction, manipulation or malfunction of physical assets	targeting wireless networks by jamming or interfering communication within these wireless networks
Data link layer	Attacks on the data link layer are attacks that disrupt the usual sender to receive the data flow.	MAC flooding
Network /transport layer	Attacks on the network and transport layer also known as network infrastructure attacks, are always attacks that contain an extremely high number of packets or data with the goal to consume bandwidth, slow down the web server and prevent users from getting access.	SYN flood, teardrop and ICMP flooding (Ping of death; Ping flood; Smurf)
Session layer	Attacks on the session layer exploit the logon and log off protocols.	Telnet attack
Presentation layer	Attacks on the presentation layer are malformed Secure Socket Layer (SSL) attacks. SSL provides security in web-services and nowadays most online transactions are protected by SSL. During a transaction there is a session of the network layer for SSL handshake after the TCP handshake is finished. During the SSL handshake messages are exchanged between both communicating entities to validate the authenticity. Several attacks make use of this SSL handshake to exhaust server resources	'Pushdo' botnet attack
Application layer	Attacks on the application layer concentrate around the protocols such as HTTP	HTTP Post attack; HTTP Get Flooding

2.4 Attacks on layer 3, 4 and 7

Almost all DDoS attacks initiated nowadays target either the network (network layer attacks), the network and transport layer (volumetric attacks) or the application layer (application layer attacks). The number of layer 7 attacks are increasing. This can be explained by the fact that layer 3/4 attacks are more easily detected and filtered, which makes the chance of success of layer 7 attacks much higher than the layer 3/4 attacks. Layer 7 attacks are more sophisticated and can be very effective from a protocol perspective and at low traffic rates. The attacks is often 'seen' as legitimate. Based on the aforementioned, the layers which are at risk the most are the network, transport and application layer. As a result the protective measures discussed in the next section of this summary and in the DDoS Security Control Framework will therefore focus on these three layers (Kostadinov, 2013).

3 The risks of DDoS

As a working assumption the following risk formula is used:

Risks = Threats x Vulnerabilities x Impact.

Definition of the vulnerabilities can be found in the description of the different types of attacks, while threat levels and impact can differ per organization. The resulting risks can be categorized in the following (most important) types of risks (i) operational risk; (ii) reputational risk; (iii) data integrity risk and (iv) fraud risk.

3.1 Operational risk

In almost all cases the goal of a DDoS attack is to make services unavailable. Depending on the type of services provided, DDoS attacks can have a (significant) impact on customers and employee productivity. Due to the DDoS attack, an organization is unable to provide its services, which can result in significant revenue losses when the services cannot be provided for a longer period of time or if the organization provides an essential service and, in case of a service level agreement, violates the service level agreement when the organization affected by the DDoS attack is the service provider under the agreement. (Verisign, 2012) (Federal Financial Institutions Examination Council, 2012)

3.2 Reputational risk

If organizations cannot provide their services, customers are impacted by that and their experience with the service with be affected negatively. When the organization is the target of multiple DDoS attacks, as we have seen with the large Dutch banks, customers will start ranking the services as unreliable and even rank the service below expectation. These negative experiences will negatively impact the brand and image of the organization and the reputation the organization has with its customers and within the market. (Verisign, 2012) (Federal Financial Institutions Examination Council, 2012)

3.3 Data integrity risk

As systems are highly connected and dependent on internal and external data, connection disruptions or delays in data processing will impact data integrity. If one application in the business (data) processing network is attacked, the applications are no longer capable of transferring data to the targeted application and the targeted application is no longer capable to transfer any data to any of the other applications within the business network. As a result the data is no longer accurate.

3.4 Fraud risk

Besides the above mentioned risks there is an actual risk that is often overlooked, but could impact a company severely. This risk occurs when a hacker uses a DDoS attack as a diversion to draw the attention from their actual goal. The DDoS attack could be coupled with a fraud attempt. In such cases organizations may also experience fraud losses, which might in turn result in liquidity and capital risks. For example DDoS attacks served as a diversionary tactic by criminals attempting to commit fraud using stolen customer or bank employee credentials to initiate fraudulent wire or automated clearinghouse transfers. (Federal Financial Institutions Examination Council, 2012)

3.5 Conclusion

To enable organizations to effectively use the DDoS Security Control Framework as set out in the next section of this summary, it is essential that an organization is familiar with the different threats, vulnerabilities and the impact which translates in a specific risk associated with the organization and the services it provides. Familiarity with the DDoS methods enables the organization to recognize the DDoS attacks and familiarity with the DDoS risks makes the organization aware of its weaknesses and the consequences associated with the risks. Together they enable an organization to mitigate the risks associated with DDoS attacks.

4 Establishing the framework

For organizations to become aware of the possible risks and to put effective measures in place, it is essential for entities to have a DDoS Security Control Framework in place.

4.1 Framework for Improving Critical Infrastructure Cybersecurity

The National Institute of Standards and Technology (NIST), a non-regulatory federal agency within the U.S. Department of Commerce, has introduced a Framework for Improving Critical Infrastructure Cybersecurity (the "NIST framework"). The NIST framework is designed to help owners and operators of critical infrastructures to manage cyber security-related risk (National Institute of Standards and Technology, 2014). The NIST framework consists of five main functions:

1 Identify: Develop the organizational understanding to manage cyber security risk to systems, assets, data, and capabilities.
2 Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
3 Detect: Develop and implement the appropriate activities to identify the occurrence of a cyber security event.
4 Respond: Develop and implement the appropriate activities to take action regarding a detected cyber security event.
5 Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event.

The NIST framework focuses on Cyber security-related risks, which makes it too broad to be used as a DDoS specific framework since DDoS is only a small piece of the Cyber security-related risks faced by entities. Furthermore, the NIST framework only focuses on the multiple approaches which are known today makes it static by nature. It does not take into account any future changes, it only provide information about the current situation an entity is in with regard to cyber security-related risks.

4.2 A dynamic framework

To improve the NIST framework and the processes it contains, the Deming Cycle also known as the PDCA Cycle, is a tool that can be used. The Deming Cycle is a continuous improvement model to improve the quality of processes, which consists of four repetitive steps (Deming, 2000):

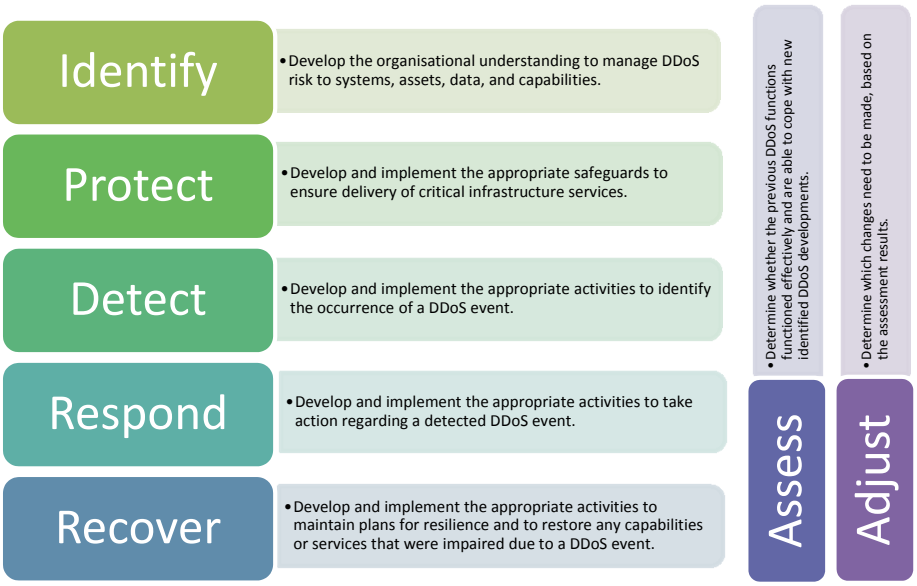
1 Plan: Design and revise business process components to improve results;
2 Do: implement the plan and measure its performance.
3 Check: study the results
4 Act: decide on the changes that need to be made to improve the process.

When apply the Deming Cycle to the NIST Framework the following division can be made:

Deming Cycle	NIST Framework
Plan	(Partially) covered by the 'Protect', 'Detect' and 'Respond' functions
Do	Partially covered by the 'Recovery' function, but due to the static nature of the framework this function only focuses on the situation to be restored to the old situation before the DDoS attack occurred. The element of studying the results of the detection, responses and recovery and making a decision on which changes to make is not included in the 'recover' function.
Check	Not covered
Act	Not covered

In order to make the NIST framework more dynamic and better fitting to the Deming Cycle, two new functions are introduced: 'Assess' and 'Adjust'. The new 'Assess' function of the NIST framework should focus on determining whether the detection of and the responses to the DDoS attacks are effective and whether the recovery of the system is good enough after the attack. The results collected during the 'Assess' function need to be used as part of the 'Adjust' function. Based on the results the organization needs to determine

which changes need to be made to either one of the other functions in order to improve its protection against, detection of, response to and recovery of a DDoS attack.
Taking into account the changes to the NIST framework as described above, the dynamic framework will look as follows:



By adding the principles of the Deming cycle to the existing model, the framework is more dynamic, but further steps need to be taken to make the framework more specific for DDoS.

4.3 A dynamic DDoS Security Control Framework

In paragraph 2.4 of this summary the most targeted OSI layers, namely the network, transport and application layer, and the risks associated with the DDoS attacks were identified. The three OSI-layers and the risks identified form the basis for determining which measures against DDoS attacks should be included in the framework.
The framework consists of three levels:

1 The function level: this level consists of all the function phases of the dynamic framework as described in paragraph 4.2;
2 The control type level: this level consists of the types of controls described below; and
3 The measures per type of control.

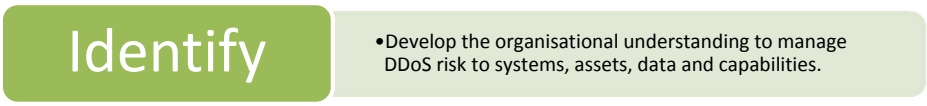
Although DDoS attacks can be linked to the different OSI layers, a framework that strongly focuses on these OSI layers would only cover technical infra components, which is too limited to establish a truly effective DDoS security control framework. Not only technical infra components, but also procedural components are important in the battle against DDoS attacks. As mitigating DDoS risks requires a combination of procedural and technical measures.

In order to keep the framework accessible and understandable for both technical and non-technical persons, the measures are not specified per OSI layer or risk, but per type of control. The framework contains the following types of controls:

- Physical controls e.g. fences, doors, locks and fire extinguishers;
- Procedural controls e.g. incident response processes, management oversight, security awareness and training;
- Technical controls e.g. user authentication (login) and logical access controls, antivirus software, firewalls;
- Legal and regulatory or compliance controls e.g. privacy laws, policies and clauses.

There are a number of measures that organizations can take in order to prevent DDoS attacks, to detect attacks when happening and respond to these attacks. The measures discussed in the research are adopted from existing researches and publications: (Govcert.nl, 2006) (IntruGuard, 2008) (Govcert.nl, 2010) (Nationaal Cyber Security Centrum, 2012) (Nationaal Cyber Security Centrum, 2012) (National Cybersecurity and Communications Integration Center, 2014) (National Institute of Standards and Technology, 2014) (Verisign, 2014) and if necessary, adjusted or expanded to make them suitable for the research and the specific topic the research covers.

4.3.1 'Identify' level



Relevance: To get familiar an organization needs to develop an overview of its network and its key appliances. Only if an organization has such an overview, it can effectively protect itself against DDoS attacks.
Goal: The goal of the measures at the 'Identify' level is to create a network scheme which contains all key appliances, data flows and bandwidth between these appliances that enables an organization to identify weaknesses within their network. Furthermore, it helps an organization to create awareness that availability and even integrity cannot be taken for granted and requires serious attention.

Measures: Possible measures are identified in more detail below.

Control Type	#	Measure
Procedural	I1.1	Physical devices and systems within the organization are inventoried.
	I1.2	Software platforms and applications within the organization are inventoried.
	I1.3	Organizational communication and data flows are mapped.
	I1.4	External information systems are catalogued.
	I1.5	Resources (e.g. hardware, devices, data and software) are prioritized based on their classification, criticality and business value.
	I1.6	Roles and responsibilities for the entire workforce and third-party stakeholders (e.g. suppliers, customers, partners) are established
	I1.7	Future Data Center Plans/Roadmap: What elements are you planning on changing? How will these affect the complexity of your data center and do they present any new risks? Adding new hardware or services comes with many known and unknown challenges.
	I1.8	Identify storage requirements to be able to maintain log data when under a

		DDoS attack.
	I1.9	Based on the gathered data a risk assessment is performed to identify the DDoS related risks within the IT environment with the use of the overall network schema. As part of this assessment organizations need to address their risk appetite, define weaknesses within their network and determine the assets that require protection.

4.3.2 'Protect' level

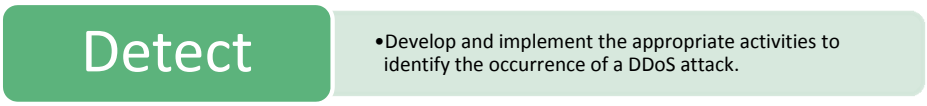
Relevance: The majority of attacks use well-known vulnerabilities, which organizations can easily protect itself against. It is best compared to a burglar who seizes an opportunity based on the likelihood that one target is easier to break in to than the other. So do what lies in your span of control to make hackers go for your neighbors' property in favor of yours.
Goal: implement pre-emptive measures to safeguard an organizations network.

Measures: Possible protective measures are identified in more detail below.

Control Type	#	Measure
Procedural	P1.1	Create baseline configuration of information technology/industrial control systems and maintain these baselines.
	P1.2	Validate that information technology/industrial control systems are setup according to their respective baseline.
	P1.3	DDoS response plans (Incident Response and Business Continuity) are in place and managed. These plans need to be defined scenario based These response plans need to be scenario based and specify which measures need to be taken to deal with the specified DDoS scenario. Furthermore, it needs to clearly specify who performs what, how and when and who has mandate to take certain decisions.
	P1.4	DDoS recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
	P1.5	The response and recovery plans are periodically tested (e.g. Bulk Volumetric Testing).
	P1.6	Agreements related to DDoS are in place with network providers to assist in blocking a DDoS attack.
	P1.7	DDoS communication plans are in place and managed. These communications plans need to cover public relations, authorities, legal and clearly specify who performs what, how and when.
	P1.8	Define (technical) measures according to the outcome of the risk assessment performed as part of measure I1.9 within the 'Identify' level.
Technical	P1.9	A SYN proxy is implemented to ensure that under SYN flood, all connection requests are screened and only those that are legitimate are forwarded.
	P1.10	Anomaly Recognition; by performing anomaly checks on headers, state and rate,

		an appliance can filter out most attack packets which otherwise would pass simple firewall rules.
	P1.11	Dark Address Prevention, IP addresses that are not yet assigned by IANA are blocked.
	P1.12	White-list and black-list are maintained. Within network, there will always be some IP addresses that you want to deny or allow. White-listing and Black-listing capability are useful during DDoS attack to ensure that such rules are honored despite rate violations or in spite of rate-violations.
	P1.13	Connection limiting; by giving preference to existing connections and limiting the new connection requests. By limiting the number of new connection requests, you can temporarily give the server respite.
	P1.14	Active verification; SYN Proxy combined with caching identified legitimate IP addresses in to a memory table for a limited period of time and then letting them go without the SYN proxy. Must be combined with rate limiting in case zombies are able to complete 3-way-handshakes to avoid misuse.
	P1.15	Implement anti-spoofing measures (e.g. unicast Reverse-Path Forwarding (uRPF), Bogon list, Access Control List (ACL)) to protect or at least reduce the likelihood of source IP spoofing taking place (EG, NTP, SNMP, DNS et cetera).
	P1.16	Firewalls are configured to apply certain filtering to monitor the traffic for certain protocols such as FTP and HTTP and examine whether the traffic meets the purpose of the RFCs.
	P1.17	Firewalls settings are configured which 'tell' the firewall what is normal behavior of a particular traffic flow such as a maximum number of connections from one specific IP-address.
	P1.18	Systems are hardened to improve the performance of the systems during a DDoS attack organization can configure a TCP/IP stack. To provide the performance the following configurations can be made: Expansion of the 'TCP window size'; Expansion of buffers for half open sockets and open sockets that wait for an 'accept' of the application; and Reduction of the time-out value of the TIME_WAIT status.
	P1.19	Implement adequate storage facilities to retain logging files when under attack to enable the opportunity to perform forensics.
	P1.20	Firewalls are configured as such that they monitor the maximum number of connections made from one IP-address

4.3.3 'Detect' level

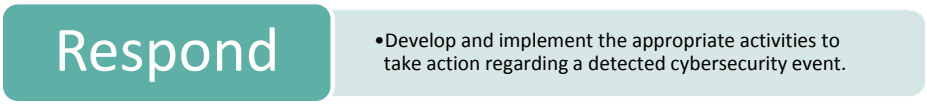


Relevance: it is important that an organization is able to detect a DDoS attack. To be able to pinpoint abnormal behavior when it occurs. If abnormal behavior is identified, it can be dealt with accordingly to prevent an attack of reaching its goal of disrupting a service.
Goal: implementing measures that enable an organization to identify an attack as soon as possible, which enables it to respond adequately to minimize the impact of the DDoS attack.

Measures: Possible detection measures are identified in more detail below.

Control Type	#	Measure
Procedural	D1.1	Detected events are analyzed to understand attack targets and methods
	D1.2	Detection processes are tested
	D1.3	Detection processes are continuously improved
	D1.4	Define the basic or standard behavior of the systems and network environment. The basic information is based on a number of data, such as: (i) the average number of visitors or users; (ii) the average package size of the data; (iii) the average memory space used; (iv) the average processor use; (v) the average broadband use of the internet connection and (vi) the average reading/writing actions on the hard drive. This information together is the overall average behavior and can be used as a basis for the detection of odd behavior such as DDoS attacks.
Technical	D1.5	An Intrusion Detection System (IDS) is in place which monitors whether the content of a network package meets certain requirements or standards and flags patterns that are plausible DDoS attacks.
	D1.6	An Intrusion Prevention System (IPS) is setup to block data traffic either by itself or by letting it apply certain rules in a firewall or router.
	D1.7	Flow-based accounting: netflow is an application that can be used in routers and is an addition to the process which determines the route of an IP package. For each IP package entering the router the hash value is calculated and then compared with the flow cache. If the package has the same hash value is detected in the flow cache the package is added to the statistics of that particular flow. Netflow can be a very effective weapon against DDoS attacks. If an organization transports the collected netflow data to a central storage, various application can interpret this data. There are even special applications which can monitor DDoS attack on the basis of the netflow data.
	D1.8	Granular Rate Limiting is a technique that identifies rate violations from past behavior.
	D1.9	Apply dynamic filtering, which is performed by identifying undisciplined behavior and punishing that behavior for a short time by creating a short-span filtering rule and removing that rule after that time-span
	D1.10	Source Rate Limiting; by identifying outlier IP addresses that break norms, you can deny them access to excessive bandwidth.
	D1.11	Within the 'protect' level numerous measures have been implemented that besides protection are able to provide organizations with information to detect DDoS attacks. Organizations need to implement monitoring measures to deal with this information accordingly.

4.3.4 'Respond' level



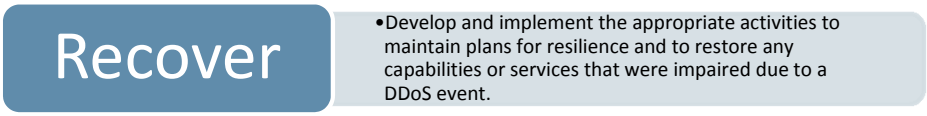
Relevance: it is important for an organization to have procedures and protocols in place on 'how to respond in case of a DDoS attack'.
Goal: to have protocols and procedures in place to specify who is in the lead, which persons have which authority, how to communicate and about what.

Measures: Possible measures are identified in more detail below.

Control Type	#	Measure
Procedural	R1.1	DDoS response plan is executed during or after an event
	R1.2	DDoS communication plan is executed during and after an event to address public relations with the press, customers, organization, authorities and legal obligations based on the DDoS communication plan.
	R1.3	DDoS response strategies are updated
	R1.4	DDoS response plans incorporate lessons learned
	R1.5	Notifications from detection systems are investigated
	R1.6	The impact of the incident is understood
	R1.7	Forensics are performed
	R1.8	Incidents are categorized consistent with the DDoS response plans
	R1.9	Incidents are contained
	R1.10	Incidents are mitigated
	R1.11	Newly identified vulnerabilities are mitigated or documented as accepted risks
Technical	R1.12	Quality-of-Service (QoS): QoS the data can be blocked, the bandwidth can be limited or the organization can decide to do nothing. Depending on the type of IP-addresses used for the attack, a decision needs to be made
	R1.13	Null-routing is in place and the potential DDoS attack IP addresses can be routed to the null interface
	R1.14	An ACL can enable an organization to block (or permit) certain source or destination IP-addresses and/or protocols to respond to an DDoS attack
	R1.15	Aggressive aging involves removing connections from the tables and may also involve sending a TCP RST packet to the server/firewall.
	R1.16	White-list and black-list are maintained. Within network, there will always be some IP addresses that you want to deny or allow. White-listing and Black-listing capability are useful during DDoS attack to ensure that such rules are honored despite rate violations or in spite of rate-violations.
	R1.17	Organizations can apply a so called 'DDoS wash street'. Internet traffic is redirected when a potential attack warrants traffic redirection. This technique is also called 'Off-Ramping'. The data is then received by the (third) party, where it is 'washed', as it goes through special purpose built appliances to filter illegitimate traffic out with the use of specific algorithms. Once the traffic is 'washed' it is rerouted back to the client, so called On-Ramping.

	R1.18	Specific DDoS appliances are available, which can be placed within the network that are able to deal with (more sophisticated) DDoS attacks.
	R1.19	Organizations are able to deflect sophisticated DDoS attacks by having multiple data centers at different Internet Exchanges, the organization can point the DNS entry of their websites to these companies who in return, handle all the requests where each packet is then inspected. Thereupon based on the signatures, illegitimate traffic can be detected and discarded. Next, legitimate traffic is sent back to end-users' browsers based on their geographical location.

4.3.5 'Recover' level

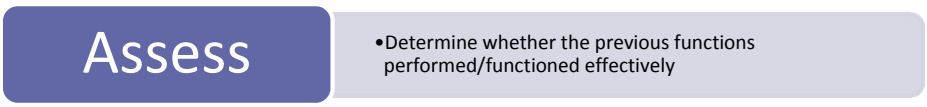


Relevance: it is of high importance for an organization to be able to restore capabilities or services, that were impaired by a DDoS attack, in a structured matter to be able to keep recovery time as minimal as possible and to get back to a 'business as usual' as soon as possible.
Goal: the goal of the recover level is to ensure that an organization is prepared to re-establish operations at an acceptable level to limit the downtime of a disruption and to resume operations in a phased approach.

Measures: Possible recover measures are identified in more detail below.

Control Type	#	Measure
Procedural	R2.1	DDoS recovery plan is executed during or after an event.
	R2.2	DDoS recovery strategies are updated.
	R2.3	DDoS recovery plans incorporate lessons learned.
	R2.4	Public relations with the press, customers, organization, authorities and legal obligations are managed based on the DDoS communication plan.
	R2.5	Reputation after an event is repaired.
	R2.6	Recovery activities are communicated to internal stakeholders and executive and management teams.

4.3.6 'Assess' level

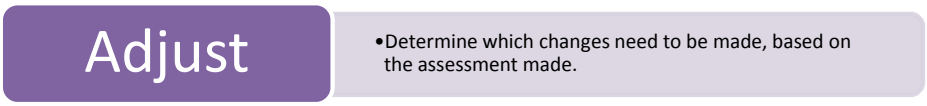


Relevance: it is of great importance that the framework is able to cope with these changes by being able to assess the impact of changes in the field of DDoS in relation to the implemented framework. Only, when an organization is able to assess the impact of these change it is able to cope with it and adjust the framework accordingly
Goal: the goal of the assess level is to evaluate the previous steps taken in order to identify the focus areas where measures will need to be implemented.

Measures: to enable an organization to assess the effectiveness of implemented measures, a process needs to be in place to gather information at each level. The gathered data is then evaluated and actions are taken.

Control Type	#	Measure
Procedural	A1.1	Execute monitoring procedures
	A1.2	Review and measure effectiveness of current DDoS controls
	A1.3	Conduct Internal DDoS Audits
	A1.4	A Security Team monitors DDoS trends and validates whether the current control framework is able to cope with these trends or developments
	A1.5	Undertake management review
	A1.6	Record actions and events that impact DDoS controls

4.3.7 'Adjust' level



Relevance: by analyzing the findings and actions needed an organization will need to update the control framework in order to prevent recurrence of attacks at the identified weaknesses. At the adjustment level the initiation of the continuous improvement cycle is activated and the lessons learned can be used as a reference for future analysis

Goal: the goal of the adjust level is to provide an organization with a tool to effectively define a corrective action plan that not only enables improvement of the current measures implemented but also creates a basis for continuous improvement.

Measures: The following measures can enable an organization to achieve this.

Control Type	#	Measure
Procedural	A2.1	The DDoS Security Control Framework is updated
	A2.2	Preventive processes are continuously improved
	A2.3	Detection processes are continuously improved
	A2.4	Respond processes are continuously improved
	A2.5	Communicate actions and improvements

4.4 How does the DDoS Security Control Framework cover the identified risks

There is no universal approach that can cover all DDoS security risks, as the risks will differ between organizations and different attacks may be used. In order to set up effective measures to fight off a DDoS attack, it is also essential to understand the various DDoS methods and to effectively battle DDoS attacks, it is key for organization to implement technical measures that not only prevent or minimize risks on either OSI Layer 3, 4 or 7, but prevent or minimize risks on all of these layers. This is why the DDoS Security Control Framework covers these three layers, as shown in the mapping below.

	Protect	Detect	Respond
OSI Layer 3	P1.10, P1.11, P1.12, P1.13, P1.14, P1.15, P1.16, P1.17, P1.18, P1.19, P1.20	D1.5, D1.6, D1.7, D1.8, D1.10, D1.11	R1.12, R1.13, R1.14, R1.16, R1.17, R1.18
OSI Layer 4	P1.9, P1.10, P1.11, P1.12, P1.13, P1.15, P1.18, P1.19	D1.5, D1.6, D1.7, D1.8, D1.9, D1.10, D1.11	R1.13, R1.15, R1.16, R1.17, R1.18
OSI Layer 7	P1.11, P1.12, P1.13, P1.14, P1.19	D1.5, D1.6, D1.11	R1.16, R1.18, R1.19

Besides the technical measures, organization also need to implement procedural measures at the protect, detect and respond level. The aim of these procedural measures is to trigger actions and to create awareness. The combination of both types of measures is key for creating an effective functioning DDoS mitigation environment.
Taking away every vulnerability is a utopia. This makes it important for organizations that they have the ability to recover and by introducing a continuous improvement cycle as part of the framework, organizations can start implementing controls which mitigate the most important risks identified, while strengthening the control set with each cycle to reduce the level of vulnerabilities in the network and as a result minimize the risks related to an attack.

4.5 How to apply the DDoS Security Control Framework

All the previous steps have now resulted in a dynamic DDoS Security Control Framework. But before organizations can start to implement or use this framework in any way, they need to come up with a plan. Simply implementing this framework will not provide them with the DDoS security control environment they are aiming for. Every organization is different in many ways. These differences needs to be taken into account when using the framework. Organizations need to adopt a so-called risk based approach when using this framework. This means that they have to ask themselves questions such as: “how much risk are we willing to take?”, “what are the risks associated with the services we provide?” and “what are the weaknesses of our network?”. Based on the answers to these questions organization can use (parts of) the framework to setup or improve their DDoS security control environment accordingly.
Furthermore, the framework contains multi-disciplinary elements. Some elements are technical, others are more risk focused. Therefore it is recommended that the framework is applied by a multi-disciplinary team which preferably consists of IT Security Experts, IT Risk and management to cover the whole spectrum and have sufficient knowledge within the team to apply the framework correctly.

5 Verification and Validation of the DDoS Security Control Framework

Please note that the validation, as set out below, is limited and purely based on the experience of subject matter experts.

5.1 Verification and validation definition

The terms verification and validation originate from software project management, software testing and software engineering. Verification and validation entails the process of checking that a software system meets requirements and fulfils its intended purpose. In other words, verification and validation are methods to control the quality of the system.

5.2 Approach

To verify and validate the framework interview sessions were organized with subject matter experts. The subject matter experts that were involved in the verification and validation process were clearly instructed that the framework should be interpreted as a 'building block' and to function properly an 'effective' IT control framework needs to be in place. This framework needs to contain the fundamental organizational, procedural and technical controls based on a well-known and accepted framework such as COBIT.

Based on the results of the interviews with the subject matter expert, it was concluded that the established framework contains the relevant elements and measures and forms a valuable basis for organizations to establish or improve their security to mitigate identified risks related to DDoS, but that some improvements could be made to make the framework even more effective. These improvement mostly related to reorganizing some measures in the framework and adding some additional information or measures.

6 Research Conclusion

This research discussed the nature of a DDoS attack and has shown that, due to the quickly growing impact and likelihood of DDoS attacks, it is very important for organizations to give proper consideration to this trend. Furthermore, the impact and risks associated with DDoS attacks and the measures that can be implemented to minimize these risks were been identified in this research. The information gathered regarding types of attacks, risks associated with DDoS attacks, and possible measures has been incorporated and taken into account when structuring the DDoS Security Control Framework in order to make the framework as dynamic and as useful as possible. The result is the DDoS Security Control Framework as set out in this Summary, and in more detail in the thesis. This control framework can enable organizations to manage the risks related to DDoS attacks and, as a result, improve its security.

7 Bibliography

Aalst, M. L. (2015). PM 2: A Process Mining Methodology. *Advanced Information Systems Engineering - 27th International Conference* (pp. 297--313). Stockholm, Sweden: Springer.

Aalst, W. M. (2016). Process Mining - Data Science in Action, Second Edition. Springer.

Arbor Networks. (2013). *Understanding DDoS*. Retrieved December 8, 2014, from Digital Attack Map: http://www.digitalattackmap.com/understanding-ddos/

Arbor Networks. (2014). *Largest DDoS Attack Reported.* Burlington: Arbor Networks.

Blank, A. (2004). *TCP/IP Foundations.* Alameda: SYBEX Inc.

Deming, W. E. (2000). *Out of the Crisis.* Cambridge: MIT Press Ltd.

EC-Council. (2010). *Ethical Hacking and Countermeasures: Treats and Defense Mechanisms.* Clifton Park: Cengage Learning.

Federal Financial Institutions Examination Council. (2012). *Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources.* Arlington: Federal Financial Institutions Examination Council (FFIEC).

Fitzgerald, J., & Dennis, A. (2009). *Business Data Communications and Networking.* Hoboken: John Wiley & Sons.

Goncharov, M. (2012). *Russian Underground 101.* Cupertino: Trend Micro Inc.

Govcert.nl. (2006). *Aanbevelingen ter bescherming tegen Denial-of-Service aanvallen.* Den Haag: Govcert.nl.

Govcert.nl. (2010). *Whitepaper Raamwerk Beveiliging Webapplicaties.* Den Haag: govcert.nl.

IntruGuard. (2008, November 10). *10 DDoS Mitigation Techniques.* Retrieved February 2, 2015, from www.slideshare.net: http://www.slideshare.net/intruguard/10-ddos-mitigation-techniques-presentation

Kostadinov, D. (2013, October 24). *Layer Seven DDoS Attacks*. Retrieved January 10, 2015, from InfoSec Institute: http://resources.infosecinstitute.com/layer-seven-ddos-attacks/

McDowell, M. (2013, February 6). *Understanding Denial-of-Service Attacks*. Retrieved December 7, 2014, from United States - Computer Emergency Readiness Team (US-CERT): http://www.us-cert.gov/ncas/tips/ST04-015

Nationaal Cyber Security Centrum. (2012). *ICT-Beveiligingsrichtlijnen voor webapplicaties - Deel 1.* Den Haag: Nationaal Cyber Security Centrum.

Nationaal Cyber Security Centrum. (2012). *ICT-Beveiligingsrichtlijnen voor webapplicaties - Deel 2.* Den Haag: Nationaal Cyber Security Centrum.

National Cybersecurity and Communications Integration Center. (2014). *DDoS Quick Guide.* Arlington: National Cybersecurity and Communications Integration Center.

National Institute of Standards and Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Gaithersburg: National Institute of Standards and Technology.

Prolexic. (2013). *Quarterly Global DDoS Attack Report Q3 2013.* Hollywood: Prolexic.

Prolexic. (2014). *Quarterly Global DDoS Attack Report Q1 2014.* Hollywood: Prolexic.

Saxena, P. (2014). OSI Reference Model – A Seven Layered Architecture of OSI Model. *International Journal of Research (IJR), 1*(10), 1145-1156.

Smits, M. S. (2011). *Hoe het internet de Nederlandse economie verandert.* Amsterdam: The Boston Consulting Group.

Symantec. (2009, September 10). *News room - press releases*. Retrieved September 4, 2014, from Symantec: http://www.symantec.com/about/news/release/article.jsp?prid=20090910_01

Tanenbaum, A. S. (2002). *Computer Networks.* Upper Sadle River: Prentice Hall PTR.

Verisign. (2012). *Distributed Denial of Service (DDoS): finally getting the attention it deserves.* Reston: Verisign Public.

Verisign. (2014). *DDoS Protection Services Overview.* Reston: Verisign Public.

Proces Mining & Process Risk Mining

Paul Kromhout
Elham Ramezani Taghiabadi
Marijn Nagelkerke
Can Hariri
Stefan Zuiderwijk

				
Paul Kromhout	Elham Ramezani Taghiabadi	Cas Hariri	Marijn Nagelkerke	Stefan Zuiderwijk
The auteurs work for KPMG in the Netherlands				

1 Introduction

Process mining automatically describes your business process directly from data. It gives an X-ray view of business processes and helps you to understand what actually is happening. It provides factual diagnostics for detecting bottlenecks and improving your operation.
Process mining is a growing discipline which leverages from omnipresence of data for fact-driven analysis of processes. Process mining allows organizations to diagnose process bottlenecks and vulnerabilities based on the reality rather than assumptions about the reality.
The purpose of companies and organizations is in most cases to eventually create value that satisfies their stakeholders. If companies or organizations are not able to create value in a reasonable time, then they will not stay in business for long. Business processes are a cornerstone of this value creation process.
A sustainable growth of companies and organizations will require periodic changes or enhancements in their processes and continuous monitoring of their performance. However, this is easier said than done. Firstly, is hard to near impossible to measure the total impact of these changes and enhancements. As with any organization of reasonable size there are unforeseen interdependencies between people and processes making it impossible to selectively target one aspect for change without deep knowledge over the processes.
Secondly, to correctly judge if a change has led to the desired enhancement one needs to rule out any external factor, such as seasonal effects, which might have influenced the outcome. One way to measure the effect would be to have two exactly the same organizations under the same conditions, where only one would implement the change. That way, the difference inferred can only be attributed to the adjustments. This method is practically often not possible.
Sometimes improvement projects do not deliver meaningful improvements to companies and no matter how close a company monitors its key performance indicators (KPIs). Often, when defining an improvement project, the leadership team will meet, put together their ideas for an improvement initiative, and then kick off the initiative. Accordingly, KPIs are defined and monitored. However, many companies put the emphasis on poorly selected improvement indicators. Consequently, when changes are made, the results achieved are disappointing or not as satisfying as expected. So if this is not the right way, then what should companies do?
In this article, we explain how we can use process mining to answer the above mentioned question. First, we would like to give an overview of different types of analysis and their application that can be applied using process mining technology. We briefly discuss different process mining techniques and focus on two domains process mining could be leveraged. For each domain, we show a case from an engagement where we used process mining. Next, we will discuss a methodology to conduct a process mining project. Finally, we conclude by discussing some lessons learned and success factors in a process mining project.

2 What is Process Mining?

Process mining provides new ways to utilize the abundance of information about events that occurs in the world surrounding us. These events such as ‘open door’, ‘approve loan’, or ‘create order’ can be collected from the underlying information systems supporting a business process or sensors of a machine that performs an operation or combined. We refer to these as ‘event data’. These event data enable new forms of analysis facilitating process improvement and process compliance. Process mining provides a novel set of tools to discover the real process, to detect deviations from desired process, and to analyse bottlenecks and waste. Process mining is generic and can be leveraged to improve processes in a variety of application domains. It can be applied for various processes such as purchase-to-pay, order-to-cash, hire-to-retire, and IT management processes. It can be leveraged in any industry sector and has already been applied in many sectors, such as banking, consumer products, healthcare, insurance, professional services, public sector, and logistic services.

Process mining bridges the gap between traditional process analysis (e.g., simulation and other business process management techniques such as lean management and six sigma) and data-centric analysis techniques such as machine learning and data mining.
An input for all of process mining techniques is event data which records the information about the executions of business processes. Process mining techniques can be categorized under four main activities:

1 Process discovery
2 Conformance checking
3 Enhancement and
4 Process analytics.

Process Discovery

Process discovery used logged event data on executions of business processes (event data) and produces a model reflecting the actual behaviour recorded in the logged data without using any information about the process. The model reflecting the actual process is a descriptive model, not to be used to steer and control the actual process, but rather to aim in capturing reality.

case id	event id	properties				
		timestamp	activity	resource	cost	...
1	35654423	30-12-2010:11.02	register request	Pete	50	...
	35654424	31-12-2010:10.06	examine thoroughly	Sue	400	...
	35654425	05-01-2011:15.12	check ticket	Mike	100	...
	35654426	06-01-2011:11.18	decide	Sara	200	...
	35654427	07-01-2011:14.24	reject request	Pete	200	...
2	35654483	30-12-2010:11.32	register request	Mike	50	...
	35654485	30-12-2010:12.12	check ticket	Mike	100	...
	35654487	30-12-2010:14.16	examine casually	Pete	400	...
	35654488	05-01-2011:11.22	decide	Sara	200	...
	35654489	08-01-2011:12.05	pay compensation	Ellen	200	...

Figure 1: Typical event data used for process discovery (Aalst W., 2016).

Event data usually contains a unique identifier (called case ID). The case ID is selected according to the perspective of an analysis. Examples of case IDs are: an order umber, a customer number, a ticket ID, a patient number, etc. In addition, event data should contain the recorded execution of activities and their timestamp. Case ID, activity name and timestamp are considered to be the minimum requirements for process discovery. When an IT system has this information not available, process mining is less feasible.

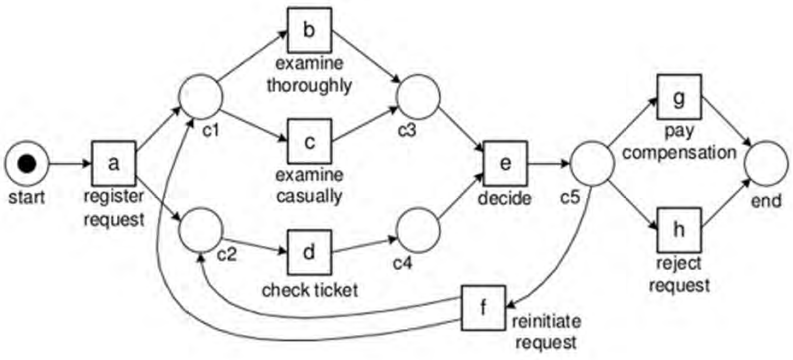


Figure 2: The process as mined from the previous figure event data (Aalst W., 2016).

Using solely this data it is possible to generate a model using process mining software ([as described below]…). Internally these software packages will use algorithms such as the "α-algorithm" to generate the above "Petri Net", which is very much human interpretable and useful for creating valuable insights on the internal processes of companies. This information can also be augmented to enable the analytics of runtimes and to discover bottlenecks in the processes.

Also, event data can contain additional information such as the person who executed an activity or quantity of an order, or the age of a patient. Adding additional information allows for deeper and more precise analysis of a process, such as describing how different resources in a process interact with each other.

Conformance Checking
By using conformance checking, the actual process (which can be based on a model obtained via process discovery) can be compared with event data and used to show deviations or alternative process paths.

Process Enhancement
Process enhancement includes extending or improving an existing process model using information about the actual process recorded in event data. For example, by extending a process model with performance information related to time or cost, or repairing the process model according to current executions shown by the corresponding event data.

Process Analytics
In addition to the above three process mining activities, other analysis techniques can be applied in the context of event data and process models, such as data mining techniques or visual analytics (e.g. histograms of events per case), of which the results can be used to understand process models with additional aspects, predict future (e.g., the remaining flow time and probability of success) and recommending suitable actions.

3 Breakthroughs for Process Mining

The corner stone of process mining is the mathematical modeling language Petri-Nets, or place/transition (PT) nets. This modeling language has been developed in 1939 by Carl Adam Petri. The concept was invented by the German mathematician for the purpose of modeling chemical processes. As these nets have a mathematical foundation, their behavior can be unambiguously specified and analyzed. This is in contrast to contemporary modeling languages such as Business Process Models (BPM).
Another important invention for process mining is the relational database management system (RDBMS). These systems allow for electronical storage of information. Implementations of RDBMS are MariaDB, Microsoft SQL Server and Oracle Database. The RDBMS signaled the transition from binary storage of data to relations expressed in row/column format. This structured data-storage allowed for various manipulation and query operators. A well-known language in this context is the Structured Query Language (SQL). As result of the adaptation of RDBMS, data became easier to store, gather and analyze. Hereby a higher quantity per entity was possible and higher inter-system-compatibility allowed for better analysis and development opportunities for the field of process mining.
Process mining concerns itself with the generation of petri-nets from event data which has been stored in these RDBMS. Various efforts has been executed in the past for doing so, such as the Viterbi Algorithm for finding Hidden Markov Models (HMM) from observed events. Technically the challenge is to create a model which describes all possible actions which can occur (what can happen) and the specific order in which they can happen (how can it happen). This is likened to learning the grammar of a formal language from the

event-log of a process. The petri-net generated on basis of the event-log is similarly able to recognize events from this event log, corresponding to how a finite state machine (type-3 in the Chomsky Hierarchy) can recognize words from a formal language. The Technical University of Eindhoven (TU/e) and its personnel (such as professor Wil van der Aalst and Boudewijn van Dongen), played a crucial role in developing both the theoretical and practical foundations for the process mining we known today.

4 Theoretical foundation of process-mining

As elaborated in previous chapters petri-nets form the corner-stone of process-mining. In this chapter we will give the reader a brief overview of how these petri-nets work, and how such petri-nets can be generated from an event-log.

4.1 Petri-Nets

We start with an example of a petri-net, hereby showing the different elements of which they are made of:

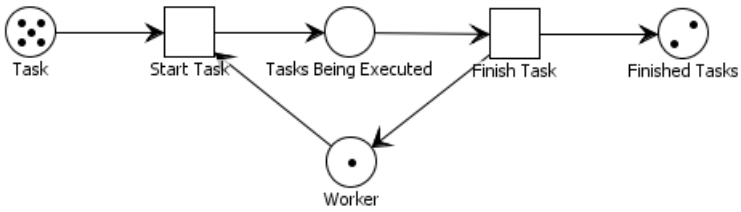


Figure 2: A simple petri-net

Classic petri-nets have three different types of elements: transitions, places, arcs and tokens. These are represented as boxes, circles, arrows and dots respectively. In fig. 3 we see an example of such net, describing a basic production process with only one worker. Actions in this network are performed by the transitions: for every incoming arcs one token is consumed, while every outgoing arrow produces a token. The places simple hold these tokens. Transitions can only function if on all the connected places from which an arc leads to the transition at least 1 token exists.

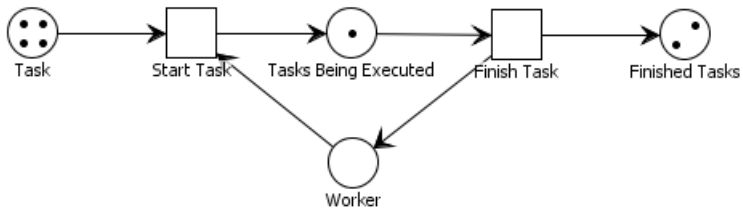


Figure 3: The state of the petri-net after executing "Start Task"

During the first-time step thus one token from both “Worker” and “Task” (two in total) have been consumed by the “Start Task” transition. The result is shown in figure 4: one token which is created in the “Tasks Being Executed” place. Please note that in this state it is impossible to perform “Start Task” a second time: although there are more than 1 tokens in the “Task” place, it also requires at least one token in the “Worker” place which is currently not present.
The only action in this state is thus to execute the “Finish Task” transition, hereby placing one token back in the “Worker” place and creating an additional token in the “Finished Tasks” place. As there are both tokens in the “Worker” and “Task” places another “Start Task” can be executed, and the cycle repeats until all tokens are consumed from “Task”.

4.2 Process Mining

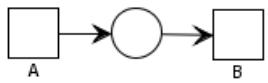
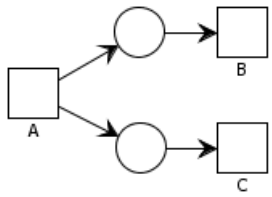
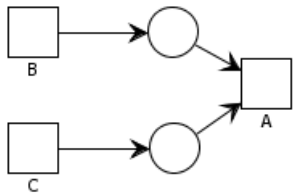
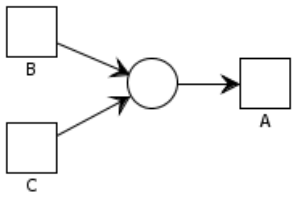
Process Mining is performed when we want to create a petri-net from a given event-log. Although there are many methods which have been invented over time, each with its own benefit and drawbacks, we will focus ourselves on the Alpha Algorithm as it is one of the most intuitive ones. Consider the following event-log, where the one letter events indicate a specific process being performed:

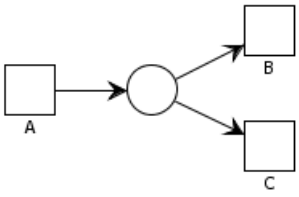
Time Stamp	Session	Event
1	1	A
2	1	B
3	2	A
4	1	C
5	1	D
6	2	C
7	2	B
8	2	D

When isolating the traces from the event log we can thus identify the following two cases:

- ABCD for session 1
- ACBD for session 2

The Alpha Algorithm describes then five different building blocks to generate a petri-net from this event data:

Type	Petri-Net	Conditions
1		A followed by B and not B followed by A
2		A followed by B and not B followed by A A followed by C and not C followed by A C followed by B and B followed by C
3		B followed by A and not A followed by B C followed by A and not A followed by C C followed by B and B followed by C
4		B followed by A and not A followed by B C followed by A and not A followed by C C not followed by B and B not followed by C

5		A followed by B and not B followed by A A followed by C and not C followed by A C not followed by B and B not followed by C

For our event log only types 2 and 3 are relevant, leading to the following model:

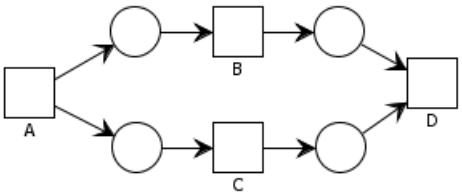


Figure 4: The model mined from our artificial event log

While the Alpha Algorithm is easy to understand it is not often used in real world scenario's due to various inefficiencies such as its inability to deal with noise in the event logs. These can be introduced for when example when by accident a process is executed which is not really part of the workflow.

5 Applications of Process Mining

Process mining can be applied for both process improvement projects and audit engagements.
A business process is a chain of activities that are connected to each other to fulfil a goal. There is often a significant gap between the officially documented process flow and what actually happens in those processes. Using process mining, we can document and visualize the actual process execution, and can detect inefficiencies and bottlenecks. After detecting improvement area's and prioritizing them, improvement initiatives can be taken. Process mining can be used to perform a fact-driven analysis of process and select improvement areas.
Process mining can be used in a continuous manner. After resolving one bottleneck, the focus shifts to the next inefficiency to resolving it. As the processes within companies continuously evolve due to both internal as external factors, process mining should not be seen as a one-time project, rather a continuous process improvement technique to keep up with the daily reality Therefore, we encourage a sustainable approach in which an expert team in-house continuously monitors processes and improves them in a gradual pace.

6 Process Mining integrated in the (Financial) Audit

Process mining can also be used during different stages of a financial audit:
1 during walkthroughs
2 used as a basis for sampling, or
3 used for compliance checking.

Process mining used during walkthroughs.
Going through time consuming interviews and meetings with clients to understand their processes? There is a better way! One of the first steps in any audit engagement, is the understanding client's business processes via walkthroughs. However, this approach is not very efficient for giving a comprehensive picture on how processes are actually executed. In addition, one cannot be sure whether the picture is complete. Often,

different departments at the client have knowledge about only parts of the process that go through their department and auditors need to contact different people to get a relatively complete understanding of the whole process. Furthermore, during walkthroughs, usually only very typical ways of performing a process are discussed and in many cases exceptions are not discussed. Using process mining, this step can be shortened and the quality of walkthroughs can be improved drastically. Using process mining, an auditor can see the overview of business processes executed in reality together with all the details and possible exceptions.
Furthermore, as process mining gives you an elaborate and automated way of discovering the processes, it is possible to re-run the execution of a process from beginning to end (so called traces). This is very useful to highlight traces which conform to the discovered process, and outliers, traces where different paths and processes are used or outlying run-times are detected.

Process mining used for sampling.
The discovered process model during walkthrough can be used for better and smarter sampling. That is, cases that have higher operational risk can be detected and used for further analysis.

Process mining used for compliance checking.
Using process mining, in particular conformance checking, the deviations from a desired process path or a compliance rule can be detected. The whole population of historic data can be checked instead of limited analysis done on sample data (100% sample data). See also 'Process Risk Mining'.

Process Risk Mining
Process mining cannot only be used to identify process performance opportunities, but also for the risks that might pop-up in processes. We identify two types of process risk analysis in which process mining can be a big help. First all the actors which are involved are easily identifiably using process mining. Actors performing multiple (critical) activities in a process, or related processes, can be easily identified. If no other actors perform critical activities in the same transactional process flow, this might result in an unmitigated risk (an unmitigated breach in the segregation of duties).

An example of such a segregation of duties conflict is a breach in the invoice payment process. When an actor both posts and pays an invoice, without other mitigating controls or other critical activities, this can result as an uncontrolled outgoing payment.

However, when the invoice is approved using an approval workflow, the risk is assumed as mitigated. The approval workflow in which a second (and even third) actor has to approve and release the invoice for payment, will further strengthen the assumption that the breached segregation of duties has been mitigated.

Secondly, process mining can help identify exceptions - in the bulk of transactions - that escape the implemented (application) controls. In the abovementioned example, blocking an invoice after posting is a control that helps mitigating the breaching of the segregation of duties. The control is that the invoice is blocked and can only be released by a second (or third) actor. With process mining the cases in which these second (or third) actors are bypassed can be identified.

Process mining can help identify process risks and see the effectiveness of both the implemented authorizations (segregation of duties) as well as implemented application controls. Analysing the process flow on transactional level can help to build an effective control framework, and afterwards, show the effectiveness of the implemented controls.

Use Case: Analysis of change management process as part of general IT controls (GITCs)

This use case describes the use of process mining as part of a financial statement audit of an international corporate client. For this audit the auditor verified the system transportation process of one of the SAP systems used. Usually, when a change in a system is requested, a change ticket is issued. If the change request is approved to be developed, it triggers a transportation process. During the transportation process, a change to the system will be prepared in the development environment, then the transport will be imported to the quality environment. Finally if the transport passes all required checks, it will be promoted to the production system.

One of the change logs that the auditor analysed contained about 577 transports. Several activities have been performed for each of these transports. Figure 8 shows the difference between the number of activities that were executed for different transports. Some transports were processed with only few number of activities, and for some more than 3000 events were logged (each event represent an execution of an activity). The question that was raised was why certain transports include so many events and some not. The auditor further analysed these occurrences and noted for example that several changes have been transported to multiple target systems and consequently some events are duplicated for those transports.

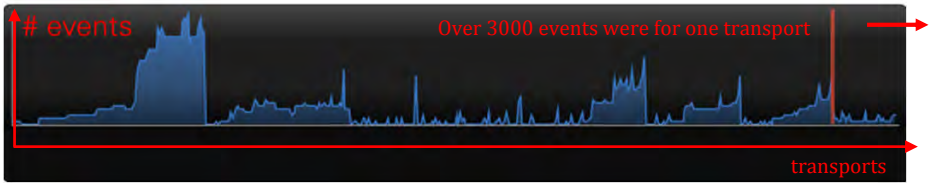


Figure 8: Number of events recorded for each transport.

Figure below shows the complete process model discovered for these 577 transports.

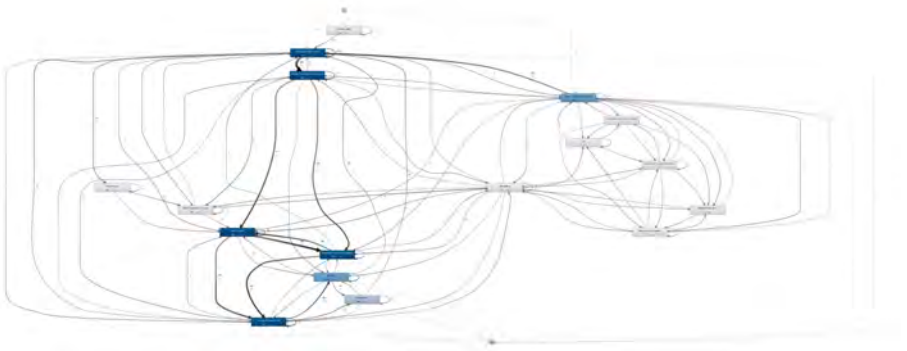


Figure 9: The complete process model discovered from the process followed by 577 transports.

As is shown in Figure 9, the discovered process model is rather complex and reveals a so called 'spaghetti model' which is difficult to understand. The auditor noted that various proces flows have been followed, based on the source system of the transports. In this use case we highlight the process flows of two of these source systems.

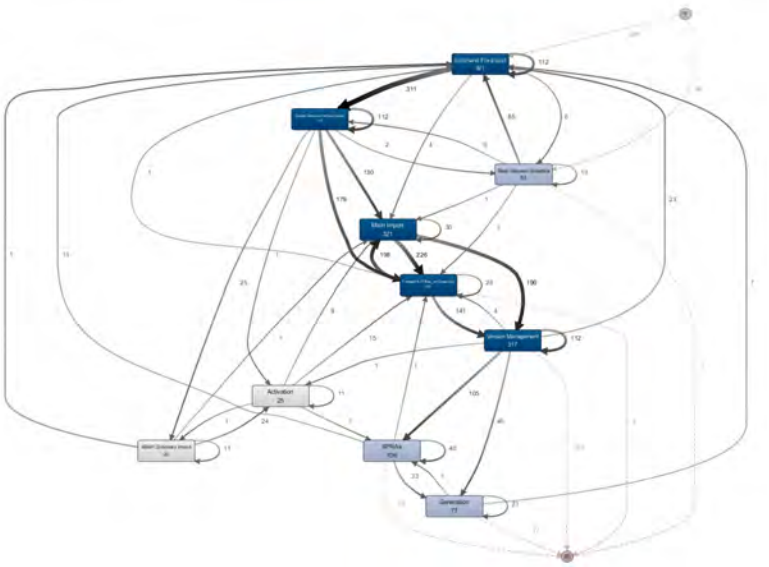


Figure 10: The transportation process discovered for transports that originate from system 1.

Figures 10 shows the process model discovered for the transports that originate from system 1 and Figure 11 shows the process model discovered from the transports originate from system 2. As can been seen, the flow for transports of system 2 is simpler and more straight-forward compared to process flow related to transports originating from system 1.

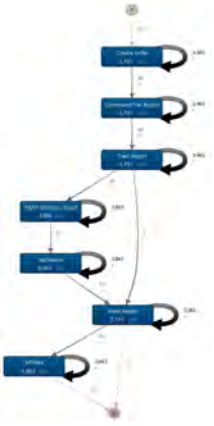


Figure 11: The transportation process discovered for transports that originate from system 2.

As a part of this analysis, we analysed the quality of transportation process. As explained earlier the transportation process starts in development environment. Several activities may be executed in development environment, then it should move to quality environment and finally to production environment. We found 36 cases that did not followed the process path as designed.

Figures 12 and 13 show example of transports that did not adhere to the desired flow illustrated in Figure above.

Figure 12: Example of a violating rapport that were imported to production environment directly from development environment.

As is shown in the Fig. 12, the transport was directly imported from the development environment (DED) to production environment (DEP) without passing through Quality environment (DEQ).

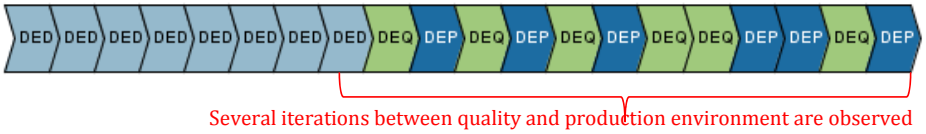


Figure 13: Another example from a violating transport that were imported from production back to quality environment.

In another violating example shown in Figure 13, the auditor observed several iterations between quality (DEQ) and production environment (DEP). This observation reveals that the transport needed to go back to the quality environment several times. Therefore, there is a high probability that the transport did not have the quality expected and should have not been imported to the production environment at the first place.

Using process mining, the auditor was able to do a precise and detailed analysis on the transportation management process. The auditor used the whole population of data for analysing the quality of transportation process and provided detailed and precise diagnostics about the violations.

Use Case: Improving business processes and perform a post-implementation process review
This use case describes the use of process mining at an insurance company. Process mining has been applied to discover variations within the insurance policy change process. All changes to insurance policies (of one specific type of policy) of one month were analysed. The primary goal was to prove process mining as a valuable contribution to the organization in a Proof of Concept.

The project had several phases. Since the insurance data model can become quite complex, we started off with a process and data understanding. The primary goal was to identify the suitable process and insurance policies group to perform process mining. Furthermore, we needed to identify the data needed to be able to perform the analysis. This activity was performed together with the functional and technical managers of the system. The result of this phase is a helicopter view of the data. This gave insights in the number of policies, the number of changes per policies (the cases), and the different activities performed in these cases.

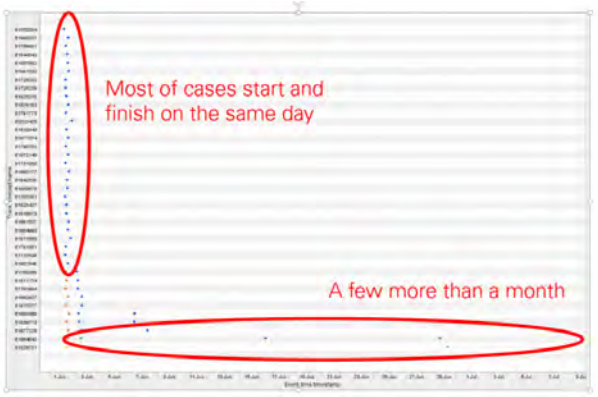


Figure 14: Distribution of completion dates of the cases in the system

Outliers in terms of run-time were also identified using graphs like Fig. 14 in which the differences in execution-time were highlighted.

The next phase was the process variation detection. In this phase, the different activities for the cases were identified. Moreover, the cases can be grouped by the activities that were performed per case.

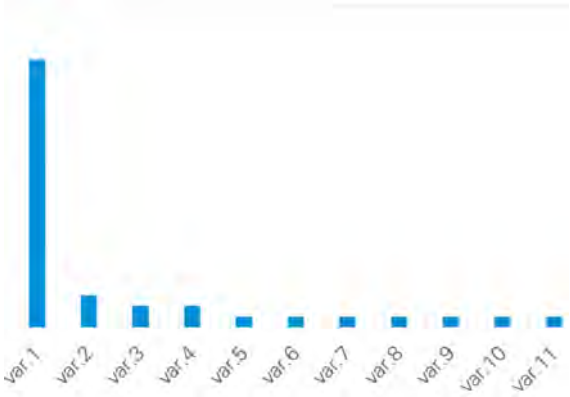


Figure 15: Number of activities performed per process variation

The end result of this phase is a grouping of cases by the variation of the same activity which are performed as shown in Fig. 15. Hereby the dominating variation can be identified and improvement can be made to this variation as it would lead to the highest impact. Also, the remainder of the variation can be investigated for what their purpose is for existing.

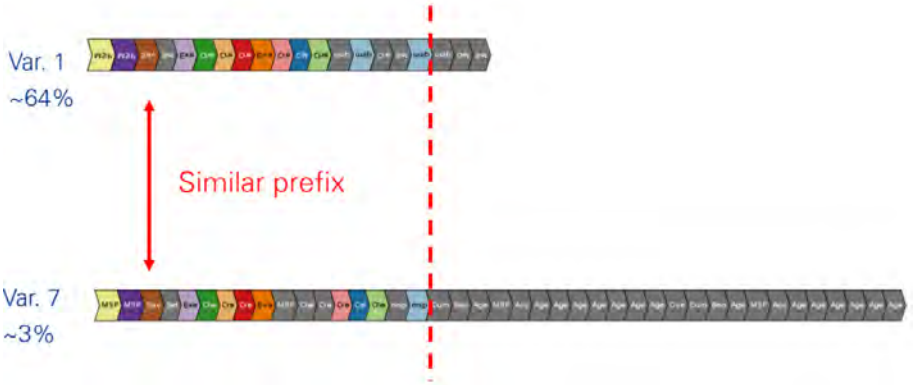


Figure 16: Similar prefix detection

A second result of the process variation detection is the discovery of similar cases. Groups of cases with similar activities but differently ordered, or groups with the same common prefix of activities are identified, such as highlighted in Fig. 16. The first two phases gave already a good insight into the process of changing insurance policies and the type of changes performed. However, the actual process mining was executed in the process discovery phase. The result of this phase is a process flow diagram. In the process discovery phase, different type of analysis were performed. The following analysis were performed:

- Control-flow analysis
- Performance analysis
- Resource view analysis

Control Flow Analysis:
With the control flow analysis, different types of insights were gained. First of all, different process variants allow for different process endings. In this particular use case, we found 2 different process endings, one resulting in a successful change in the insurance policy. The secondary process ending showed to be an infinite loop: the case would never actually be closed.

A second insight that was gained, was the identification of redundant and skipped activities. Both redundant and skipped activities can be identified in the insurance policy change process by the criterion on for how many cases these activities are performed. However, skipped activities are not always redundant activities: it is up to the interpretation of the end user how to value those and which skipped ones were crucial for the process.

The third insight in this phase, were the case bottlenecks. Such a bottleneck is either an (in)finite loop over multiple activities, or an activity that is performed over and over again before going to the next activity. Also for each of these activities a root cause had to be made.

The process flow diagram shows insights such as different ending activities, redundancy in activities

performed, and bottlenecks.

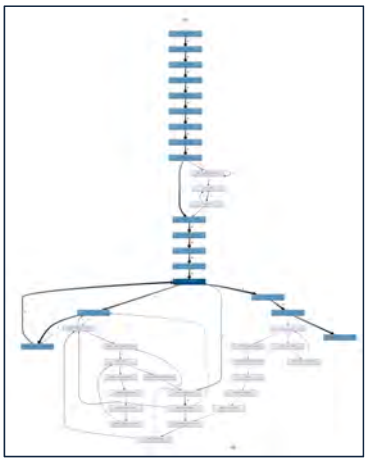


Figure 17: A typical process flow diagram with different ending activities, redundancy in activities performed and bottlenecks.

Performance analysis:
In the performance analysis, the activities were identified that took on average a long time to execute. Besides the averages, also the median, minimum and maximum amount of execution time were taken into account.

This analysis resulted in the insight that some activities within the process flow took almost 30 days on average! This is demonstrated in Fig. 18 below.

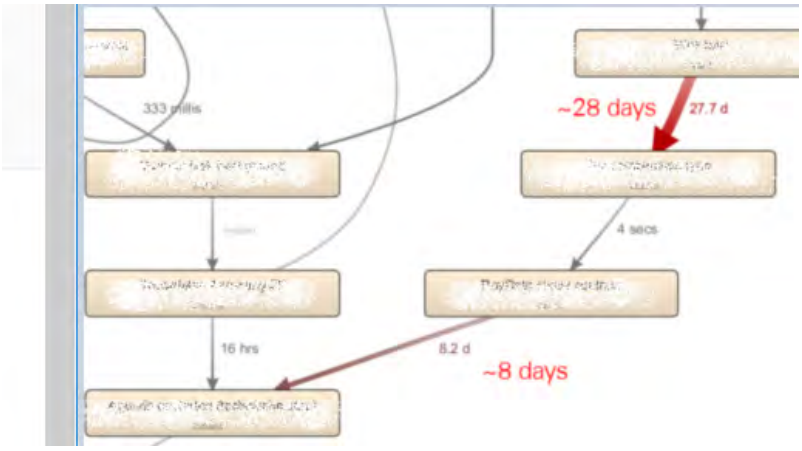


Figure 18: Average run-time of processes

The final analysis that was performed during the process discovery phase, was the resource view analysis. This analysis show the different employees who have performed an activity within the process.

The handover of work and the employees working close together can be identified using the resource view; Fig. 19.

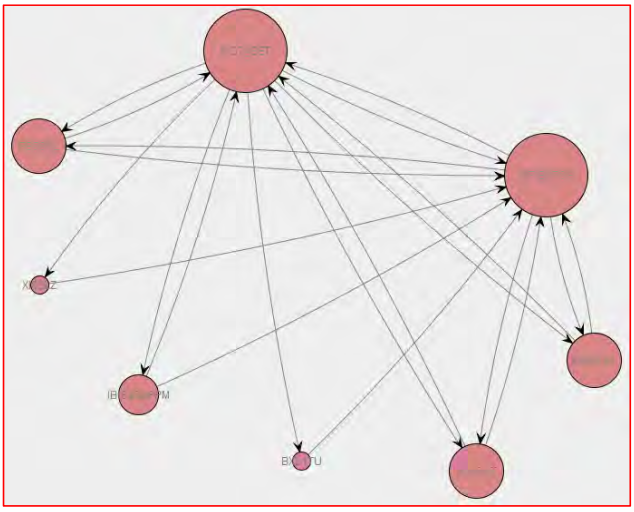


Figure 19: Resource view analysis

There are multiple other kinds of analysis that can be performed using process mining, depending on the wishes and desires of the client.

7 Process Mining Methodology

Conducting a successful process mining project, whether in context of an audit or a process analysis and improvement project, is not trivial. A systematic approach is recommended to be followed. Below, we present a generic methodology that can be adopted according to the requirements of a specific project.

A process mining project can have a very concrete target, e.g., increasing efficiency and reducing cost by 10% for a given process. The goal may also be more abstract, e.g. obtaining valuable insights regarding the compliance state of several processes. Either way, it is necessary to translate these goals into concrete analysis questions. Using process mining mythology, these questions are iteratively investigated, refined and answered. The result of such analysis are the basis of improvement initiatives and concrete action point for the selected process.

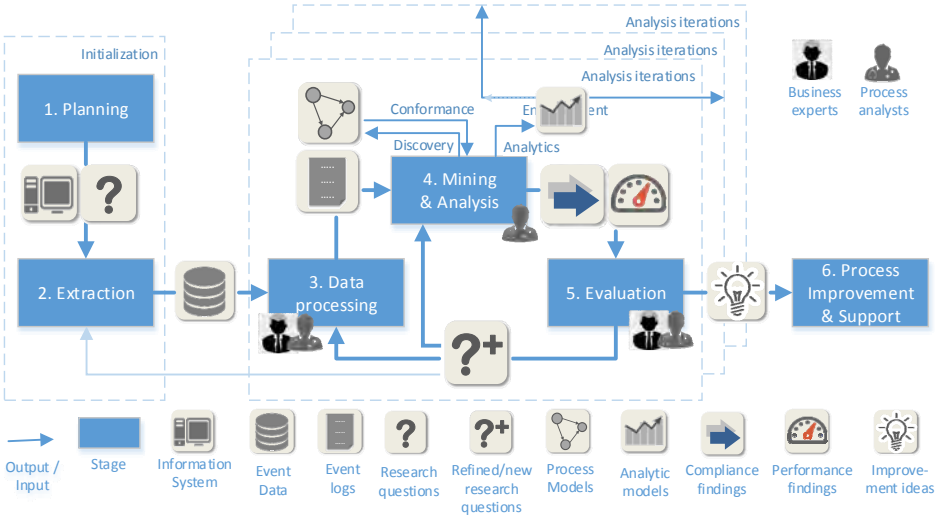


Figure 20: Process mining mythology (Aalst M. L., 2015)

An overview of the process mining methodology is shown in figure 20 above. The methodology consists of six stages that relate to several different input and output objects.
The first two stages of the methodology are (1) planning and (2) extraction, during which initial analysis questions are defined and event data are extracted. The processes in scope, the period of the analysis, the business questions to be answered, the team composition and the analysis timeline are defined during the planning. During data extraction, data requirements are defined, scope of the data extraction is set and the data is retrieved. The systems and tables that need to be retrieved, the attributes (data fields), granularity of the data, and the logic with which the data should be collected and connected must be defined at this stage.

The third stage is (3) data processing. In many situations, the retrieved data cannot be directly used for process mining, rather some preparation and transformation steps are required. Depending on different analysis questions, data processing may be executed multiple times to enable a specific analysis. For standard analysis questions such as "how does a specific process look like?" established techniques can be used. However, if the analysis questions are more abstract, more explorative analysis is required and sometimes a combination of several techniques must be used.
The object of the fifth stage in the process mining methodology, (5) evaluation, is to relate the analysis findings to improvement ideas that achieve the project goals. This include the correct interpretation of the results. Note that this interpretation need to be validated and verified by domain experts.
Finally during the (6) process improvement & support stage, the insights obtained from the previous stages are used to modify the actual process execution. Note that at this stage, process re-engineering techniques and Six Sigma can be leveraged. Finally process mining can be used to continuously monitor the processes and support a sustainable change in the operation.

Aspect of Process Mining Tooling
Although process mining is a relatively new discipline in data science, during the last few years many commercial tools have been introduced to the market. There are various ways to characterize process mining software. Process mining software can be dedicated to purely process mining or they can be embedded in a larger suite such as a larger BPM, BI or data mining suite. Below we list some criteria which can be used to characterize process mining tools. As such it is important to determine which functionalities are important, and look for a process mining tool which best fits the requirements.

Data import. As discussed before, the input for process mining is event data. Process mining software may have different mechanisms to import event data: File (event data stored as XES, MXML, CSV, or Excel file), Database (event data loaded from a database system), Adapter (event data from a particular application (e.g. SAP) through a dedicated piece of software), or Streaming (stream of events read through an event bus or a web service). In most cases, the data of processes will not be in the event data format. This means that data has to be transformed so it fits the requirements of the process mining tool.

Hosting. Process mining software may run locally or remotely as: Stand-alone (the software runs locally, e.g., on the laptop used for analysis), On premise (the software runs a server inside the organization) and Cloud (the software runs on cloud).

Supported process mining techniques. We can categorize process mining tools w.r.t the process mining techniques they support: Discovery, conformance checking, enhancement and process analytics.

Open source versus closed source. Process mining software can be open source or commercial. ProM is the leading open-source process mining tools with over 1500 plugins that cover the state-of-the-art in process mining techniques. There are some other non-commercial tools like PMLAB or CoBeFra, however the majority of research in process mining is implemented in ProM.

As mentioned earlier, several commercial tools emerged on the market in recent years. Compared to ProM, these tools are easier to use, but provide less functionality compared to academic tools.
Most of the commercial process mining tools support process discovery but only a few support conformance checking. The functionalities of the commercial tools are rather limited compared to academic tools such as ProM. However these tools aim at supporting less experienced users. Most of the commercial tools can work with large sized event data efficiently.

8 How to Conduct a Successful Process Mining Project

Usually process owners and middle-level managers are the group which appreciate the true value and insight process mining technology can add to business. Hence, usually process mining is not a top-down initiative in companies. Nevertheless, support and commitment of high-level management is required to overcome the difficulties on the way.
Similar to any project that introduces and establishes a new technology in an organization, process mining projects may face the typical challenges. Apart from these challenges one should not have an unrealistic picture of data availability and data preparation. Although in big data era, omnipresence of data has stimulated several data analysis projects in companies, we should know that obtaining meaningful data is not always easy. As described earlier, data has to comply with minimal requirements when using process mining techniques. In addition, like many other data analysis projects, data quality plays an important role in gaining useful results. For example, in many situations the timestamp of events are missing or they are recorded only on day level whereas several events occurred during day. Consequently, it is not possible to know the exact ordering of these events. Note that many of these problems have already been researched and for many problems solutions exist to overcome them or minimize their negative impact on the analysis. Nevertheless, we would like to emphasize the importance of data preparation before starting a process mining project.
In the following, we list some criteria that help to increase the success in a process mining project.

Understand the business problem and prove value

First of all, it is important to understand and know in detail the business questions that should be answered using a process mining analysis. Process mining technology has an explorative nature and offers a lot of possibilities to analyse a dataset. However, one can get drown in the analysis results. Therefore, it is of essential to specify exactly what business questions should be answered and iteratively relates the findings to these questions. That is, one need to focus on the value that the results of the analysis should provide instead of getting excited about all the different analysis possibilities.

Choose your first project wisely

The event logs obtained from workflow driven systems are usually the best candidates to start with process mining. It is better to start with such datasets which requires less preparation. It is also important to start with a process that you know and has a clear structure (and has only one source of data). In this case it is easier to interpret the results and obtain insights. In addition, it would be easier to convince higher-level management about the value that can be added to the business using process mining. Special care is also required during the preparation of data. Sloppy data preparation step can lead to inaccurate results. In this case, you may lose the interest of higher-management.

Involve people and communicate openly

Input for process mining projects are event data. However, in many situation context of a business process is not captured in data. Therefore, it is important to communicate the results with relevant people as observations rather than presenting subjective conclusions. Involve domain experts and speak openly and transparently about the data that you use and about the facts that come out of this analysis.

9 References

Acknowledgement
This article is based on, and an update and expansion of, the article “Process Mining: Let data describe your process” in Compact magazine, issue 2016/4, https://www.compact.nl/en/articles/process-mining/
We would like to thank our colleagues Bert Scherrenburg and Sander Kuilman for their substantial support in writing this paper.

Aalst, M. L. (2015). PM 2: A Process Mining Methodology. *Advanced Information Systems Engineering - 27th International Conference* (pp. 297--313). Stockholm, Sweden: Springer.

Aalst, W. M. (2016). Process Mining - Data Science in Action, Second Edition. Springer.

Arbor Networks. (2013). *Understanding DDoS*. Retrieved December 8, 2014, from Digital Attack Map: http://www.digitalattackmap.com/understanding-ddos/

Arbor Networks. (2014). *Largest DDoS Attack Reported.* Burlington: Arbor Networks.

Blank, A. (2004). *TCP/IP Foundations.* Alameda: SYBEX Inc.

Deming, W. E. (2000). *Out of the Crisis.* Cambridge: MIT Press Ltd.

EC-Council. (2010). *Ethical Hacking and Countermeasures: Treats and Defense Mechanisms.* Clifton Park: Cengage Learning.

Federal Financial Institutions Examination Council. (2012). *Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources.* Arlington: Federal Financial Institutions Examination Council (FFIEC).

Fitzgerald, J., & Dennis, A. (2009). *Business Data Communications and Networking.* Hoboken: John Wiley & Sons.

Goncharov, M. (2012). *Russian Underground 101.* Cupertino: Trend Micro Inc.

Govcert.nl. (2006). *Aanbevelingen ter bescherming tegen Denial-of-Service aanvallen.* Den Haag: Govcert.nl.

Govcert.nl. (2010). *Whitepaper Raamwerk Beveiliging Webapplicaties.* Den Haag: govcert.nl.

IntruGuard. (2008, November 10). *10 DDoS Mitigation Techniques.* Retrieved February 2, 2015, from www.slideshare.net: http://www.slideshare.net/intruguard/10-ddos-mitigation-techniques-presentation

Kostadinov, D. (2013, October 24). *Layer Seven DDoS Attacks*. Retrieved January 10, 2015, from InfoSec Institute: http://resources.infosecinstitute.com/layer-seven-ddos-attacks/

McDowell, M. (2013, February 6). *Understanding Denial-of-Service Attacks*. Retrieved December 7, 2014, from United States - Computer Emergency Readiness Team (US-CERT): http://www.us-cert.gov/ncas/tips/ST04-015

Nationaal Cyber Security Centrum. (2012). *ICT-Beveiligingsrichtlijnen voor webapplicaties - Deel 1.* Den Haag: Nationaal Cyber Security Centrum.

Nationaal Cyber Security Centrum. (2012). *ICT-Beveiligingsrichtlijnen voor webapplicaties - Deel 2.* Den Haag: Nationaal Cyber Security Centrum.

National Cybersecurity and Communications Integration Center. (2014). *DDoS Quick Guide.* Arlington: National Cybersecurity and Communications Integration Center.

National Institute of Standards and Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Gaithersburg: National Institute of Standards and Technology.

Prolexic. (2013). *Quarterly Global DDoS Attack Report Q3 2013.* Hollywood: Prolexic.

Prolexic. (2014). *Quarterly Global DDoS Attack Report Q1 2014.* Hollywood: Prolexic.

Saxena, P. (2014). OSI Reference Model – A Seven Layered Architecture of OSI Model. *International Journal of Research (IJR), 1*(10), 1145-1156.

Smits, M. S. (2011). *Hoe het internet de Nederlandse economie verandert.* Amsterdam: The Boston Consulting Group.

Symantec. (2009, September 10). *News room - press releases*. Retrieved September 4, 2014, from Symantec: http://www.symantec.com/about/news/release/article.jsp?prid=20090910_01

Tanenbaum, A. S. (2002). *Computer Networks.* Upper Sadle River: Prentice Hall PTR.

Verisign. (2012). *Distributed Denial of Service (DDoS): finally getting the attention it deserves.* Reston: Verisign Public.

Verisign. (2014). *DDoS Protection Services Overview.* Reston: Verisign Public.

Aalst, W. (2016). Process Mining – Beyond Intelligence

Aantoonbaarheid van de effectieve werking van het incident management proces door KPI-rapportages bij IT Service Organisatie

Michelle Kroon-Bakker
Nathan Versnel

	
In 2016 Michelle graduated with a master degree IT audit, compliance and Advisory at the VU University Amsterdam. Before, in 2012, Michelle graduated on the topic riskmanagement in healthcare as Bachelor of Business Administration at Hanze University of Applied Science. In 2015 she started working at Auditdienst Rijk (ADR), Ministery of Finance. She works at the ADR as a senior auditor at the departments VWS, OCW and SZW. In the past she worked at KoutersVanderMeer as advisor.	Nathan has been working in the IT & Telecom sector since 2008. As an entrepreneur the world of Risk, Compliance and Audit was first introduced to him in 2010 and he performed several projects within multinationals as Getronics, T-Mobile and Royal KPN N.V. In 2012 he joined Royal KPN N.V. where he has fulfilled the roles of IT Risk Manager and IT Compliance Manager. In 2015 he joined the Audit department where he is working as a Senior IT Auditor within Royal KPN N.V.

1 Inleiding

“In veel ondernemingen staat de relatie tussen riskmanagement en prestatiemanagement onder druk” (Kerklaan, 2006). Dit is een uitspraak die we vanuit onze dagelijkse praktijk beleven, waarbij onvoldoende synergie wordt ervaren tussen de three lines of defense.

Dit onderzoek is gericht op de mogelijke integratie tussen riskmanagement en prestatiemanagement, waarbij de focus met name ligt op het, IT-gerelateerde, incidentmanagement proces en de benadering vanuit een auditperspectief. Met andere woorden op welke wijze kan de effectieve werking van het incident management proces worden aangetoond door middel van KPI-rapportages?

1.1 Aanleiding

IT is voor vele organisaties ondersteunend aan het primaire proces. Vanwege het gebrek aan expertise en kostenreductie kan door een organisatie worden gekozen om IT uit te besteden aan een IT service organisatie. IT service organisaties nemen hierbij een deel van de verantwoordelijkheden met betrekking tot IT-beheer over, dit is afhankelijk van de gemaakte afspraken, die vaak zijn opgenomen in een contract en onderliggende service level agreements. Om vast te kunnen stellen of hetgeen een organisatie met zijn klanten is overeengekomen, voor de levering en beschikbaarheid van diensten, ook daadwerkelijk gerealiseerd is, dienen de service levels bewaakt en gemonitord te worden. Het bewaken van de service levels is altijd de verantwoordelijkheid van de afnemende partij. Service levels zijn veelal geborgd in afspraken ten aanzien van performance waarop vervolgens een norm in de vorm van een KPI is gedefinieerd. Of terwijl, een zekere mate van beschikbaarheid en continuïteit van diensten. Hierin wordt een onderscheid gemaakt of het een KPI is die met een inspanningsverplichting of resultaatverplichting gepaard gaat (Gubbels, 2015):

- Inspanningsverplichting: Een verplichting tot inspanning die een partij aangaat. Dat wil dus zeggen: de partij zal zich inspannen om een bepaald resultaat te bereiken, maar garandeert dat resultaat niet.
- Resultaatverplichting: Een verplichting die veel verder gaat dan de inspanningsverplichting. De partij op wie deze verplichting rust, verplicht zich om een bepaald resultaat te behalen.

Een gebalanceerde overeengekomen service level agreement bestaat uit beide type KPI’s.

Het incident management proces heeft hierin een essentiële rol aangezien een continue levering van IT diensten (lees: aanbod) cruciaal is voor het kunnen vervullen van de primaire functie en het uitvoeren van de primaire processen. Een service organisatie is er dus bij gebaat verstoringen zo snel mogelijk op te lossen conform SLA-afspraken en met een zo beperkt mogelijke down time.

Door deze prestaties te meten, focust prestatiemanagement, zich met name op het beheersen door middel van het opstellen van concreet geformuleerde en meetbare KPI’s. Op basis van strategische doelen van een organisatie wordt bepaald welke prestaties (KPI’s) gemeten moeten worden. Strategische doelen zijn dus een afgeleide van de strategie. De strategie wordt bepaald aan de hand van de missie, visie en kernwaarden van een organisatie. Strategische doelen zullen vervolgens moeten worden vertaald in concrete (jaar)plannen waarin beschreven wordt hoe de organisatie verwacht deze strategische doelstellingen te realiseren. Het blijkt dat het hebben van een missie en een visie voor heel veel organisaties als vertrekpunt geldt. Om tot een goede doorvertaling te komen dient deze te worden uitgevoerd op zowel tactisch als operationeel niveau in een organisatie oftewel, de strategie zal geïmplementeerd en vervolgens gemeten moeten worden (Kaplan, 1991).

Risk management focust met name op het in de greep krijgen van de risico’s waardoor organisaties ‘in control’ zijn. Risico’s worden vaak beschouwd als negatief, waarbij het management een afweging moet

maken tussen mijden, mitigeren of accepteren. Risico's worden onder andere bepaald door maatregelen die worden opgelegd vanuit de toezichthouder of de externe accountant in het kader van bijvoorbeeld de jaarrekeningcontrole of assurance rapportages. Ook met betrekking tot IT-beheersing zijn risico's te onderkennen, die samenhangen met de controlemaatregelen, de zogenoemde IT General Controls. Om aan te kunnen tonen dat de risico's met betrekking tot de betrouwbaarheid van de geautomatiseerde gegevensverwerking in de greep worden gehouden en de geautomatiseerde beheersmaatregelen (application controls) gedurende een periode effectief hebben gewerkt, is het noodzakelijk dat de aantoonbare werking van IT General Controls worden getoetst (Cobit 4.1).

Maar waar komt de waterscheiding tussen prestatie- en riskmanagement daadwerkelijk tot uiting? In het business control framework, dat is opgesteld in het kader van interne beheersing. Risico's worden vertaald naar beheersingsdoelstellingen en beheersingsmaatregelen, maar sluiten vaak niet aan op de strategie. Een strategie wordt, om in te spelen op de veranderende omgeving en afzetmarkt, periodiek opnieuw bekeken door de directie en waar nodig bijgesteld. Echter wordt het business control framework en de bijbehorende risicoafweging niet meegenomen bij het tussentijds bijstellen van de strategie en de bijbehorende strategische doelstellingen. De risico afweging wordt hierdoor niet primair gemaakt op basis van de strategie, maar wat er op dat moment vanuit de externe omgeving is opgelegd (bijv. ACM, AFM, DNB, SOx, de externe accountant etc.) De scope is dan ook vaak met name gericht op de financiële verantwoording met de daaraan gekoppelde financiële risico's. Door riskmanagement niet louter en alleen af te stemmen op de financiële verantwoording, maar te formuleren vanuit de strategie, kunnen risico's worden afgestemd op het zo effectief en efficiënt mogelijk behalen van de strategische doelstellingen.

1.2 Centrale vraagstelling en deelvragen

De mogelijke tegenstelling tussen risk management en prestatiemanagement, heeft geleid tot de volgende centrale vraag:

Op welke wijze en in hoeverre kan de effectieve werking van het incident management proces worden aangetoond met behulp van KPI rapportages bij een IT service organisatie?

Hierbij gelden de volgende deelvragen:

1 *Hoe kan een KPI-stelsel bijdragen aan zowel het risk management- als het prestatiemanagement proces en hoe komt dit tot uiting bij het toetsen van het incident management proces? (beschrijvend)*

2 *Hoe wordt de effectieve werking van het incident management proces getoetst in het kader van de jaarrekeningcontrole en assurancerapportages bij een IT Service Organisatie en op welke wijze komt dat tot uiting in het KPI-stelsel? (analyserend)*

3 *Welke aanbevelingen kunnen worden voorgesteld op basis van de uitgevoerde oordeelsvorming? (beschouwend)*

2 Theoretisch kader

2.1 Prestatiemanagement en riskmanagement

Managers staan altijd te popelen om de kansen die voorbij komen met beide handen aan te grijpen en deze tot een groot succes te maken, maar wegen zij hierbij de risico's ook voldoende af? De afdeling Riskmanagement houdt nauwlettend in de gaten of alles omtrent de interne beheersing volgens de afgesproken procedures verloopt en of de risico's die gelopen worden niet over de grenzen heen gaan, maar belemmeren zij hierbij niet de organisatiedoelstellingen?

2.1.1 Prestatiemanagement

Om prestaties te kunnen beheersen zullen deze gemeten moeten worden. Op basis van strategische doelen van een organisatie wordt bepaald welke prestaties gemeten moeten worden. Strategische doelen zijn dus een afgeleide van de strategie. De strategie wordt bepaald aan de hand van de missie, visie en kernwaarden van een organisatie. Strategische doelen zullen vervolgens moeten worden vertaald in concrete (jaar)plannen waarin beschreven wordt hoe de organisatie verwacht deze strategische doelstellingen te realiseren. Het blijkt dat het hebben van een missie en een visie voor heel veel organisaties als vertrekpunt geldt. Een top-down doorvertaling over alle managementlagen is hierbij essentieel, waarbij een gedegen risicoanalyse gewenst is. Om tot een goede doorvertaling te komen dient deze te worden uitgevoerd op zowel tactisch als operationeel niveau in een organisatie oftewel, de strategie zal geïmplementeerd en vervolgens gemeten moeten worden.

Kaplan en Norton hanteren geen specifieke definitie voor prestatiemanagement, hierdoor wordt, in lijn met de Business Balance Scorecard, de definitie gehanteerd van Dr. Andre de Waal MBA.

> *Prestatiemanagement is het proces waarin sturing van de organisatie plaatsvindt door het systematisch vaststellen van missie, strategie, doelstellingen van de organisatie, deze meetbaar maken om acties te kunnen ondernemen voor bijsturen van de organisatie (Waal 2002).*

Business Balance Scorecard

De Business Balance Scorecard is een framework om managers te helpen bij het beheersen van de strategische doelstellingen. De Business Balance Scorecard bevat de maatstaven die nodig zijn om performance en prestaties te kunnen besturen. De Business Balance Scorecard bevat financiële maatstaven die inzicht verschaffen in geboekte resultaten naar aanleiding van genomen acties.

De Business Balance Scorecard is een praktisch hulpmiddel om het sturen van een organisatie vorm te geven vanuit meer dan alleen een financiële invalshoek. Key Performance indicators (hierna: KPI) meten hierbij of de strategische doelstellingen ook daadwerkelijk worden gerealiseerd.

2.1.2 Riskmanagement

Risk management is een begrip dat de afgelopen jaren steeds vaker naar voren komt. Sinds de financiële crisis zijn organisaties zich steeds meer gaan focussen op het in de greep krijgen van de risico's waardoor organisaties 'in control' zijn.

Hierdoor wordt voor riskmanagement de volgende definitie gehanteerd:

> *Ondernemingsrisicomanagement is een proces dat bewerkstelligd wordt door het bestuur van de onderneming, het management en ander personeel en wordt toegepast bij het formuleren van de strategie en binnen de gehele onderneming, ontworpen om potentiële gebeurtenissen die invloed kunnen hebben op de onderneming te identificeren en om risico s te beheren zodat deze binnen de risicoacceptatiegraad vallen, om een redelijke zekerheid te bieden ten aanzien van het behalen van de ondernemingsdoelstellingen (Flaherty, 2004).*

COSO-ERM

Het COSO-ERM model is geïntegreerd risicomanagement raamwerk, waarbij risicomanagement wordt aangesloten op de organisatie.

Figuur 1: COSO-ERM

Bij COSO wordt naast het identificeren, benoemen en beheersen van risico's (event identification, risk assessment en risk response, control activities) ook rekening gehouden met:

- Internal environment: De toon van de organisatie;
- Objective setting: De doelstellingen waar de risico's op van toepassing zijn;
- Information & communication: Effectiviteit van communicatie;
- Monitoring: Het monitoren van risico's.

Daarnaast kunnen risico's worden ingedeeld in vier categorieën, te weten:

- Strategic: Risico's voor globale doelen die samenhangen met de missie van een organisatie;
- Operations: Risico's voor het gebruik van middelen;
- Reporting: Risico's voor de betrouwbaarheid van rapportages;
- Compliance: Risico's voor het nakomen van wet- en regelgeving.

Ook kan bij COSO-ERM worden aangegeven op welk deel van de organisatie het risico raamwerk wordt ingezet. Dit kan de gehele organisatie betreffen of slechts een business unit (Flaherty, 2004).

In deze paragraaf worden Risk Response en een voorbeeld van een Control Activity nader toegelicht, om de vertaalslag te kunnen maken naar key risk indicators en het aantonen van de effectieve werking.

Risk response

"Onze organisatie is risicomijdend" is een uitspraak die door organisaties wordt gebruikt om de risk response, te duiden. Het wordt neergezet als een kwalitatief begrip. De vraag hoe dit daadwerkelijk tot uiting komt, wordt dan niet beantwoord. Risk response is een 'vaag' begrip waar organisaties de juiste definitie niet van kennen.

De algemeen aanvaarde definitie van risk response volgens COSO is

> *Het management selecteert de reacties op risico's vermijden, accepteren, verminderen of delen van risico waarbij een set acties wordt ontwikkeld om risico s af te stemmen op de risicotolerantie en risicoacceptatiegraad.*

Een voorkomende misvatting is dat organisaties de risk response als een formeel aspect zien welke slechts eenmaal geformuleerd dient te worden. Het is namelijk allesbepalend voor de inrichting van risk management binnen een organisatie. Ook wordt de risk response gezien als een strategisch aspect. Ook dit is een misvatting, want het moet vanuit de strategie voortvloeien over de gehele organisatie. De risk response hoeft dan ook niet voor alle onderdelen in een organisatie hetzelfde uit te vallen. Vaak wordt op strategisch niveau meer risico genomen, terwijl op operationeel niveau er meer aandacht aan de interne beheersing wordt besteed.

Om de risk response te kunnen toetsten op tactisch en operationeel niveau is het van belang om de risico's meetbaar te maken in de vorm van Key Risk Indicatoren (KRI). KRI's zijn indicatoren die worden gemeten door organisaties die vroegtijdige signalen afgeven voor het toenemen van het voorkomen van een risk event in verschillende delen van organisaties. Hierdoor heeft het management en de directie inzicht in potentiële risico's waardoor vroegtijdig geanticipeerd kan worden op risico's die mogelijk de organisatiedoelstellingen in gevaar zullen brengen (Baesley, 2010).

Control activities
Een voorbeeld van beheersmaatregel op organisatorisch niveau zijn de three lines of defense (hierna: 3LoD). Hierbij wordt een organisatie dusdanig ingericht dat het beheersen van risico's via drie lagen in de organisatie geschiedt. Dit drietrapsmodel draagt zorg voor een bepaalde mate van objectiviteit met betrekking tot het signaleren en bewaken van risico's en ingerichte mitigerende maatregelen.

De opbouw van 3LoD is als volgt:
- 1e lijn: De eerste lijn is de business die verantwoordelijk is voor haar eigen processen en de daaraan gekoppelde risico's: 'risk owner'.
- 2e lijn: De tweede lijn ondersteunt en adviseert de eerste lijn over het inrichten van de beheersmaatregelen ten behoeve van het mitigeren van risico's.
- 3e lijn: Om de onafhankelijkheid tussen de eerste en tweede lijn te bewaken en te waarborgen is een derde lijn noodzakelijk. De derde lijn controleert of het mechanisme tussen de eerste en tweede lijn correct verloopt.

2.2 Meetbaarheid incidentmanagement
Een incident, in het kader van de incidentmanagement, is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. De volgende definitie van incidentmanagement wordt gehanteerd:

> *Een incident is een ongeplande onderbreking of kwaliteitsvermindering een IT Service (applicatie/infrastructuur). Incident management is het proces om elke ongeplande onderbreking zo snel en goed mogelijk op te herstellen. (ITIL)*

Bij ITIL ligt de focus op de alignment tussen de IT service en de behoefte vanuit de business. ITIL beschrijft processen, procedures, taken en checklists die toepasbaar zijn voor organisaties ter bevordering van de integratie met de strategie.

IT service organisaties nemen een deel van de verantwoordelijkheden met betrekking tot IT-beheer over van de business, dit is afhankelijk van de gemaakte afspraken, die vaak zijn opgenomen in een contract en onderliggende Service Level Agreements (hierna: SLA's).

Om vast te kunnen stellen of de gemaakte afspraken, voor levering en beschikbaarheid, daadwerkelijk zijn gerealiseerd, dienen de service levels bewaakt en gemonitord te worden. Service levels zijn veelal geborgd in afspraken ten aanzien van performance waarop vervolgens een norm in de vorm van een KPI is gedefinieerd. Of terwijl, een zekere mate van beschikbaarheid, continuïteit en kwaliteit van diensten.

2.2.1 KPI's in het IncIdentmanagement proces
Om te kunnen bepalen welke KPI's van toepassing zijn voor het incidentmanagementproces is bij dit onderzoek gebruik gemaakt van een benchmark van COBIT met ITIL (M Sharifi, 2008). Dit heeft aangetoond dat deze in hoge mate met elkaar overeenstemmen.

Een selectie, uit de benchmark, van de voornaamste KPI's voor het incidentmanagement proces is hieronder weergegeven:

1 Klanttevredenheid
2 Percentage aantal incidenten buiten SLA oplostijd
3 Gemiddelde hersteltijd (MTTR – Mean Time To Repair)
4 Incident wachttijd cijfer (aantal gesloten incidenten gesloten, ten opzichte van het aantal openstaande incidenten in een bepaalde periode)
5 Aantal incidenten tijdig opgelost
6 Percentage van opnieuw geopende tickets
7 Percentage van herhaal verstoringen
8 Aantal incidenten veroorzaakt door onvoldoende opleiding van gebruiker (root cause)
9 Percentage van de incidenten die prioriteit veranderen tijdens de levenscyclus

2.2.2 KRI's in het incidentmanagementproces

Deze set aan KPI's draagt bij aan de meetbaarheid van het incidentmanagement. Hiermee worden niet per definitie de voornaamste risico's binnen incidentmanagement gemeten. Hiervoor dienen, naast KPI's, ook KRI's te worden ingericht om de risico's te kunnen meten. Vanuit beheersings- en jaarrekeningperspectief en vanuit de financiële verantwoording zoals beschreven in het COSO-ERM model, wordt met name gefocust op het risico met betrekking tot de betrouwbaarheid (NV COS 500). Betrouwbaarheid valt uiteen in juistheid, volledigheid en tijdigheid.

2.3 Conclusie Theoretisch Kader

Aan de hand van de literatuur, de Business Balanced Scorecard, COSO-ERM, ITIL v3 en CoBiT 4.0/4.1, zoals deze in voorgaande hoofdstukken zijn geanalyseerd en beschreven, is het Bakker&Versnel model ontworpen. Dit model is ontwikkeld met als doel de waterscheiding tussen prestatie management, risk management en audit terug te dringen. NOREA en het Platform voor Informatiebeveiliging (PvIB) hebben op basis van de normenstelsels van CobiT 4.0, ISO/IEC 1799:2005 en ISO/IEC 20000 beheersmaatregelen geformuleerd die als input dienen voor het Bakker&Versnel model (NOREA en PvIB, 2007).

Beheersmaatregelen	Relevante KRI's	Relevante KPI's
3) Capaciteit is gereserveerd ter afhandeling van incidenten. 4) Oplosgroepen beschikken over informatie over bekende fouten en beschikbare standaardoplossingen. 5) Op basis van risico analyse is vastgesteld voor welk type incidenten er aparte oplosgroepen fungeren, waarin onder meer deelname van specialistische functionarissen is geborgd. 6) Bij (een vermoeden van) het overtreden van beveiligingsregels worden gegevens die betekenis hebben bij de bewijsvoering veiliggesteld. 9) Een incident wordt afgesloten nadat is vastgesteld dat alle vereiste gegevens zijn ingevuld en nadat melder heeft bevestigd dat het incident is opgelost.	**Juist**	1) Klanttevredenheid (I) 6) Percentage van opnieuw geopende tickets(I) 7) Percentage van herhaal verstoringen(I) 8) Aantal incidenten veroorzaakt door onvoldoende opleiding van gebruiker(I) 9) Percentage van de incidenten die prioriteit veranderen tijdens de levenscyclus(I)
1) Voor alle typen incidenten is een formeel en bereikbaar loket ingesteld 2) Incidenten worden systematisch geregistreerd, geclassificeerd op impact en urgentie, en geprioriteerd in overeenstemming met de afspraken over het dienstenniveau. 3) Capaciteit is gereserveerd ter afhandeling van incidenten. 7) Voortgangsbewaking wordt uitgeoefend op de afhandeling van incidenten; incidenten die afspraken over tijdslimieten dreigen te overschrijden worden geëscaleerd. 8) Prioriteren en voortgangsbewaking van incidenten zijn functioneel gescheiden van oplosgroepen.	**Tijdig**	2) Percentage aantal incidenten buiten SLA oplostijd (R) 3) Gemiddelde hersteltijd (MTTR – Mean Time To Repair) (R) 4) Incident wachttijd cijfer (R) 5) Aantal incidenten tijdig opgelost(R) 9) Percentage van de incidenten die prioriteit veranderen tijdens de levenscyclus (I)
1) Voor alle typen incidenten is een formeel en bereikbaar loket ingesteld 2) Incidenten worden systematisch geregistreerd, geclassificeerd op impact en urgentie, en geprioriteerd in overeenstemming met de afspraken over het dienstenniveau. 3) Capaciteit is gereserveerd ter afhandeling van incidenten. 7) Voortgangsbewaking wordt uitgeoefend op de afhandeling van incidenten; incidenten die afspraken over tijdslimieten dreigen te overschrijden worden geëscaleerd. 8) Prioriteren en voortgangsbewaking van incidenten zijn functioneel gescheiden van oplosgroepen.	**Volledig**	1) Klanttevredenheid (I) 6) Percentage van opnieuw geopende tickets (I) 7) Percentage van herhaal verstoringen (I) 8) Aantal incidenten veroorzaakt door onvoldoende opleiding van gebruiker (I) 9) Percentage van de incidenten die prioriteit veranderen tijdens de levenscyclus (I)

Legenda
I = Inspanningsverplichting, een verplichting tot inspanning die een partij aangaat. Dat wil dus zeggen: de partij zal zich inspannen om een bepaald resultaat te bereiken, maar garandeert dat resultaat niet.
R = Resultaatverplichting, een verplichting die veel verder gaat dan de inspanningsverplichting. De partij op wie deze verplichting rust, verplicht zich om een bepaald resultaat te behalen.

Figuur 2: Bakker & Versnel Model

Vanuit het studierapport 'Normen voor de beheersing van uitbestede ICT-beheerprocessen' (NOREA) zijn de beheersmaatregelen gecategoriseerd in:

- Incidenten dienen tijdig en volledig te worden afgehandeld .
- Incidenten dienen doeltreffend te worden afgehandeld.

De beheersmaatregel met de categorie 'tijdig en volledig' zijn geschaard onder de relevante KRI's tijdigheid en volledigheid. Wanneer de beheersmaatregel gecategoriseerd is met 'doeltreffend' zijn deze geplaatst onder de relevante KRI juistheid.

De KPI's vanuit de best practices van ITIL en CobiT zijn gecorreleerd aan de voornaamste risico's (lees: KRI's) vanuit COSO. De KPI's met een tijdigheidsaspect zijn geschaard onder de relevante KRI 'tijdigheid'. Door de dusdanige overlap en samenhang van de risico's met betrekking tot juistheid en volledigheid, gelden de relevante KPI's voor beide relevante KRI's.

Dit heeft geresulteerd in een geïntegreerd model waarbij KPI's kunnen worden ingezet ten behoeve van het informeren van het management over performance van het incident management proces en waarbij eveneens de effectieve werking van het incident management proces kan worden aangetoond ten behoeve van de jaarrekeningcontrole, assurance rapportages en interne beheersing.

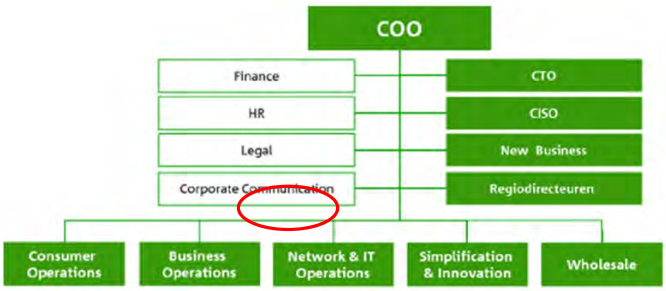
Op basis van de theorie kan worden geconcludeerd dat het mappen van beheersmaatregelen en KPI's vanuit de best practices niet volledig kan worden uitgevoerd zonder deelname van alle stakeholders (3-LoD). Hierbij is het van groot belang dat gezamenlijke (bedrijfs)doelstellingen worden nagestreefd om voor audit-werkzaamheden te kunnen steunen op de KPI-rapportages.
Een goede methode om tot een KPI-stelsel te komen, is een workshop met de voornaamste stakeholders. Hierbij wordt een afgewogen besluit genomen welke beperkte set als KPI wordt aangemerkt. Essentieel bij het besluit is te bekijken welke doelstellingen binnen de afgestemde periode haalbaar zijn.

3 Empirisch Onderzoek

3.1 Situatieschets

De organisatie waarbinnen het empirisch onderzoek zal worden uitgevoerd is een grote telecom-en ICT-dienstverlener gericht op de Nederlandse markt. De organisatie volgt een strategie die op drie pijlers is gebaseerd: versterken, vereenvoudigen en groeien.

Het empirisch onderzoek is uitgevoerd binnen de afdeling ICT Management welke onderdeel is van de Network & IT Operations organisatie van het bedrijfsonderdeel COO, oftewel de operatie (zie figuur 3). Deze divisie, verantwoordelijk voor de beschikbaarheid en bedrijfszekerheid van alle (geïntegreerde) IT diensten en netwerken, maakt het technisch mogelijk dat de telecom-en ICT-dienstverlener zijn diensten en producten kan laten 'draaien'.



Figuur 3: Verantwoordelijkheidsverdeling COO

Binnen Netwerk & Operations wordt voor dit onderzoek specifiek naar de afdeling ICT management gekeken. ICT Management is verantwoordelijk voor eenvoudige, betrouwbare en veilige netwerkdiensten, netwerken en ICT voor de eigen organisatie. ICT Management levert hierbij:

- Beheer op werkende en geïntegreerde ICT diensten en actieve netwerken aan de eigen organisatie.
- Bewaking van de passieve infrastructuur aan Consumer Operations (verantwoordelijk voor aansluitingen en verbindingen consumenten markt).
- Beheer van datacenters, generieke platformen, IT applicaties en werkplekken voor de eigen organisatie.

ICT Management heeft SLA's afgesloten over de keten heen die leidt tot de dienstverlening aan de verschillende afdelingen binnen de organisatie. Hierin zijn ook afspraken ten aanzien van incident management (bijvoorbeeld incident response- en oplostijden) vastgelegd.

De belangrijkste beheersmaatregelen voor het incident management proces hebben betrekking op de verschillende processtappen van:

- Registratie – alle incidenten worden geregistreerd in de gehanteerde registratietool;
- Classificatie – het incident wordt geanalyseerd en de classificatie wordt bepaald aan de hand van impact en urgentie;
- Oplossing – de oplossing wordt geregistreerd en de gebruiker wordt geïnformeerd en accepteert de oplossing;
- Monitoring – KPI-rapportages worden gegeneerd om te monitoren of de incidenten conform de SLA's zijn opgelost en actiepunten worden belegd.

Aan de hand van deze belangrijkste beheersmaatregelen wordt de effectieve werking van het incident management proces vastgesteld op basis van testwerkzaamheden die uitgevoerd worden door de tweede lijn (2nd LoD). De huidige testwerkzaamheden bestaan uit jaarlijks een deelwaarneming van 25 gesloten incidenten te selecteren en op basis van de belangrijkste beheersmaatregelen op de individuele incidenten een aantal zaken vast te stellen aan de hand van de genoemde beheersmaatregelen.

De internal audit afdeling vormt de derde lijn (3rd Lod) en is, onder de verantwoordelijkheid van de Chief Auditor, o.a. verantwoordelijk voor de relatie met de externe auditor. De relatie met de externe auditor wordt hierbij gekenmerkt door:

1 De Chief Auditor is verantwoordelijk voor het vendor management ten aanzien van de geleverde diensten door de externe auditor oftewel het beheren van de contacten en het contract met de externe auditor. Belangrijke elementen hierin zijn:
   - Verantwoordelijkheid voor het budget voor de audit activiteiten ten behoeve van de jaarrekening door de externe auditor.
   - Bewaken van de onafhankelijkheid bij alle door de externe auditor uit te voeren werkzaamheden.
   - Het uitvoeren van een jaarlijkse evaluatie van waargenomen kwaliteit en kosten van de externe auditor.
2 De Chief Auditor is verantwoordelijk voor het realiseren van 'one audit voice'. Zowel interne als externe auditor streven maximale effectiviteit en minimale verwarring na door het helder afstemmen van auditbevindingen, conclusies en aanbevelingen, indien van toepassing.

3.2 Onderzoeksresultaten

In deze paragraaf worden de onderzoeksresultaten naar aanleiding van het empirisch onderzoek gepresenteerd. Het empirisch onderzoek is opgedeeld in twee delen:
- Aan de business manager, de riskmanager, de auditmanager en de externe auditor is een korte vragenlijst en het Bakker&Versnel voorgelegd;
- Er is een assessment georganiseerd, waarbij de vier zelfde key players aanwezig zijn geweest om de input vanuit de vooraf ingevulde vragenlijst te bediscussiëren en tot een gezamenlijke aanpak te komen.

3.2.1 Analyse input managers

Om de input van de managers in de juiste context te kunnen plaatsen, is allereerst nagegaan vanuit welk perspectief de diverse managers, vanuit hun functies, naar het incidentmanagement proces zouden kijken. Hier is het volgende uit naar voren gekomen:
- Business manager (1e lijn) – Downtime reductie als afgeleide van de bedrijfsstrategie;
- Riskmanager (2e lijn) – Mitigeren van de risico's die optreden als gevolg van de gestelde bedrijfsdoelen;
- Audit manager en externe auditor (3e lijn) – Betrouwbaarheid gegevensverwerking ten behoeve van de financiële verantwoording.

Uit de analyse van de vooraf verkregen input is naar voren gekomen dat de antwoorden voor een deel overeenkomstig zijn. Dit biedt aanknopingspunten om uiteindelijk tot een gezamenlijke aanpak te komen om, voor het vaststellen van de effectieve werking van het incidentmanagement proces, te kunnen steunen op de KPI's. Het betreft de volgende punten:
- Tijdig oplossen de incidenten;
- Juistheid en volledigheid van de incidentenregistratie;
- Incidentmanagement dient als input voor problem management;
- Incidenten die veroorzaakt worden door changes (1e lijn en externe auditor);

- Trendanalyses en deep dive/rout cause analysis op geconstateerde incidenten (1e lijn en externe auditor).

Een opvallend punt vanuit de verkregen antwoorden was dat klanttevredenheid als één van de vijf belangrijkste KPI's werd genoemd door de auditmanager (3e lijn). Voor de businessmanager behoort klanttevredenheid niet tot de belangrijkste KPI's, wat gezien de doelstellingen van de organisatie wel in de lijn der verwachtingen ligt.

3.2.2 Analyse assessment

Om te kunnen concluderen of een gezamenlijk aanpak over de verschillende lines of defense heen tot de mogelijkheden behoort, is er voor gekozen om een assessment met alle betrokken managers uit te voeren. Hierdoor kunnen de managers, naast antwoord geven op de gestelde vragen, tevens met elkaar in discussie over de vooraf gegeven antwoorden.

Vanuit de businessmanager werd de waterscheiding tussen prestatiemanagement en riskmanagement onderschreven, waarbij met name werd aangegeven dat de auditlast hoog is als gevolg van de grote hoeveelheid stakeholders. De stakeholders voeren geen overleg over de uitvoering van de diverse audits en onderzoeken, waardoor dezelfde vraag vanuit een ander perspectief meerdere malen wordt gesteld.

Vanuit de riskmanager, de auditmanager en de externe auditor werd aangegeven dat het incidentmanagement proces voor de jaarrekeningcontrole (financiële verantwoording) met name een signaal gevende functie heeft ten behoeve van de IT-beheerprocessen change management en logische toegangsbeveiliging. Voor de jaarrekeningcontrole zijn met name de aspecten juistheid en volledigheid van belang en de tijdigheid speelt in mindere mate een rol.
In het kader van assurance rapportages, zoals ISAE3402 of ISAE3000, wordt incidentmanagement als zelfstandig proces getoetst, waarbij alle drie de aspecten (juistheid, volledigheid en tijdigheid) een rol spelen.

Tijdens het assessment is met name gefocust welke beheersmaatregelen door de managers als belangrijkste kunnen worden beschouwd voor de jaarrekeningcontrole en eventuele assurance rapportages. Daarnaast of er voor deze beheersmaatregelen op KPI-rapportages gesteund kan worden. Uit de discussie is naar voren gekomen dat niet voor iedere beheersmaatregel een juiste KPI beschikbaar is. In sommige gevallen zullen namelijk analyses plaats moeten vinden op de oorzaak van individuele incidenten. Dit wordt niet ondersteund door KPI-rapportages.

Op basis van de vooraf gestelde vragen en de discussie tijdens het assessment is, conform de antwoorden van de managers uit de verschillende lines of defense, een aangepast Bakker&Versnel model opgesteld. De aanpassingen zijn als volgt tot stand gekomen:

Juistheid

De beheersmaatregel die door de managers uit alle lijnen is aangemerkt als 'key' is:
"Op basis van risico analyse is vastgesteld voor welk type incidenten er aparte oplosgroepen fungeren, waarin onder meer deelname van specialistische functionarissen is geborgd."
Echter werd aangegeven dat het toewijzen van incidenten aan oplosgroepen niet geschiedt op basis van het type incidenten, maar op basis van de asset die geraakt is. Voor iedere asset zijn aparte oplosgroepen ingericht. Om te kunnen bepalen welke asset wordt geraakt moet geen risicoanalyse, maar een root cause analysis worden uitgevoerd. Om een uitspraak te kunnen doen over het juist toewijzen van incidenten wordt gekeken naar herhaalverstoringen en opnieuw geopende tickets. Dit geeft een indicatie dat, bij het opnieuw openen van een ticket, een incident nog nader bekeken moet worden, of dat, bij herhaalverstoringen, de root cause nog niet is weggenomen.

Daarnaast is beheersmaatregel 9 aangewezen:
"Een incident wordt afgesloten nadat is vastgesteld dat alle vereiste gegevens zijn ingevuld en nadat melder heeft bevestigd dat het incident is opgelost."
Deze beheersmaatregel is niet als 'key' aangewezen voor juistheid, maar om aan te geven dat wanneer alle verplichte velden gevuld zijn, deze ook juist gevuld worden. Aangezien het hier de inhoudelijke informatie van de afzonderlijke tickets betreft, kan dit enkel worden bekeken door op incidenten een incident (of problem) analyse uit te voeren. Dit is niet af te vangen met KPI-rapportages, waar naar het grote geheel wordt gekeken.

Tijdigheid
Beheersmaatregel 7 is als key is aangewezen voor tijdigheid en betreft:
"Voortgangsbewaking wordt uitgeoefend op de afhandeling van incidenten".
Het bewaken van de voortgang van de afhandeling van incidenten, zorgt er voor dat incidenten niet langer openstaan dan door de organisatie als noodzakelijk wordt geacht. Door de gemiddelde hersteltijd te analyseren kan door de managers een inschatting worden gemaakt of dit aansluit bij de afgesproken service levels. Hierdoor is het noodzakelijk om de gemiddelde hersteltijd in te delen per prioriteit.

Volledigheid
Om de volledigheid vast te stellen is slechts één beheersmaatregel als key aangewezen, namelijk:
"Een incident wordt afgesloten nadat is vastgesteld dat alle vereiste gegevens zijn ingevuld en nadat melder heeft bevestigd dat het incident is opgelost."
Vooraf wordt door de organisatie aangegeven welke velden bij de registratie ingevuld moeten worden om over voldoende informatie te beschikken om het incident te kunnen oplossen binnen de gestelde kaders (bijv. service levels). Wanneer alle vereiste gegevens ingevuld zijn, is de registratie van het incident volledig ingevuld, maar over de juistheid kan in dat geval geen uitspraak worden gedaan. De minimale set aan gegevens kunnen in de registratietool worden afgedwongen (application control), waardoor het systeem afdwingt dat alle velden ingevuld moeten zijn alvorens een incident gesloten wordt. Uit de discussie is naar voren gekomen dat hiervoor geen KPI beschikbaar is en dat dit enkel kan worden vastgesteld door een analyse op de verplichte invoervelden, ofwel het testen van de application control op de registratietool.

Op basis van bovenstaande input van de managers en de discussie zijn de volgende constateringen naar voren zijn gekomen en is het Bakker&Versnel model aangepast. De uitkomst is als volgt:

Beheersmaatregelen	Relevante KRI's	Relevante KPI's
5) Op basis van root cause analyse is vastgesteld voor welk type asset er aparte oplosgroepen fungeren, waarin onder meer deelname van specialistische functionarissen is gebordg.*) 9) Een incident wordt afgesloten nadat is vastgesteld dat alle vereiste gegevens zijn ingevuld en nadat melder heeft bevestigd dat het incident is opgelost *(primaire beheersmaatregel voor volledigheid en secundair voor juistheid)*	**Juist**	Beheersmaatregel 5 **6) Percentage van opnieuw geopende tickets** **7) Percentage van herhaal verstoringen** Beheersmaatregel 9: Geen KPI voor beschikbaar Vaststellen d.m.v. incident/problem analyse
7) Voortgangsbewaking wordt uitgeoefend op de afhandeling van incidenten.*)	**Tijdig**	**3) Gemiddelde hersteltijd per prioriteit (MTTR – Mean Time To Repair)**
9) Een incident wordt afgesloten nadat is vastgesteld dat alle vereiste gegevens zijn ingevuld en nadat melder heeft bevestigd dat het incident is opgelost.*)	**Volledig**	Geen KPI voor beschikbaar Vaststellen d.m.v. analyse op verplichte invoervelden

Randvoorwaarden:
2) Incidenten worden systematisch geregistreerd, geclassificeerd op impact en urgentie, en geprioriteerd in overeenstemming met de afspraken over het dienstenniveau.
8) Prioriteren en voortgangsbewaking van incidenten zijn functioneel gescheiden van oplosgroepen.

) Dikgedrukt is aangemerkt als key control

Figuur 4: Bakker & Versnel model Conform Empirisch onderzoek

Uit de discussie is eveneens naar voren gekomen dat er twee soorten KPI's te onderscheiden zijn:

- Harde KPI's – De harde KPI's zijn met name gericht op resultaat. Op harde KPI's kan gesteund worden met betrekking tot de effectieve werking van een beheersmaatregel. Harde KPI's zijn met name van toepassing voor het aspect tijdigheid.
- Signaal gevende KPI's – Voor de aspecten juistheid en volledigheid geven de KPI's met name een signaal om een deep dive te doen om zo oorzaken van individuele incidenten nader te analyseren. Er kan voor deze aspecten niet direct gesteund worden op KPI's.

Om te kunnen steunen op de KPI-rapportages is tijdens de discussie tevens een aantal randvoorwaarden naar voren gekomen. Deze belangrijkste randvoorwaarden moeten, volgens de managers, aanwezig zijn om gebruikte kunnen maken van het Bakker&Versnel model:

1 Definieer duidelijke definities voor zowel de beheersmaatregelen, als de KPI's. Door definities op te stellen is voor alle interne en externe stakeholders duidelijk hoe de beheersmaatregel en KPI geïnterpreteerd moeten worden. Wanneer beheersmaatregelen multi-interpretabel zijn, kunnen de verwachtingen uiteenlopen waardoor het achteraf niet mogelijk blijkt te zijn om gebruik te maken van de gegevens/informatie.
2 KPI's moeten niet manipuleerbaar zijn vanuit het management. Wanneer KPI's te manipuleren zijn door de business, zijn deze niet langer betrouwbaar om op te kunnen steunen vanuit beheerperspectief. KPI-rapportages moeten objectief tot stand komen. Dit hangt sterk samen met het eenduidig formuleren van de KPI's.
3 Toets periodiek de IT-General Controls voor de registratietool. De KPI rapportages worden rechtstreeks uit de registratietool ontsloten, waardoor de betrouwbaarheid van de registratietool en het genereren van output vanuit deze registratietool vastgesteld moet worden. Door periodiek minimaal de logische toegangsbeveiliging en change management te toetsen, wordt gecontroleerd of de registratietool wordt beheerd met een redelijke mate van zekerheid.

Tot slot werd tijdens de discussie, ten aanzien van het omlaag brengen van de auditlast voor de eerste lijn, aangegeven door de auditors dat de eerste lijn ervoor moet zorgen dat de juiste stakeholders aan tafel komen wanneer de eerste lijn hierover in gesprek te gaat. Door de eerste lijn werd echter aangegeven dat door stakeholders zou moeten worden bepaald waar de prioriteiten moeten liggen.

4 Conclusies

"In veel ondernemingen staat de relatie tussen riskmanagement en prestatiemanagement onder druk". Dit is een uitspraak die we vanuit onze dagelijkse praktijk beleven, waarbij onvoldoende synergie wordt ervaren tussen de three lines of defense (hierna: 3-LoD). Bij het opstellen van de missie, visie en strategie van een organisatie wordt de richting voor de lange termijn bepaald, maar wordt hierbij rekening gehouden met de risico's die deze richting met zich meebrengt? Hoe wordt deze richting, maar ook de risico's door vertaald naar tactisch en operationeel niveau, uiteindelijk gemeten? Tijdens het onderzoek is bekeken hoe de brug tussen prestatiemanagement, riskmanagement, maar ook audit (3-LoD) kan worden geslagen, door gebruik te maken van elkaars informatiestromen. In deze conclusie worden allereerst de deelvragen beantwoord, om vervolgens de hoofdvraag te beantwoorden.

Deelvraag 1. Hoe kan een KPI-stelsel bijdragen aan zowel het risk management- als het prestatiemanagement proces en hoe komt dit tot uiting bij het toetsen van het incident management proces?
Met de introductie van de Business Balanced Scorecard is de KPI (hierna: Key Performance Indicator) ontstaan om de strategische doelstellingen vanuit een financiële invalshoek te kunnen meten. Dit is bij uitstek het meten van de prestaties van een organisatie: prestatiemanagement. Echter geeft het meten van de strategische doelstellingen niet aan of deze doelstellingen op een beheerste wijze worden behaald.

Vanuit riskmanagement wordt op strategisch niveau ook aangegeven op welke wijze risico's beheerst moeten worden, ook wel de risicoacceptatiegraad genoemd. Deze risicoacceptatiegraad bepaalt in hoeverre een organisatie bereid is om risico's te nemen. Hierdoor heeft de risicoacceptatiegraad invloed op de gestelde strategische doelstellingen en dit komt tevens tot uiting in het meetbaar maken van zowel riskmanagement als prestatiemanagement. Hierdoor kunnen voor het meetbaar maken van strategische doelstellingen KPI's worden geformuleerd en voor het mitigeren van de bijbehorende risico's een KRI (hierna: Key Risk Indicator).

Het toetsen van het incidentmanagement proces gebeurt aan de hand van een normenkader dat is opgesteld aan de hand van risico's die binnen het proces worden geïdentificeerd. De voornaamste risico's binnen het incidentmanagement proces zijn "het onjuist, onvolledig en niet tijdig registreren en afhandelen van incidenten". Op basis van de aspecten juistheid, volledigheid en tijdigheid worden normen opgesteld. Hierdoor vormen de risico's, onjuist, onvolledig en niet tijdig de schakel tussen de KPI's vanuit prestatiemanagement enerzijds en de beheersmaatregelen anderzijds. Aan de hand van best practices als ITIL, COBIT en studierapporten vanuit de NOREA is het Bakker&Versnel model opgesteld die handvatten biedt om, voor de aantoonbaarheid van het incidentenmanagement proces, te kunnen steunen op KPI-rapportages.

Vanuit het literatuuronderzoek kan worden geconcludeerd dat lagging indicatoren (financial), resultaten geven en deze enkel van toepassing zijn voor het aspect tijdigheid. Om de effectieve werking van de beheersmaatregelen met betrekking tot tijdigheid vast te kunnen stellen, kan er gesteund worden op de KPI-rapportages.
Voor de aspecten juistheid en volledigheid kan geconcludeerd worden dat de KPI's een signaal gevende functie hebben, oftewel de leading indicators (non-financial). De KPI's zullen in dit geval signalen geven om analyses uit te voeren op individuele incidenten. Hierbij kan niet gesteund worden op de KPI-rapportages.

Deelvraag 2. Hoe wordt de effectieve werking van het incident management proces getoetst in het kader van de jaarrekeningcontrole en assurancerapportages bij een IT Service Organisatie en op welke wijze komt dat tot uiting in het KPI-stelsel?
Wanneer er vanuit auditperspectief wordt gesproken over effectieve werking dan wordt er vanuit de beroepspraktijk vrijwel direct verwezen naar de begrippen van opzet, bestaan en werking. Echter in het kader van de jaarrekeningcontrole en assurance rapportages is vanuit het literatuuronderzoek naar voren gekomen dat volgens de Richtlijn 3402 en de controle- en overige standaarden NV COS, de effectieve werking de "onderzochte periode" betreft waarover de werking wordt vastgesteld op basis van het toetsen van de "interne beheersmaatregelen". Hieruit kan worden geconcludeerd dat het van belang is dat een organisatie voor processen interne beheersmaatregelen definieert (opzet), implementeert in de bedrijfsprocessen (bestaan) en deze gedurende de onderzochte periode aantoonbaar hebben uitgevoerd (werking). Indien er deviaties worden geconstateerd, zullen aanvullende toetsen of gegevensgerichte controles noodzakelijk zijn om de effectiviteit te kunnen bepalen.

In de huidige situatie zijn vanuit de organisatie de interne beheersmaatregelen vastgelegd in de key controls voor het incident management proces. Deze hebben betrekking op de verschillende processtappen van registratie, classificatie, oplossing en monitoring van incidenten. De key controls zijn zowel opgenomen in het bouwwerk van de organisatie als in het design van het proces.

Aan de hand van deze key controls wordt de effectieve werking van het incident management proces vastgesteld op basis van testwerkzaamheden die uitgevoerd worden door de tweede lijn, de Risk & Compliance afdeling van de organisatie. Bij het testen van de key controls wordt een deelwaarneming van 25 incidenten genomen om het proces te toetsen. De derde lijn, internal audit en de externe auditor, voert

een kwaliteitscontrole uit op de uitkomst en vastlegging van de testwerkzaamheden door de tweede lijn. De derde lijn streeft hierbij naar 'one audit voice' waarbij zowel interne als externe auditor streven naar maximale effectiviteit en minimale verwarring door het helder afstemmen van auditbevindingen en conclusies. Indien de derde lijn de testwerkzaamheden op het incident management proces als positief beoordeeld heeft dan steunt de derde lijn op de resultaten van de testwerkzaamheden door de tweede lijn.

Om tot een gemeenschappelijke aanpak voor het testen van de effectieve werking aan de hand van Bakker&Versnel model te komen is er een interactieve sessie met stakeholders vanuit alle lines of defense georganiseerd. Op basis van de vooraf gestelde vragen en de discussie tijdens interactieve sessie is, conform de antwoorden van de managers uit de verschillende lijnen, een aangepast Bakker&Versnel model opgesteld. In het aangepaste model zijn de KPI's vanuit het literatuur onderzoek gevalideerd op de toepasbaarheid binnen de organisatie met als resultaat een set aan KPI's die kan worden gebruikt ten behoeve van de aantoonbaarheid van de effectieve werking van het incident management proces. De wijze van testen zal bij het steunen op KPI-rapportages ten opzichte van de huidige situatie met name verschillen in het aantal incidenten dat wordt bekeken gedurende een periode. Bij het steunen op KPI-rapportages wordt de gehele populaties bekeken, in plaats van maximaal 25 incidenten per jaar. De conclusies vanuit de interactieve sessie komen aan bod tijdens de beantwoording van de hoofdvraag.

Deelvraag 3. Welke aanbevelingen kunnen worden voorgesteld op basis van de uitgevoerde oordeelsvorming?

Op basis van de uitgevoerde oordeelvorming naar aanleiding van het empirisch onderzoek kan een aantal aanbevelingen worden gedaan voor de toepassing van het Bakker&Versnel model:

- Om voor het incidentmanagement proces vanuit auditperspectief te kunnen steunen, of gebruik te maken van KPI-rapportages, is het noodzakelijk dat de stakeholders met elkaar in gesprek gaan alvorens KPI's en beheersmaatregelen worden opgesteld. Hierdoor kan op voorhand worden afgestemd welke prioriteiten, belangen en verwachtingen de verschillende stakeholders binnen de organisaties hebben. Gedeelde prioriteiten, belangen en verwachtingen van verschillende stakeholders kunnen beter op elkaar worden afgestemd, waardoor één uitvraag bij het lijnmanagement als voldoende wordt beschouwd. Dit heeft een positief effect op de auditlast. Tijdens de interactieve sessie is naar voren gekomen dat wanneer de diverse lijnen met elkaar in gesprek gaan tot een eenduidige aanpak kan worden gekomen.

- Tijdens het assessment werd meermaals aangegeven dat tijdigheid geen aspect is voor de werking van het incidentmanagement proces met betrekking tot de jaarrekeningcontrole. Echter sinds 2014 is door de NBA de nieuwe controleverklaring geïntroduceerd voor organisaties van openbaar belang (OOB's) (NBA, 2014). Door de nieuwe controleverklaring zijn accountants genoodzaakt om de continuïteitveronderstelling door het management te onderschrijven. Om hier een uitspraak over te kunnen doen, is inzicht in de werking van het incidentmanagement proces noodzakelijk. Hierbij speelt naast de aspecten juistheid en volledigheid, die vanuit het empirisch onderzoek naar voren zijn gekomen, ook het aspect tijdigheid een belangrijke rol. Door trendanalyses uit te voeren op de tijdsaspecten van incidenten, kunnen metingen en vergelijkingen worden gedaan ten behoeve van de continuïteitveronderstelling, zoals het tijdig oplossen van major incidenten.

Vanuit de beantwoording op de deelvragen kan de hoofdvraag worden beantwoord: **Op welke wijze en in hoeverre kan de effectieve werking van het incident management proces worden aangetoond met behulp van KPI rapportages bij een IT service organisatie?**

Middels een interactieve sessie met stakeholders vanuit alle lines of defense wordt een consensus nagestreefd aangaande de voornaamste risico's, beheersmaatregelen en KPI's voor het incident management proces. Hierbij vormen best practices als COBIT en ITIL, de richtlijn 3402 en controle- en overige standaar-

den NV COS, welke zijn samengebracht in het Bakker&Versnel model, het uitgangspunt voor het vaststellen van de KPI's die kunnen worden ingezet bij het aantonen van de effectieve werking van het incident management proces bij een IT Service Organisatie.

De effectieve werking van het incident management proces dient te worden vastgesteld op basis van het toetsen van de beheersmaatregelen welke voor het incident management proces zijn opgesteld. Beheersmaatregelen staan nimmer op zichzelf maar zijn afgeleid van de beheersdoelstellingen oftewel wat wil een IT Service Organisatie realiseren in het kader van IT beheerprocessen. Hierbij is het van belang dat de organisatie de risico's voor het incident management proces heeft vastgesteld en de daarbij behorende beheersmaatregelen die deze risico's dienen te mitigeren. De voornaamste risico's binnen het incidentmanagement proces zijn "het onjuist, onvolledig en niet tijdig registreren en afhandelen van incidenten". Op basis van de aspecten juistheid, volledigheid en tijdigheid worden normen opgesteld middels de beheersmaatregelen voor het incident management proces.

Voor de aspecten juistheid en volledigheid is tijdens de interactieve sessie met stakeholders geconcludeerd dat deze KPI's een zogenaamde signaal gevende functie hebben, oftewel de 'leading' indicators zijn. De KPI's zullen in dit geval signalen geven om analyses uit te voeren op individuele incidenten. Hierbij kan niet gesteund worden op de KPI-rapportages.
De KPI's die als' lagging' indicatoren zijn aangeduid, bieden resultaten die enkel van toepassing zijn voor het aspect tijdigheid. Om de effectieve werking van de beheersmaatregelen met betrekking tot tijdigheid vast te kunnen stellen, kan er wel gesteund worden op de KPI-rapportages. Op basis hiervan is het Bakker&Versnel model herzien tot het volgende:

Beheersmaatregelen	Relevante KRI's	Relevante KPI's
5) Op basis van root cause analyse is vastgesteld voor welk type asset er aparte oplosgroepen fungeren, waarin onder meer deelname van specialistische functionarissen is geborgd.*) 9) Een incident wordt afgesloten nadat is vastgesteld dat alle vereiste gegevens zijn ingevuld en nadat melder heeft bevestigd dat het incident is opgelost *(primaire beheersmaatregel voor volledigheid en secundair voor juistheid)*	**Juist**	<u>Beheersmaatregel 5</u> **6) Percentage van opnieuw geopende tickets** **7) Percentage van herhaal verstoringen** <u>Beheersmaatregel 9:</u> Geen KPI voor beschikbaar Vaststellen d.m.v. incident/problem analyse
7) Voortgangsbewaking wordt uitgeoefend op de afhandeling van incidenten; incidenten die afspraken over tijdslimieten dreigen te overschrijden worden geëscaleerd.*)	**Tijdig**	**3) Gemiddelde hersteltijd per prioriteit (MTTR – Mean Time To Repair)**
9) Een incident wordt afgesloten nadat is vastgesteld dat alle vereiste gegevens zijn ingevuld en nadat melder heeft bevestigd dat het incident is opgelost.*)	**Volledig**	Geen KPI voor beschikbaar Vaststellen d.m.v. analyse op verplichte invoervelden
***) Dikgedrukt is aangemerkt als key control**		

Figuur 5: Bakker & Versnel Model

Samenvattend kan worden geconcludeerd dat de KPI voor de 'Gemiddelde hersteltijd' kan bijdragen aan het vaststellen van de effectieve werking van het incident management proces. De KPI's van 'Percentage van opnieuw geopende tickets' en 'Percentage van herhaal verstoringen' zijn signaal gevend ten aanzien van het aspect van de juistheid. Voor het aspect ten aanzien van de volledigheid is tijdens de interactieve sessie geen KPI vastgesteld. De volledigheid dient te worden vastgesteld door een analyse op de verplichte invoervelden, ofwel het testen van de application control op de registratietool.

Om te kunnen steunen op de KPI-rapportages dient aan de randvoorwaarden, die naar voren zijn gekomen tijdens interactieve sessie met stakeholders, te worden voldaan om gebruikte kunnen maken van het Bakker&Versnel model:

- *Definieer duidelijke definities voor zowel de beheersmaatregelen, als de KPI's;*
- *KPI's moeten niet manipuleerbaar zijn vanuit het management;*
- *Toets periodiek de IT-General Controls voor de registratietool.*

Tenslotte is met name de methode voor het opzetten van het model bruikbaar, want de inhoud van het model zal per organisatie verschillend zijn door de relevante beheersmaatregelen, KRI's en KPI's die worden toegepast binnen individuele organisaties.

5 literatuurlijst

Boeken en artikelen

- Anderson, R. (2011) “Risk appetite and Risk Tolerance Institute of Risk Management”
- Baesley. M.S., B.C. Branson & B.V. Hancock (2010) “How key risk inidicators can sharpen focus on emerging risks COSO”
- Cobbold I. & G. Lawrie (2002) “The development of the Balanced Scorecard as a strategic management tool”
- Flaherty, J & T. Maki (2004) “Summary Enterprise Risk Management Integrated Framework (ERM)”
- Groot, T. (2003) “De Balanced Scorecard in bedrijf”
- Haisma, Geert en Erik van Marle (2009) “ISO 31000 stimuleert integraal risicomanagement, TPC”
- Hout van H. (2012) “Three lines of defense: kwestie van dijkbewaking?” (Audit Magazine)
- Kaplan, R.S. & D.P. Norton (1991) “The Balanced Scorecard Measures That Drive Performance”
- Kerklaan L., R. Bode & M. Schijff (2006) “Stop de waterscheiding tussen prestatie- en risk management” (Finance & Control)
- NBA (2014) “Voorlichting Nieuwe controleverklaring voor oob’s”
- M Sharifi et al (2008) “An empirical study identifying KPI’S”
- NOREA en PvIB (2007) “Normen voor de beheersing van uitbestede ICT-beheerprocessen”
- Yin (2009) “Case study research, design and methods” (4th edition)
- Waal, A.A. de (2002) “Lexicon Prestatiemanagement”

Best practice, richtlijnen en regelgeving

- Cobit 4.1
- ITIL V2 en V3
- NV COS
- Richtlijn 3402 NOREA

Websites

- INK Model - http://www.ink.nl/model/ink-managementmodel
- Risman Model - http://www.risman.nl/
- Wetrecht, Gubbels, B.G.N. - http://www.wetrecht.nl/inspanningsverplichting-of-resultaatsverplichting/

Risk management
with Cloud based solutions for small banks

Serkan Kaplanoglu
Patrick Chu

	
Serkan Kaplanoglu is currently working as the CISO of a financial institution. He is a senior IT GRC and Audit professional with over 15 years of experience gained in different major organizations in Finance, Banking and Insurance domains. Having worked previously as an audit manager, he accumulated extensive experience in managing and performing complex IT and business process audits in international environments. He has also involved in the management of Operational Risk Management and Regulatory & Internal Control activities allowing him to have valuable insights in Treasury, Payment, SWIFT, Know Your Customer (KYC), Trade Finance and Accounting operations among others.	As manager at Ernst & Young Accountants LLP in the Netherlands, Patrick is specialized in providing IT audit and advisory services related to Cyber Security, Data Protection and as well as Cloud solutions to a number of EY's Global 360 accounts (G360). Prior joining a Big 4, he was a financial analyst with a strong focus on performing big data analytics to discover patterns, trends and relationships hidden in the raw data.

1 Introduction

1.1 Background

Information and communication technology (ICT) brought a complete paradigm shift on the banks' performance and on the customer service delivery in the banking industry. Banks represent a mixed market for IT solutions and services. In a bid to catch up with global development, banks have invested heavily in ICT to improve the quality of customer service delivery and to reduce transaction cost. Banks have widely adopted ICT networks for delivering a wide range of value added products and services. The ICT developments also have a significant effect on flexibility and user friendliness of banking services[1].

In order to gauge and benchmark trends within the IT industry, each year the Society for Information Management, CIONet, and other leading management associations conduct a survey (the 2013/2014 survey is still currently open) to determine the information technology (IT) practices and trends in organizations around the globe. The research is based on data from five geographic regions: the United States, Europe, Asia, Australia and Latin America. According to the research results, which is reported in "Compact[2]", shows that Cloud Computing is one of the five most influential technologies. The five most influential technologies and their trends are listed below (top down, fig 1):

Application& Technology development	2012/ 2013	2011	2010	2008	2009
Business intelligence	1	1	1	1	2
Cloud Computing (SaaS, Paas, Iaas)	2	2	5	17	-
Enterprise resource planning (ERP)	3	3	3	3	14
Apps development	4	-	-	-	-
Customer relationship management (CRM)	5	5	9	13	-

Figure 5 "Five most influential technologies and their trends from Compact's research results"

Furthermore, in the same "Compact" research, one of the mega trends is identified, which is "Life is in the Cloud". In other words, the trend is that everyone is (or will soon be) online; working online, purchasing online, selling online, communicating online, all creating and consuming data hundreds of times each day.

Although Cloud Computing seems just the latest point in outsourcing's long arc, for banks, it promises to be one of the most significant, if complex. Significant because Cloud's value is proving to be vast and varied at the precise time that banks are eager to lower costs, increase capital and move fast on IT. Complex because Cloud formations come in as many shapes and sizes as there are bank strategies. Rampant cybercrime only adds to that complexity. The Cloud conversation at many banks has been reenergized by regulators' latest demand for higher bank capital levels. Cloud offers the tempting opportunity to shrink capital expenditures on technology and shift them to operating expenditures[3].

The different requirements enable banks to choose from several types of Cloud applications such as private Clouds, for the more sensitive data, and public Clouds to store other information. More frequently, banks are going with a hybrid model that combines the two. Survey results also showed that 50 percent of those surveyed responded that they were likely or highly likely to use private Clouds in the near future[4].

[1] Aliyu, A.A., Tasmin, R.B.H.J., "The Impact of Information and Communication Technology on Banks' Performance and Customer Service Delivery in the Banking Industry", International Journal of Latest Trends Finance and Economic Sciences, Volume 2, No. 1 March 2012, p.80-90

[2] http://www.compact.nl/en/articles/C-2013-4-Derksen.htm

[3] Olson B., Lacey C., Almad A. "Banking's 'Sweet Spot' in the Cloud" BAI Banking Strategies

[4] http://www.forbes.com/sites/tomgroenfeldt/2014/06/26/some-banks-are-heading-to-the-Cloud-more-are-planning-to/

1.2 Problem statement

The Cloud - the savior of IT. Cheap, easy and hassle free, or so the marketing spiel would have you believe. However, there is much more to consider, and recent events have underlined some of the perils that the Cloud can pose. Of course, there is no doubt that the Cloud is here to stay, as huge $1bn investments from the likes of HP, but many firms are still wary about using the Cloud, and with good reason. Banks in general, especially small banks are more cautious than other industries about adopting Cloud services, because of concerns with regard to data security and compliance with law and legislation. These concerns are not limited to security, law and regulatory related ones, but also include lack of knowledge; what is Cloud Computing and what are the business impacts and the deployment issues? Moreover because of a lack of understanding, some (small) banks do not realize that some Cloud solutions are already in place[5], e.g. Microsoft Office 365 and Salesforce Service Cloud. And not forget to mention the availability of the stored data in the Cloud. We live in an age of ubiquitous connectivity that data connections and WiFi services are usually working fine, but we all know the frustration of an unreliable network or even more worse the access disappears, which could leave you cut off from the Cloud and your worst nightmare becomes reality!

Last but not least to mention is the overall security of the stored data. Putting information into services that are accessible over the public internet means that criminals have a potential gold mine of targets. Besides it is not just criminals and hackers who pose a risk. Because simple acts such as sharing links for documents on popular services Dropbox and Box could make information accessible to unintended third parties. The firm that uncovered this, Intralinks, stumbled across the problem and said that it was able to see all types of sensitive data, which no business in their right mind would want to be accessible: tax returns, bank records, mortgage applications, blueprints and business plans. Clearly, if such vital information can be made visible through the simple act of sharing a link via a Cloud storage service, many firms may wonder whether the benefits of the Cloud are worth such big risks[6].

In order to provide more insights in the level of information security within banks, the De Nederlandsche Bank ("DNB") introduced a COBIT 4.1 based self-assessment in 2010. All financial institutions (including banks) in the Netherlands were requested by DNB to reach maturity level 3 for all control objectives, which meant that the control objectives are documented and executed organization wide in a structured and formalized way[7].

On 30 January 2014, DNB published the results of their DNB's self-assessments over 2013. The worst scoring control objectives are presented in the below table (fig 2).

Banks	Insurance companies	Pension funds
13.2 Identification and maintenance of configuration items	***16.3 Internal control at third parties***	18.3 Cryptographic key management
13.1 Configuration repository	17.2 User Accountmanagement	***16.3 Internal control at third parties***
16.3 Internal control of third parties	*2.2 Data classification scheme*	16.1 Security testing, surveillance and monitoring
8.3 Dependence upon individuals	18.5 Exchange of sensitive data	*2.2 Data classification scheme*
2.1 Enterprise Information Architecture Model	16.1 Security testing, surveillance and monitoring	16.2 Monitoring of internal control framework

Figure 6 "DNB's self-assessment worst scoring control objectives"

[5] http://searchitchannel.techtarget.com/feature/Cloud-compliance-management-solutions-in-use-at-small-banks-credit-unions

[6] http://www.v3.co.uk/v3-uk/news/2343547/top-10-Cloud-computing-risks-and-concerns

[7] Koning, E., Brink, M. ten, Baveco, M., Presentation DNB self-assessment results 2013 on seminar "Security: the next level ..." 30 January 2014, p.13

From the worst scoring resulted controls table, we observed that "internal control at third parties" is a concern for all financial institutions, including banks (see fig 2 in dash dots). Within this control the status of external service providers' internal controls are assessed. Furthermore it also evaluates that whether related procedures are in place to ensure that external service providers comply with legal and statutory requirements and contractual obligations.
Via a circular, which was shared on 10 January 2012, DNB drew attention to the supervised institution that the prudential statutory and subsidiary legislation relevant to the subject of Cloud Computing.
In the circular is including that, when using third-party Cloud Computing services, the supervised institution is subject to the legal requirements that apply to outsourcing:

- risks must be demonstrably known and mitigated, and
- outsourcing to third parties may not obstruct supervision.

According to the DNB, before a supervised institution proceeds to engage in Cloud Computing, DNB expects to be informed of this prospective outsourcing arrangement. DNB will ask the supervised institution to submit its risk analysis concerning Cloud Computing for assessment in the context of risk-based supervision.

1.3 Research questions

The main research question is formulated as follows:

> *"Which are the main arguments for management control when adopting Cloud solutions for small banks and which strategic, organizational and managerial objectives for compliance and risk management need to be addressed?"*

In order to answer the main research question, the following three sub-questions are defined and will be answered during our thesis writing.

1. Descriptive: Which major trends in Cloud solutions are relevant for Banking and IT Operations, and which risks domains are being introduced that are relevant for banks?
2. Analysis: Which risks objectives and control areas need to be addressed when using Cloud Computing for small banks?
3. Synthesis: Which key objectives, controls for risk management and compliance can be considered when implementing Cloud based solutions by small banks?

The first sub-question deals with the major trends of Cloud sourcing and banking operations. The second and third sub-questions are to help small banks to identify and to mitigate the risks when implementing Cloud based solutions. We strongly believe that we can contribute to the field of Cloud Computing if we answer these questions properly and these may be used as input for further researches.

2 Cloud is transforming the business of banking

In this chapter, the market (IT) trends in general will be described. Furthermore, the definition of Cloud will be explained in order to help the reader gain a better understanding of what Cloud Computing is and the relation with the banks. It also includes numerous examples across the industry where Cloud has enabled business and operating model innovation.

2.1 Market (IT) trends

Market forces are characterized by headwinds that challenge growth. In IBM's presentation (source from Capital IQ)[8], the headwinds are characterized as turbulent economic conditions, intense competition (non-traditional entrants), evolving consumer expectations, decreasing returns on equity (need to opti-

[8] Cloud Consumer Banking Point of View, Institute for Business Value, IBM, 2014

mize use of capital and shrinking operating margins), increasing regulations and oversight and rebuild customer trust & marketplace confidence.

To overcome these challenges, banks should deliver on four key imperatives:

1 Create a customer focused enterprise: Optimize data and leverage analytics to adapt to new behaviors, cultivate trust, and drive profitable growth;
2 Increase flexibility and streamline operations: Improve operating leverage with variable cost structures that increase flexibility and reduce risk;
3 Drive innovation while managing cost: Deliver new services quickly that decrease cost per transaction and drive competitive differentiation;
4 Optimize enterprise risk management: Maximize return on equity, combat fraud and mitigate operational risk while achieving compliance objectives.

Therefore, business is being transformed on three technology enabled dimensions:

- Data: The new natural resource
- Systems of engagement: Redefines customer relationships
- Cloud: Enables new business models
- Data: Data is the new natural resource and basis of competitive advantage.
- Systems of engagement: Redefines customer relationships. Mobile connectivity and social media is quickly becoming the primary communication and collaboration format.
- Cloud: Enables new business models, such as cloud fosters capabilities that traditional computing cannot (fig 3).

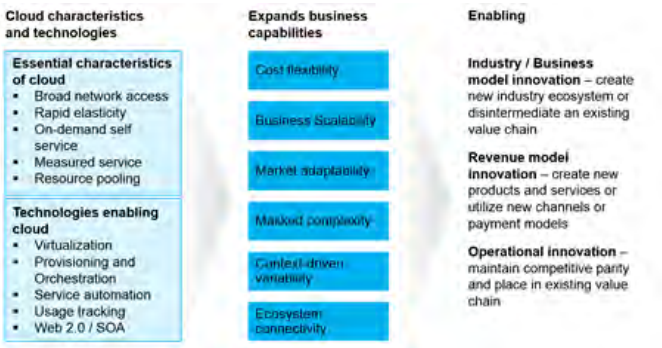


Figure 7 "Cloud capabilities"

2.2 Banking and Cloud based solutions

Cloud Computing is expected to be one of the fastest-growing technologies in the coming years. But what is Cloud Computing? Currently, there are many definitions on what Cloud Computing exactly is.

In 2009, Gartner collected at least 27 'formal' or working definitions on Cloud Computing. The main reason why Cloud Computing is so hard to define, is that it is a specific mix of technologies used and services provided which can be deployed and managed in several ways. Cloud Computing is an umbrella concept, which contains multiple concepts. Defining Cloud Computing can therefore only be done by breaking down the individual components of Cloud Computing. Since our focus is on (small) banks we start with the definition of DNB (De Nederlandsche Bank). DNB defined Cloud Computing in the circular as an "on-demand service model for the provision of IT services, often based on virtualization techniques and distributed computer environments". Also definitions from three other organizations come to the forefront when defining the Cloud: Gartner, Forrester, and the National Institute of Standards and Technology (NIST). Although both Gartner and Forrester provide definitions of Cloud Computing, the NIST definition is

more concise and uses industry-standard terms[9]. Therefore we have used NIST's definition as guidance in our thesis.

National Institute of Standards and Technology's (NIST) definition[10]:

> *"Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."*

2.2.1 Cloud Computing Overview model

Cloud Computing, defined by NIST, is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
This Cloud model is composed of five essential characteristics, three service models, and four deployment models. This information is also visualized below in "NIST's visual model of Cloud Computing" (fig 4).

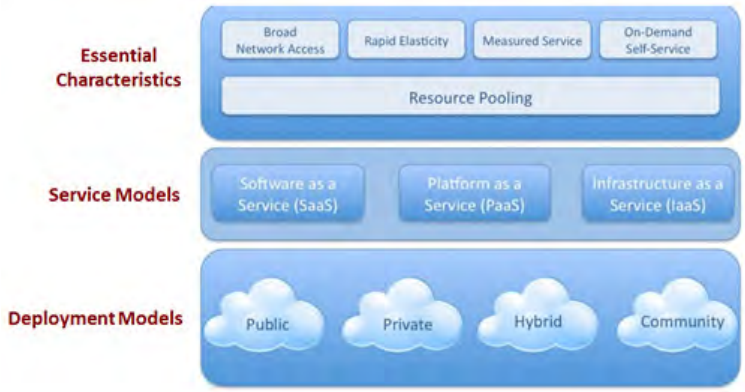


Figure 8 "NIST visual definition of Cloud Computing"

Cloud Service Models

With the internet enabling technologies in place, and together with the IT components, a Cloud is ready to offer financial institutions the option to move from a capital intensive approach to a more flexible business model that lowers operational costs. A Cloud can offer one or more services. Most common services known are: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Cloud Deployment Models

There are three ways service providers most commonly deploy Clouds (fig 5):

1 Private Clouds: The Cloud infrastructure is operated uniquely for a specific organization. It may be governed by the company or a third party and may prevail inside or outside the premises. This is the most impregnable of all Cloud choice.
2 Public Clouds: The Cloud infrastructure is made attainable to the common public or a large industry group and is governed by an organization that trades Cloud services.

[9] http://www.educause.edu/ero/article/Cloud-computing-explained
[10] http://www.nist.gov/itl/Cloud/

3 Hybrid Clouds: The Cloud infrastructure is consist of two or more Clouds (private or public) that remain sole entities but are associated in order to administer services.

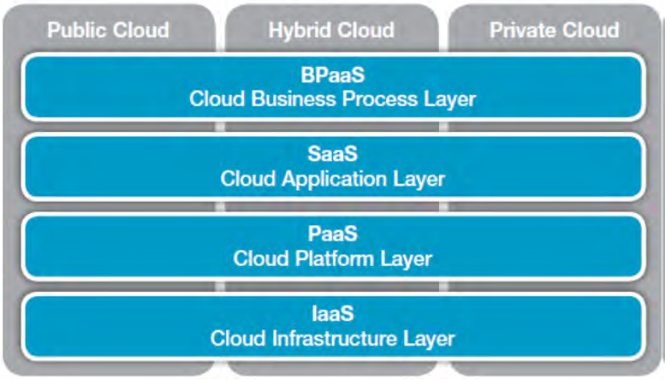


Figure 9 "Cloud Service and Deployment Models"

Cloud Operating Models

Choosing the right Cloud services delivery model is determining the appropriate operating model for the required mix of resources and assets. We have identified three operating models for Cloud services:

1 Staff augmentation: Financial firms can gain Cloud expertise by hiring people with the right skill sets from service vendors. The additional staff can be housed in the firm's existing offshore captive center. This operating model allows for flexibility and lets firms choose the best resource for each specific requirement.
2 Virtual captives: Virtual captives have a dedicated pool of resources or centers to help with Cloud operations and meet demand. This operating model is a good alternative to a complete outsourcing approach.
3 Outsourcing vendors: This approach uses offshore centers, facilities, and people from a third party vendor to handle Cloud operations. The model combines resources and investments to cater to Cloud services for multiple banks[11].

2.2.2 Trends in the banking industry

A new business model with Cloud Computing will shake up the banking industry. According to Accenture's case study, a powerful nexus of changing customer behavior through the use of web, mobile and social connectivity and emerging new technology (e.g., digital, analytics and Cloud) are motivating "smart banks" to re-examine and re-engineer their business models[12].

Accenture sees at least three unique business models emerging among smart banks (fig 6):

1 The "analytical multichannel" bank: Engages customers frequently through various channels while offering personal preferences.
2 The "socially engaging" bank: Interacts with customers who spend their time leveraging information provided via social media.
3 The "digital ecosystem" bank: Offers extended services by leveraging a dynamic network of partners.

[11] http://www.capgemini.com/resource-file-access/resource/pdf/Cloud_Computing_in_Banking.pdf
[12] http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-New-Era-Banking-Cloud-Computing-Changes-Game.pdf

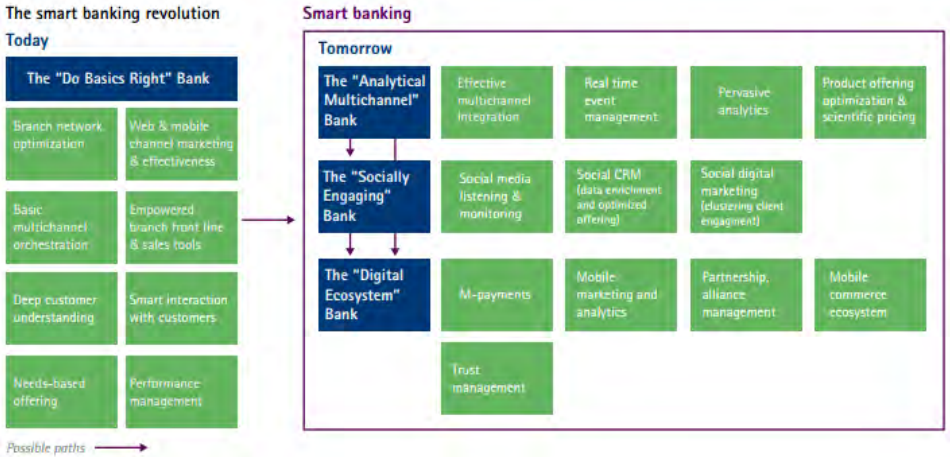


Figure 10 "The smart banking revolution and emerging business models"

As banks adapt to these changes in their competitive and technology environments, Cloud Computing will play a major role to support core banking applications.
Furthermore from Accenture's view, there will be three key trends in banks' use of Cloud Computing, reflecting the different "flavors" outlined in the accompany information panel (fig 7).

Cloud-based financial services offerings will leverage social and mobile media to transform the banking experience and relationship for customers.

Single-tenant private Clouds —through virtualization — will play a pivotal role in core banking, enabling banks to keep control over the location of sensitive customer data. Over time, hybrid Clouds and public sovereign Clouds will enter this domain.

Public Cloud and Cloud-based shared services will dominate non-core and non-differentiated banking activities, from workforce collaboration to document management and even payments.

Figure 11 "Three key trends in banks' use of Cloud Computing"

Regulatory authorities also recognized cloud's role in banks' business transformation, operational efficiency and innovation. They are in various stages of evaluation to provide necessary guidelines in cloud usage. We encountered three examples for these recognitions by regulatory authorities:

- De Nederlandsche Bank (DNB), the Dutch national banking regulator, has approved the use of cloud in the country's financial sector subject to its guidelines. DNB cleared Amazon Web Services for a range of banking services including websites, mobile applications, retail banking platforms, high performance computing and credit risk analysis.
- Monetary Authority of Singapore approved use of cloud subject to completion and approval of Technology Checklist and rights to conduct its own audit.

2.2.3 Cloud model innovations for banks

Based on IBM's experience and research, they identified three main types of model innovation, which can used alone or in combination for Cloud (fig 8):

- Business model innovation
- Revenue model innovation
- Operational innovation

Figure 12 "Model innovations"

Below IBM has for each model innovation several example how banks capture the benefits of Cloud (see fig 9).

Figure 13 "IBM helped leading banks capture the benefits of Cloud"

2.3 Benefits of having Cloud based solutions

Characteristics of Cloud Computing, mentioned in chapter 2.2, could add value to small banks in several ways. We can split the main benefits into three groups: strategic, technical and economic[13].

Cloud Computing provides persuasive savings in IT related costs including lower implementation and maintenance cost. From an economic benefit perspective, business sharpness is determined by the cost an organization incurs. There are a few self-service based, and perceptually cost effective public Cloud Computing solutions. Low-cost price plans advertised by public Cloud vendors have inspired IT departments to gain an insight into costs, resource allocation models and the variety of Cloud models, including public, private and hybrid. Billing is a non-core process for banks, and outsourcing it to a less expensive mediator allows them to route their capital into core technology-based functions[14].

An important strategic benefit is the scalability. If well designed, Cloud solutions empower banks to meet customer demands and scale quickly, dynamic provisioning of computing resources, will save business users and IT experts from engineering the systems for peak loads. Banks can tackle the challenges of security and data privacy by devising a hybrid Cloud where precise data can reside on a private Cloud and computing power can be available on a public Cloud. These private and public Clouds can be integrated in a virtual private network to forge a single scalable hybrid Cloud.

A combination of technical and strategic benefits is:

1 Time to market: With Cloud Computing, time to market can be curtailed from months to weeks or days, depending on the size of a bank.
2 Data Virtualization: Data virtualization is the assimilation of data from multiple and diverse sources across the enterprise or external sources for the on-demand consumption by a wide range of applications in a virtualized manner.
3 Mobility: Many of today‘s corporate world techno savvy workers want to access risk and analytics reports while they are on the move. They see the benefits of accessing the internet on their smart phones and iPad‘s, instantly even in remote locations.
4 Green IT: Organizations can use Cloud Computing to transfer their services to a virtual environment that reduces the energy consumption and carbon footprint that comes from setting up a physical infrastructure. It also leads to more efficient utilization of computing power and less idle time[15].

Another potential benefit, which can be considered as a technical, as well as a strategic benefit, is improved security. Security measures are cheaper when implemented on a larger scale. The centralized nature of as well off and on premise Cloud Computing means the application of security-related processes is cheaper compared to a non-Cloud IT landscape and security updates for the software and infrastructure can be quicker applied. Further, Cloud providers can dynamically reallocate resources for defensive measures, which has advantages for resilience[16].

3 Organizational impact, Risk and Compliance Management for small banks

This chapter describes the literature review, which is relevant for the central research question. The literature is categorized as following:

- Organizational impact
- Risks and compliance management

[13] Zabalza, J., Rio-Belver, R., Cilleruelo, E., Garechana, G., Gavilanes-Trapote, J., “Benefits Related to Cloud Computing in the SMEs”, 6th International Conference on Industrial Engineering and Industrial Management, 2012, p.637–644
[14] http://www.ijarcce.com/upload/2014/february/IJARCCE7E%20%20%20a%20sahil%20%20Cloud.pdf
[15] http://www.capgemini.com/resource-file-access/resource/pdf/Cloud_Computing_in_Banking.pdf
[16] ENISA, “Cloud Computing - Benefits, risks and recommendations for information security”, 28 December 2009

3.1 Organizational impact

New research from the London School of Economics and Accenture—based on a survey of 1,035 business and IT executives, as well as in-depth interviews with more than 35 service providers and other stakeholders—finds that the Cloud will have a strong near-term impact on the majority of organizations[17].

When choosing the Cloud solution the impact(s) on the firms always should be taken into account. Cloud Computing is more than simply a technical paradigm. It can change fundamentally how IT is used and provisioned. The firms' business, organization and technology will be affected. Although Cloud Computing is based on existing technologies and in many cases, existing core skill sets transfer directly to Cloud technologies. IT employees need to develop new skills sets that meet the demand of emerging Cloud job roles. Beside the skills their role is likely to change as well. The role of the IT employees could change from "provider to certifier, consultant and arbitrator" (Yanosky, 2008). IT department also needs to understand which types of services are consumed and needed in Cloud Computing, from as well an operational as financial perspective[18]. In order to ensure that no security, privacy or intellectual property policies are violated, the IT manager has a significant responsibility to identify those risks in using Cloud services and determining the SLA's with the providers of these Cloud services (Sraker & Young, 2011).

What will also change is the system support. Administrators will no longer have complete control of a systems infrastructure; as a result their work will be different because they will have to involve contacting Cloud providers and be depending for them to look into problems (Ali Khajeh-Hosseini e.a., 2012). Their new role comes together with a decrease in authority and control. The IT department can take this change of role as a threat to their corporate culture, in which they had a certain amount of authority, and to the security of their job[19]. But a case study performed by Sarkar and Young (2011) shows that no evidence was found to support the notion that the role and influence of the IT department will erode. Besides the impact on the IT department, not a lot of scientific research is done on the effects on other stakeholders or on end-users.

Ali Khajeh-Hosseini e.a. has mentioned that the accounting department will also be affected, because of the hardware and network infrastructure that will be consumed according to a utility model in the case of an outsourced Cloud, instead of upfront payments[20].

Cloud Computing, Software as a Service (SaaS), and Managed Hosting allow smart pay-as-you-go structures. That can make the process of getting a small organization's infrastructure started, or quickly adopting a solution for an internal application a breeze; but changing from any one of these services is not always an easy process. These services result new ways to move an expense from what would usually land on the capital expenditures (Capex) budget to the operation expenses Opex budget.

Furthermore, Sultan and Van de Bunt-Kokhuis debated Cloud Computing adoption from the perception of a radical innovation and the role of the corporate culture in the adoption and use of Cloud Computing[21]. The authors determine "that Cloud consuming organizations will need to reconsider how they deliver their products and services, view their IT resources and roles, evaluate and calculate their expenditures, value and manage their security, and how they foresee themselves in a, potentially, more environmentally friendly future environment with ethically conscious consumers".

Despite which type of Cloud implementation private, hybrid or a public cloud, the organization's processes will always be impacted (Rebollo, Mellado, and Fernandez-Medina, 2012). Cloud solutions can change the way the work is processed such as the nature of SaaS applications and or of new potentials, such as the flexibility to work with Cloud applications on the road, with mobile devices. Moreover, the off-site

[17] http://www.accenture.com/us-en/outlook/Pages/outlook-online-2011-business-impact-Cloud-computing.aspx

[18] Erbes, J., Motahari Nezhad, H. R., Graupner, S., "The Future of Enterprise IT in the Cloud", Computer, 45(5), p.66–72

[19] Khajeh-Hosseini, A., Greenwood, D., Smith, J.W., Sommerville, I. "The Cloud Adoption Toolkit: supporting Cloud adoption decisions in the enterprise", Software: Practice and Experience, 42(4), 2012, p.447–465

[20] Khajeh-Hosseini, A., Greenwood, D., Smith, J.W., Sommerville, I. "The Cloud Adoption Toolkit: supporting Cloud adoption decisions in the enterprise", Software: Practice and Experience, 42(4), 2012, p.447–465

[21] Sultan, N., Van de Bunt-Kokhuis, S., "Organisational culture and Cloud Computing: coping with a disruptive innovation", Technology Analysis & Strategic Management, 24(2), 2012 p.167–179

Cloud services need other management instead of traditional IT infrastructure (Birla & Sinha, 2011). Erbes, Nezhad, & Graupner stress the importance of an integrative service management function for the management of hybrid Cloud solutions. This business role contains the governance of the whole life cycle of the services; including providers' selection, SLA management, and financial management. To make sure that the business strategy is aligned with the service portfolio. This suggests the responsibility of life cycle of Cloud services that should move to specific 'life cycle' roles within the organization when the Cloud environment becomes complex[22]. Shimba (2012) and Conway and Curry (2012) speak of the processes that are needed for maintaining a Cloud solution. They communicate to the ones included in the management or governance framework 'Information Technology Infrastructure Library' (ITIL). This is the most used framework for IT service management (Sahibudin, Sharifi & Ayat, 2008). Jansen (2010) has analyzed the processes of the ITIL framework for applicability to the Cloud solutions. He has concluded that all of the processes
(from service strategy to service design) are relevant, but need to be adjusted. Moreover, Mather (2009) has mentioned that the security management processes that are required for securing a Cloud solution and also a risk management process is needed to identify, manage and monitor risks (ENISA, 2009). In addition, ISACA's (2012) adaption of COBIT for Cloud Computing delivers some information on the structural changes within the organization. A summary of above can be found below (fig 10).

Figure 10 "Overview of impacts"

3.2 Risks and Compliance Management

This section describes the risk and compliance management in the Cloud and the challenges when banks will move to the Cloud. First these risks will be listed. By discussing Cloud risk management and appropriate risks responses and controls some light is shed on how these risks can be controlled and managed. We assumed that associated risks for banking is also valid for the small banks, therefore no distinction is made between big banks and small banks in this section.

3.2.1 Cloud Computing risks

It is obvious that Cloud Computing provides many (business) opportunities. Reducing costs and improving flexibility are the main business drivers for Cloud Computing. However, Cloud Computing is not without risks. Depending on how Cloud Computing is put in to practice, several (business, technology, regulatory, compliance, continuity) risks exist.
The risks mentioned below are an extraction from ENISA[23] on Cloud Computing. The risks listed below do not follow a specific order of criticality; they are just ten of the most important Cloud Computing specific

[22] Erbes, J., Motahari Nezhad, H. R., Graupner, S., "The Future of Enterprise IT in the Cloud", Computer, 45(5), p.66–72
[23] ENISA, "Cloud Computing - Benefits, risks and recommendations for information security", 28 December 2009

risks identified. The risks of using Cloud Computing should be compared to the risks of staying with traditional solutions. Note that some of these risks also apply to Outsourcing – applying Outsourcing within an organization is also a matter of trust. Knowing what risks are involved, and which controls to apply to these risks will establish a first basis of trust towards the CC provider. A more comprehensive list of risks can be found below (fig 11).

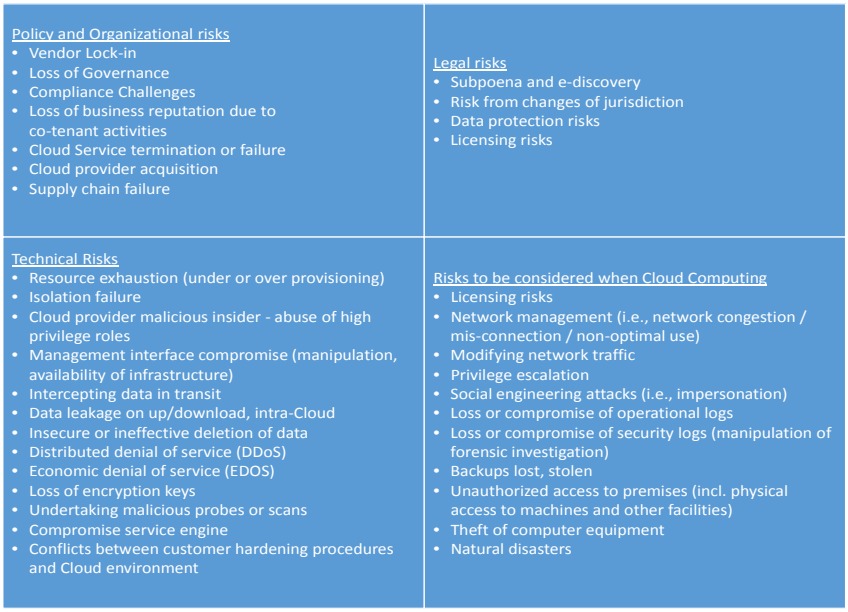


Figure 11 "Comprehensive overview of Cloud Computing risks"

3.2.2 The challenges when moving to the Cloud

Cloud offers a lot of tools and capabilities to resist disintermediation by leveraging social/mobile networking and differentiated bundling capabilities for the changing consumer profile[24]. But when a bank moves into Cloud Computing, there are two prime challenges that must be addressed:

- Security: The confidentiality and security of commercial and personal data and mission-critical applications is preeminent. Banks cannot allow the danger of a security breach. Despite economic strain for business to cut down charges and fervent assurances from Cloud Computing technology providers, security remains a top barrier to Cloud technology acceptance. Ultimately, for Cloud Computing to gain full acceptance within the banking services sector, Cloud services must be harmlessly integrated into existing security platforms and processes.
- Regulatory and compliance: Customers are basically responsible for the security and integrity of their own data, even when it is govern by a service provider. Conventional service providers are subjected to external audits and security certifications. Cloud Computing providers who ignores to undergo this evaluation are signaling that customers can only use them for the most superficial activities. Many banking mangers require that financial data for banking consumers stay in their native country.

[24] http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-New-Era-Banking-Cloud-Computing-Changes-Game.pdf

Certain compliance arrangements require that data not to be mixed with other data such as on shared servers or databases. As a result banks must have a fair understanding of where their data is stored in the Cloud. Security issues which Cloud clients should advert are:

- Privileged user access: There dwell sensitive data that is processed outside the organization inherent risk of security of data because outsourced services bypass the physical and logical IT controls;
- Regulatory compliance: Customers are responsible for the security of their data. Traditional service providers are subjected to external audits and security certifications;
- Data location: When users use the Cloud, they have no knowledge about the hosted data. Distributed data storage is a main reason of Cloud providers that can cause lack of control and that is risky for customers;
- Data segregation: As Cloud is typically in a shared environment in that data can be shared. So there is the danger for data loss. Is encryption available at all phases, and were these encryption patterns designed and tested by experienced professionals;
- Recovery: It is very essential to recover the data when some problem occurs and creates failure. So the main question arises here is that can Cloud provider restore data completely or not, this issue can cause a stalemate in security;
- Investigative support: Cloud technology services are difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers;
- Long-term viability: Ideally, Cloud Computing provider will never go broke or get acquired by a larger company with maybe new policies. But clients must be sure their data will remain available even after such an event.

In the early phases of Cloud Computing adoption, it is expected that banks will own and operate the Cloud themselves with service providers playing more vital role in increasing ownership and control of the Cloud infrastructure as Cloud Computing matures and more rigorous controls become available[25] (fig 12).

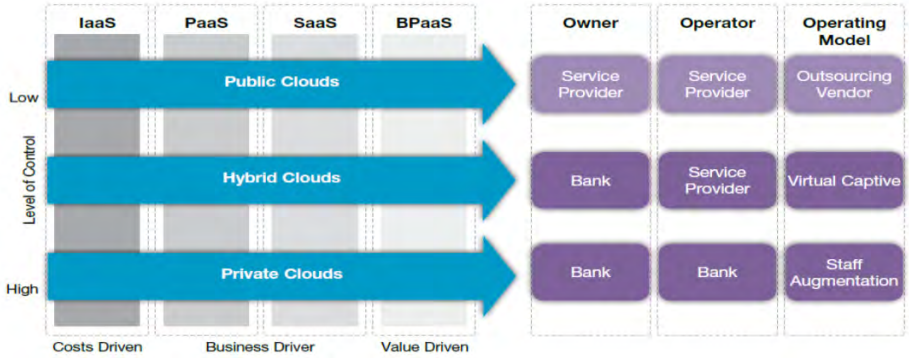


Figure 12 "Cloud Service Delivery Models: How Much Control?"

3.2.3 Risk and Compliance Management

Along with the increasing spread of Cloud Computing concepts and technologies, new fields of activity entailing new risk factors emerge and require new approaches to Risk and Compliance Management (Martens, Pöppelbuß and Teuteberg, 2011; Martens and Teuteberg, 2009).

Risk Management

[25] http://www.capgemini.com/resource-file-access/resource/pdf/Cloud_Computing_in_Banking.pdf

Risk is defined as the possible impact of an event on an organizations asset and the corresponding expected and unexpected consequences that occur as a result (Levin & Schneider, 1997; Stoneburner, Goguen, & Feringa, 2002)[26].
In Cloud settings, risk management is an essential element in the hybrid environment. Next to the traditional management activities for the traditional IT, specific attention should be paid to measures mitigating the risks of excessive provider-dependency, complexity of processes and technology, and assurance.
Cloud Computing has a number of specific characteristics with major an impact on risk profile, such as external data storage and processing, the sharing of IT resources with other customers (multi-tenancy) and the dependency on the public internet. These characteristics imply potential high risks and mitigations concerning multiple dimensions including data, security, privacy, compliance and finance.
Therefore, risks relating to all dimensions should be assessed, mitigating measures defined and responsibilities/accountabilities assigned[27].

Compliance Management
Compliance is integrated in the risk management process through the organizational objectives. An organizational objective is therefore to be in compliance with regulations and laws. Smaller banks, in particular, may lack staff that understand the regulations and know how to put controls in place to comply with those regulations. While the compliance pressure grows, smaller banks and credit unions also find themselves with a bigger target drawn on their backs. LeBoeuf[28], executive vice president of sales and marketing at TraceSecurity, said the big banks traditionally were the prime candidates for breaches, but those institutions have deployed layers of security and have become harder to successfully attack. Accordingly, the smaller institutions have emerged as more tempting targets. Smaller banks and credit unions need to shore up their defenses, but they have found in-house GRC expensive to deploy.
In past years, only a few large corporations used GRC systems, noted Bob Bender, chief technology officer of Founders Federal Credit Union, based in Lancaster, S.C. He said on-premises GRC is a huge system to maintain, requiring multiple administrators. The cost to install a basic, three-module configuration can cost $500,000, with a full deployment running into seven figures, he said[29].

Reference Model
Open issues on Risk and Compliance Management in Cloud Computing are identified by Martens and Teuteberg and they tried to account for most of below issues to increase user awareness:

- Location of the data center causes the applicable jurisdiction (Govindarajan and Lakshmanan, 2010);
- Foreign law may allow government access to the outsourced data (Weinhardt et al., 2009) or restricts or prohibited the export of data to another country (legislation) (Gagliardi and Muscella, 2010);
- Occasionally unknown location of the data center and thus uncertain jurisdiction (Govindarajan and Lakshmanan, 2010);
- Data are spread across multiple data centers or are replicated in a different data center with several jurisdictions (Govindarajan and Lakshmanan, 2010);
- Lack of control over the physical infrastructures (Khajeh-Hosseini, Sommerville and Sriram, 2010), which constrains infrastructure audits;

[26] https://domino.fov.uni-mb.si/proceedings.nsf/0/efbd217bc9216e7cc12578f9007bd359/$FILE/P2_Troshani.pdf
[27] https://www.kpmg.com/NL/nl/IssuesAndInsights/ArticlesPublications/Documents/PDF/IT-Risk-and-Compliance/Orchestrating-New-Paradigm-2.pdf
[28] Dariel LeBoeuf, executive vice president of sales and marketing at TraceSecurity, said regulatory pressure and resource constraints compel mid-tier financial institutions to consider Cloud solutions. Ninety percent of TraceSecurity's customers are in the financial services sector. The company's core market consists of organizations with assets in the range of $100 million to $1 billion.
[29] http://searchitchannel.techtarget.com/feature/Cloud-compliance-management-solutions-in-use-at-small-banks-credit-unions

- Lack of monitoring and auditing approaches and software products (Govindarajan and Lakshmanan, 2010; Heinle and Strebel, 2010);
- Governance issues like people and decision rights are less important in contrast to major concerns about risk and compliance issues (Brandic et al., 2010; Guo et al., 2010).

As a result, they concluded that RCM issues in Cloud Computing have been identified as a major concern but only little research has been conducted yet. Also to find that governance issues are related to compliance, risk and security issues. In particular, it does not become clear how a software solution should be built to tackle these problems. To solve those problems, they introduced a meta-reference model which serves as a regulation framework to structure the application problem and its different aspects (fig 13). It illustrates the grouping and interrelations between the model perspectives KPI, Risk, Compliance and Cloud Computing Services[30].

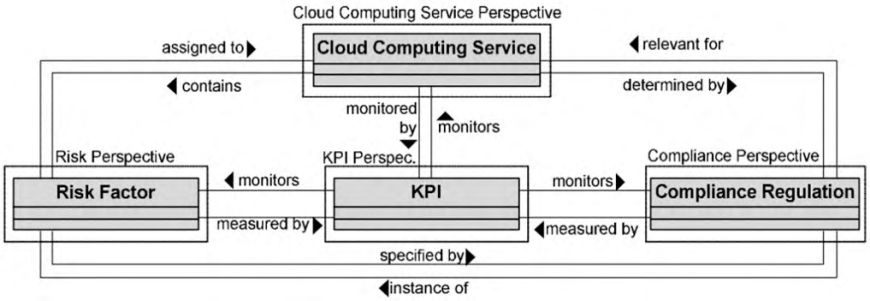


Figure 13 "Meta model for risk and compliance management in the Cloud"

While the assessment and risk management of Cloud Computing is discussed many times in literature, we concluded that no complete process-oriented risk and compliance management framework is developed yet. The best-practice situation is when management uses the COSO ERM framework to identify the ideal configuration of Cloud solution options (i.e., business process, deployment model, and service delivery model) that fits management's risk appetite. By evaluating the Cloud solution candidates in the context of each component of the COSO ERM framework, management can succinctly identify the related risks and desired risk acceptance or mitigation strategies with each Cloud solution scenario (as risks will vary with each combination of options). This evaluation enables management to make prudent risk management and governance decisions in selecting its ideal set of Cloud solution options and creating a well-thought-out Cloud governance program before the Cloud solution is implemented.

The remaining material elaborates on some of the key concepts with respect to evaluating Cloud solution candidates through each of the components of the COSO ERM framework:

- Internal environment: The internal environment component serves as the foundation for and defines the organization's risk appetite in terms of how risks and controls are viewed.
- Objectives setting: Management needs to evaluate how Cloud Computing aligns with the organization's objectives. Depending on the circumstances, Cloud Computing might present an opportunity for the organization to enhance its ability to achieve existing objectives, or it might present an opportunity to gain a competitive advantage, which would require new objectives to be defined.
- Event identification: Management is responsible for identifying the events (either opportunities or risks) that can affect the achievement of objectives. The complexity of event identification and risk assessment processes increases when an organization engages Cloud service providers.

[30] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.231.6718&rep=rep1&type=pdf

- Risk assessment: Management should evaluate the risk events associated with its Cloud strategy to determine the potential impact of the risks associated with each Cloud Computing option. Ideally, risk assessments should be completed before an organization moves to a Cloud solution.
- Risk response: Once risks have been identified and assessed in the context of organizational objectives relative to Cloud Computing, management needs to determine its risk response. There are four types of risk responses: 1. Avoidance, 2. Reduction, 3. Sharing and 4. Acceptance.
- Control activities: The traditional types of controls – preventive, detective, manual, automated, and entity-level – apply to Cloud Computing as well. The difference introduced by Cloud Computing is that some control responsibilities might remain with the organization while certain control responsibilities will be transferred to the CSP.
- Information and communication: To effectively operate its business and manage the related risks, management relies on timely and accurate information and communications from various sources regarding external and internal events. Management should also monitor external information related to its CSP (e.g., financial reports, public disclosures, regulatory filings, industry periodicals, and announcements by fellow Cloud tenants), since certain events impacting the CSP or fellow Cloud tenants might also have an impact on the organization.
- Monitoring: Management must continue to monitor the effectiveness of its ERM program to verify that the program adequately addresses the relevant risks and facilitates achieving the organization's objectives. Effective ERM programs are evolving and dynamic in nature and must be increasingly so given the pace of Cloud Computing's evolution in terms of solution offerings, competitors' adopting the Cloud, and changing laws[31].

3.2.4 Best practices for Cloud solution options

The best-practice situation is when the framework is used to identify the ideal configuration of Cloud solution options (i.e., business process, deployment model, and service delivery model) by evaluating different solutions in the context of each of the components. This evaluation will enable management to make adequate risk management and governance decisions in both selecting an ideal set of Cloud solution options and creating a Cloud governance program (risk management strategies, roles and responsibilities) before the Cloud solution is implemented. A 'tool' to support risk identification is developed by the Cloud Security Alliance (2011). That model is called the Cloud Security Reference Model (fig 14). An organization conducts a gap analysis of Cloud Computing service and deployment models by mapping them against a set of required or recommended security controls and corresponding compliance models (e.g., SOX, HIPAA, PCI). The output of this tool is the 'gaps', the security risks that must be managed. It will also guide organizations to select a Cloud offering that suit their specific needs.

[31] http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf

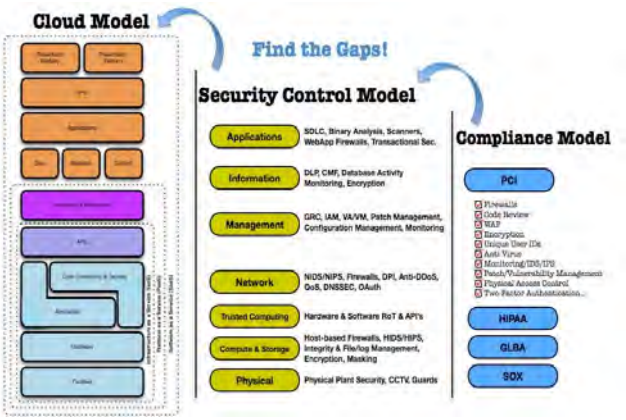


Figure 14 "The Cloud Security Reference Model (CSA, 2011)"

As written, Cloud Computing presents a lot risks and necessary risks management for many organizations, but Deloitte's best practice with their Cloud risk framework (fig 15) can help the organization get to the heart of risks by providing a view on the pervasive, evolving and interconnected nature of risks associated with Cloud Computing. The framework includes governance, risk management and compliance; delivery strategy and architecture; infrastructure security; identity and access management; data management; business resiliency and availability; and IT operations. This framework can also improve efficiency in compliance and risk management efforts and can also be used to develop risk event scenarios that require integrated responses.

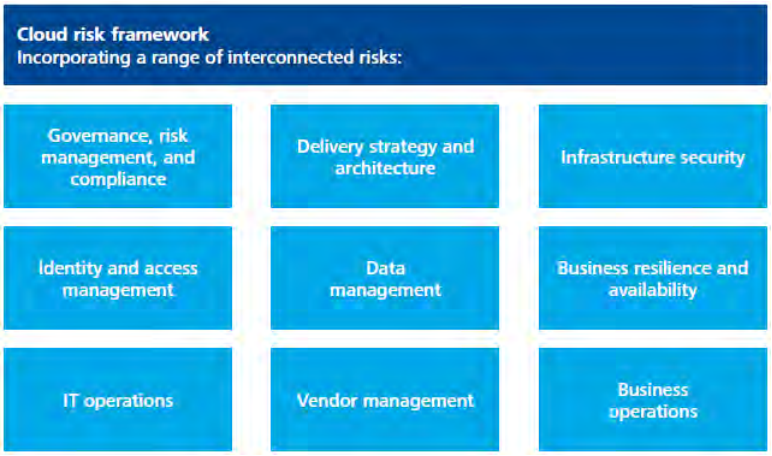


Figure 15 "A recommended approach Cloud risk framework from Deloitte"

To be more effective, the framework should be customized to include regulatory, geographic, industry and other specific issues that impact the organization. As IA modifies its organizational risk framework and guides the risk conversation with IT and the business, the following issues pertaining to infrastructure security, identity and access management and data management should be taken into account:

- Infrastructure Security — Companies should verify that Cloud providers have acceptable procedures in areas such as key generation, exchange, storage and safeguarding, as flawed security could result in the exposure of infrastructure or data;

- Identity and Access Management — Organizations should consider how their authorization and access models will integrate with new Cloud services and assess whether they are using appropriate identity and authorization schemes;
- Data Management — Because organizations may have to relinquish control over their data to Cloud providers, it is crucial that they fully understand how data will be handled in the Cloud environment[32].

4 Case study: Interviews and Process

In addition to the literature, we performed research on theoretical concepts and models by interviewing experts. The goal of the interviews with experts is to receive answers for our main research question:

> *"Which are the main arguments for management control when adopting Cloud solutions for small banks and which strategic, organizational and managerial objectives for compliance and risk management need to be addressed?"*

Each interview contains 19 questions and is categorized around three aspects:
- The business case: how can it be developed for Cloud Computing?
- The organizational impact: what happens to the organization when Cloud Computing is adopted?
- Risks: what are the Cloud related risks and how can they be managed?

We interviewed the following experts.

Expert	Company	Size company in FTE (+/-)	Function	Interviewed on
1	Small bank	100	Head of Internal Audit	Wednesday 25 March 2015
2	Small bank	250	Director Information Security Department	Friday 7 November 2014
3	Accountancy and Consultancy	3000	Partner	Wednesday 11 March 2015
4	Accountancy and Consultancy	3000	Advisor	Tuesday 3 March 2015
5	Small bank	250	IT Security & Governance Architecture	Tuesday 17 February 2015
6	Small bank	250	Department Manager ISM & ORM	Tuesday 18 February 2015

5 Case study: Analysis and conclusions

In this chapter the results of the interviews are discussed for each of the following aspects:
- The business case: how can it be developed for Cloud Computing?
- The organizational impact: what happens to the organization when Cloud Computing is adopted?
- Risks: what are the Cloud related risks and how can they be managed?

5.1 The business case: how can it be developed for Cloud Computing?

Five out of six interviews – In general, the experts commented that business case can be developed in a traditional way, by adding the Cloud Computing component. Such as Cloud is a solution, just as another form of outsourcing, but the essentials for the business case remains the same. It covers aspects like

[32] http://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-internal-audit-and-risk-of-Cloud-computing-022614.pdf

costs, efficiency, risks, and controls. And with Cloud Computing, the firm does not have to develop and maintain software and systems anymore.

[Expert 5] stated that the threats related to IT security are evaluating very rapidly and these also need to be considered. The information shared between the malicious parties is very fast and effective. Protection against the IT security threats is getting harder and harder. The information sharing and gathering against these malicious parties, and the methodology and tools they are using is essential in order to have the appropriate protection. Cloud base security services such as continuous vulnerability scanning, sharing database of the networks and systems that the attackers are actually using during their activities and their new malwares using zero-day vulnerabilities are the key points of today's IT security strategies.

[Expert 1] stated that there are considerations that should be understood for each public Cloud business case:

- When leveraging a public Cloud service, the acquiring organization no longer needs to invest significant capital for building their own data center capability, which can include buildings, HVAC, storage, and servers.
- Acquisition costs, such as program management, contracting, and systems engineering, can vary substantially for Cloud Computing capabilities.
- Moving applications to Cloud environments may require porting and the use of proprietary application programming interfaces (APIs). Some Cloud providers do not support standard structured query language (SQL) for their database offerings. Applications that rely upon this standard would need to be ported.
- Moving applications to the Cloud will require funds for integration and testing, which could be substantial.
- Data migration costs may be driven by the movement of vast amounts of data over a secure network and may require mapping relational data to a non-relational database management system. Many Cloud Computing vendors charge a fee for uploads and downloads—uploading vast amounts of information could be costly.
- Traditional data center IT differs significantly from community and public Clouds in the analysis of fixed versus variable costs.

5.2 The organizational impact: what happens to the organization when Cloud Computing is adopted?

All the experts have another opinion on organizational impact. But in general, five out six experts, they agreed on that the organizational impact on the firm is significant.

[Expert 1] stated that adopting Cloud Computing will impact the organization, especially the banking environment:

- Customer relationships should be redefined
- The overarching and most disruptive impact of Cloud Computing will be how it redefines the relationship between consumers and their providers of banking products and services. Cloud Computing will make these services more convenient, more accessible, easier to use, and more personalized to the individual's needs and lifestyle. This is both a threat and an opportunity as it remains to be seen whether it is banks that lead this change— or, increasingly, non-banking entrants.
- Cloud Computing will steadily progress at all levels of the stack
- Scale of IT infrastructure will also influence Cloud Computing adoption. Newer and smaller banks built on client/server architectures have less overlapping legacy systems and infrastructure, and will therefore be quicker to adopt Cloud technology higher up the stack.
- Larger banks currently tend to focus on virtualization, and may be culturally more resistant to expanding their adoption at the higher levels. That said, some large banks are already picking specific activi-

ties and radically Cloud-enabling them with SaaS and BPaaS—underscoring the fact that Cloud Computing adoption is not an all-or-nothing choice.
- Non-banking Cloud-based competitors will keep up the pressure
- Rather than being technologically innovative, the emerging generation of Cloud-based, socially-driven money management tools are customer services and experience innovators. They will continue to ramp up efforts to win customers not just from banks, but from each other. Banks must, therefore, continue to respond to these competitive pressures in order to avoid disintermediation-by investing in capabilities around social media, analytics, and targeted product and service bundling.
- Collaborative Cloud-based shared services will emerge between banks
- In a similar way to telecoms sharing network infrastructure, banks will start to collaborate to pool non-differentiated activities into joint ventures (JVs) using "private Clouds" within a closed group of banks. These JVs could provide shared services that interact with customers in more engaging ways while simultaneously freeing banks from the burden of routine transactions.
- Cloud-enabled collaborative bundling will expand across and beyond financial services
- Banks' growing use of Cloud Computing to enable dynamic and responsive bundling will trigger an industry-wide drive to make third-party financial and non-financial products interoperable in the Cloud. This will enable a bank to operate as an integrator and aggregator of a diverse array of products, using its differentiated Cloud-based bundling capability as the "glue."
- Payments in the Cloud will be a key focus
- Consumers' migration to digital mobile and contactless payments will affect buying habits, channels and customer service in all markets, and will impact all consumer-facing industries. The preparations for when these services reach critical mass are intensifying convergence and competition between banks, retailers, telecoms, card issuers and other participants in the payments value chain, especially around the consumer interface and digital mobile payments channel.

[Expert 2] stated that there are lots of benefits of Cloud Computing, but there might be also some negative impacts.

Benefits:
- Organizations can focus more on their business and not on managing data centers,
- Many operational tasks can be automated,
- Expanding the business quickly,
- The new applications can be developed faster,
- The new infrastructures can quickly be adopted to support new applications,
- Reduce the costs such as IT equipment and staff
- Users can access information from anywhere anytime

Negative Impacts:
- Performance on shared infrastructure can be inconsistent
- Security of the Cloud infrastructure is always a threat
- Not all workloads may be ready for the Cloud
- Legal and compliance requirements may not be met

[Expert 5] stated that organizations get the external vulnerability management service, advance malware analysis and reputational databases feed for malicious systems and networks are taking into consideration the level of the trust of the service company. The trustworthiness between the parties is significant in terms of data sharing and data processing. Especially during the advance malware analysis service, companies are sending their files, some of them with the highest confidentiality level, to processing companies systems. Additional to this, the companies providing Cloud base vulnerability management services are storing the details of the vulnerabilities of customers. Confidentiality of the data has the top level priority for the customers.

[Expert 6] stated that Cloud Computing should not give a big impact to the organization, although the IT landscape might change significantly (resources, in house develop appl, infra, etc).

5.3 Risks: what are the Cloud related risks and how can they be managed?

All the experts have the same perspective on Cloud related risks. They listed the risks such as: security, availability, integrity, confidentiality, privacy, and legal risks.

[Expert 1] stated that risks arise due to Cloud:

- Change management is out of control
- While managing your own software and systems upgrades can take more time, it does at least give you the control to decide how and when it is implemented, so allowing you to prepare for the changes.
- Cloud Computing gets much more expensive as the business scale up
- Cloud Computing gets the companies and start-ups up and running quickly, however, as the demand grows Cloud Computing gets much more expensive than the in-house IT solutions.
- External network issues become risks of business continuity
- When the companies host their services in house are immune from external network issues. For example, there may be DOS attacks to the website, reduced bandwidth of internet channels or regulatory blockage on some services do not affect an internally hosted core business application. When using Cloud Computing the scope of business continuity has to span these issues.

[Expert 2] explains that these risks can be managed by the following solutions:

- A reliable and reputable provider should be selected.
- While preparing the SLAs, all risks mentioned above should be considered and covered.
- Before going live extensive tests should be made which includes security, functionality, disaster recovery etc.
- All users should be trained and make sure that they all aware of above mentioned risks and the security controls they should apply.
- Third party audit and penetration reports of Cloud provider should be reviewed regularly etc.

5.4 Main observations

Numerous studies and articles have been published with regard to major trends in Cloud solutions for banking operations, risk objectives addressed using Cloud Computing and best practices.

We noted that Cloud service models offer small banks the option to move from a capital-intensive approach to a more flexible business model that lowers operational costs. The key to success lies in selecting the right Cloud services model to match business needs.
Cloud's distinction benefits and their usage are expected to increase significantly. Therefore in the foreseeable future, Cloud solutions will be omnipresent. However we noticed that the adaption of Cloud solutions at small banks is slower than others. Currently Cloud solutions are still in the minority of all applications in small banks.

This observation was confirmed through our interviews with experts and employees of small banks. We noted that due to their background, experience, and work environment, the majority of experts think in their own silos and limitations. Furthermore, we noted that not all small banks' experts are aware of the benefits of using Cloud solutions to maximize their bank's potential. This prevents the proper definition and management of the risks associated with Cloud Computing.

We also noted that many small banks are less than halfway to have a Cloud strategy in place with controls and security remaining primary concerns. Small banks are facing a reality that their current governance and organization are not ready yet to tackle Cloud solution choices. Most of the small banks have an idea about Cloud Computing and Cloud solutions, but still there is mix-up about the real definition of Cloud Computing and how to deal with the risks. As a result, in the future this might lead to many projects where the risks during and after the implementation of the Cloud project are not managed properly how it should be. In other words, to close this sub chapter, this can be considered as a major business risk!

6 Revisiting central research question

Cloud Computing offers a number of important benefits to the organizations, such as significant cost savings and operational efficiencies. Small banks in general seek for outsource and Cloud-based solutions as a way to save money, be compliant with regulations and compensate for limited in-house resources. At the same time small banks are hesitating to adopt and implement Cloud solutions because of the security concerns, privacy issues and complexity barriers. Barriers can obstruct cloud solutions. These can be overcome by applying a holistic approach, supported by leadership at the top. Therefore the objective of our thesis is to assist small banks with the adoption of Cloud solutions. This chapter describes our main conclusion which is based on our main research question and underpinning sub questions (recalled from chapter 1.3).

Our main research question was:

> *"Which are the main arguments for management control when adopting Cloud solutions for small banks and which strategic, organizational and managerial objectives for compliance and risk management need to be addressed?"*

Our sub questions were:

1. *Descriptive: Which major trends in Cloud solutions are relevant for Banking and IT Operations, and which risks domains are being introduced that are relevant for banks?*
2. *Analysis: Which risks objectives and control areas need to be addressed when using Cloud Computing for small banks?*
3. *Synthesis: Which key objectives, controls for risk management and compliance can be considered when implementing Cloud based solutions by small banks?*

Our conclusions and answer to the sub questions are as follows regarding Cloud-based solutions for small banks:

Which major trends in Cloud solutions are relevant for Banking and IT Operations, and which risks domains are being introduced that are relevant for banks?

(Small) banks will need to have essential changes to be able to achieve and sustain high performance in the future. As the banks adapt to these changes in their competitive and technology environments, Cloud Computing will play a major role. Cloud's combination of low cost and high scalability, unlimited processing power and storage, exceptional agility and speed to market, and variable pay per-use cost structures all support the qualities that banks will need to compete and win in the future.

A major trend for adaptation of Cloud based solutions for small banks is the lack of knowledge and expertise for maintaining (major) applications on the required technical and quality level. For instance, we noticed that small banks are more focused on costs and revenues. Trends and major developments in the IT domain are usually not followed. Therefore also some migrations to Cloud solutions are made on initiative of a third party – to which already a number of business or IT services are outsourced.

Another driver for using Cloud solutions is to maintain a level playing field between smaller banks and large-sized institutions. In this perspective, SaaS vendors basically help keeping small banks alive, because while using Cloud solutions they are able to deliver the same products or keep interest margins on an appropriate level.
Cost cutting is also a main driver for small banks. Usually the underlying reason is decreasing of costs for usage of IT services or decreasing of IT staff costs.

Which risks objectives and control areas need to be addressed when using Cloud Computing for small banks?
We noted from the result of DNB's self-assessments over 2013 that assessing the status of external service providers' internal controls and confirming that external service providers comply with legal and regulatory requirements and contractual obligations is a general concern for all banks. Therefore the banking industry needs to self-assess whether they are appropriately monitoring and managing compliance risk associated with third parties. It is also important to recognize that, when banks deal with third-party risks that they are also dealing with a continuous evolving environment. We identified the following risk drivers for internal control at third parties:

- Insufficient assurance over the service provider's control framework and control performance,
- Failures of mission-critical systems during operation,
- IT services failing to meet the service specifications,
- Failures and degradations of service from the provider not identified in a timely manner,
- Reputational damage caused by provider service performance degradation.

From the literature, we noted that the types of risks (e.g., security, integrity, availability, and performance) are the same with systems in the Cloud as they are with non-Cloud technology solutions. And an organization's level of risk and risk profile will in most cases change if Cloud solutions are adopted (depending on how and for what purpose the Cloud solutions are used).

From literature and interviews we were able to identify the most important risks. We noted that in general the following risks fall under a number of major headings such as security, regulatory and compliance, contractual arrangements, supplier lock-in, and information governance issues.

We conclude that data security is a fundamental issue, also for small banks. Many banking regulators require that financial data for banking customers are stored in their home country. Certain compliance regulations require that data should not be intermixed with other data, such as on shared servers or databases. With the migration to a Cloud solution also sensitive data might be transferred outside the bank environment. As a result, small banks must have a clear understanding of where their data resides in the Cloud and which risks will be involved. Small banks should be aware whether sensitive data will be shared, since bank regulators are more and more focusing on third-party provider risks and there is a strong focus on privacy regulation. The bank security professionals know how to secure their infrastructure against the threats, but they are not able to secure the Cloud environment.
Furthermore Cloud Computing makes it harder for small banks to be sure to be compliant with industry and government regulations. Usually small banks have internal controls in place, but moving to a Cloud-based solution will mean to transfer the responsibility of implementing and maintaining some controls to the Cloud vendors. IT auditors, IT and legal experts offer advice on how to stay in compliance even when their applications reside in the Cloud. In practice, it is difficult to get a hold on the standing of regulatory compliance in a Cloud solution.
Moreover the main concern of Cloud Computing is found in its major benefit; the ability to outsource the IT to an adequate Cloud provider. Moving to the Cloud sounds initially like a wise decision, but with a move to the Cloud one also gives up the in-house control of the traditional IT department to an "trusted' Cloud service provider. Therefore it is very important not to assume that your Cloud vendor's standard

terms and conditions will fit your requirements. Also as a smaller bank, you might find it difficult to negotiate good terms with a large Cloud vendor. Moreover, even in case you may have a good SLA, but if the vendor's Cloud goes down, what happens to business continuity?
These risks can be mitigated by starting with a due diligence examining the vendor's contract to see if the vendor's standard contract is sufficient for your internal and external compliance needs. If not, the small bank should determine its need to negotiate, to increase its comfort level. Smaller business can find leverage, too, if it represents a new industry for a Cloud vendor that wants to expand its market. For business continuity the best strategy might be to use multiple Clouds for backup assurance.
We noted from the literature that Clouds Security Alliance (CSA) released new Cloud Controls Matrix (CCM) V3.0.1 and this CCM, which provides a controls framework in 16 domains, are cross-walked to other industry-accepted security standards, regulations, and controls frameworks to reduce audit complexity. This will allow cloud providers to be more transparent in the baseline assessment process, helping accelerate the implementation process where cloud users will be able to make smart, efficient decisions. We expect the new versions to have an enormous and positive impact on the cloud industry[33].

Which key objectives, controls for risk management and compliance can be considered when implementing Cloud based solutions by small banks?
There is no single Cloud Computing services model that will meet all the technology requirements. Small banks therefore need to select the right service, deployment, and operating models to address corresponding security and compliance concerns that come with Cloud Computing.
Following four points can be considered as best practices for Cloud implementations for small banks:

1 Small banks should conduct a full risk assessment before setting up a contract with any Cloud provider. They should not look only at the provider's security and compliance activities, but also how stringently they apply their policies to their subcontractors, how easily the bank can migrate their data to another platform at the end of a contract, and how likely the provider is to drop offline or go bankrupt. Cloud standards bodies have already published frameworks and benchmarks which bank can use to conduct their assessment.
2 Small banks should look at how their own security works in a Cloud environment, how comprehensive is their existing security capability, and can they adequately protect their data and their user identities beyond the perimeter? Techniques like authentication and encryption are also vital.
3 Small banks should implement a strong ongoing governance framework. Gather information from providers and from their own systems, and monitor for security events and compliance with accepted best-practice and specific regulation/standards where appropriate. They should check whether providers are fulfilling their SLAs and contracted obligations. Small banks should also plan for how they will respond to and remediate problems.
4 Small banks should get involved in how Cloud security develops.

In the long term, we expect that small banks will make an application portfolio mix with on premise and Cloud-based services delivered across a combination of private, hybrid, and public Cloud-based deployment models with the share of Cloud services gradually increases in the service mix. We also expect that private Clouds will increasingly become the deployment model for Cloud services among small banks, because it gives the bank the full control through ownership and operations of their successfully implemented Cloud systems.

[33] https://cloudsecurityalliance.org/media/news/csa-releases-new-ccm-caiq-v3-0-1/

7 References

Articles

- Ahmad, R., & Janczewski, L., "Governance Life Cycle Framework for Managing Security in Public Cloud: From User Perspective", IEEE International Conference on Cloud Computing (CLOUD), 2011, p.372 – 379
- Aliyu, A.A., Tasmin, R.B.H.J., "The Impact of Information and Communication Technology on Banks' Performance and Customer Service Delivery in the Banking Industry", International Journal of Latest Trends Finance and Economic Sciences, Volume 2, No. 1 March 2012, p.80-90
- Almorsy, M., Grundy, J., & Ibrahim, A. S., "Collaboration-Based Cloud Computing Security Management Framework", IEEE International Conference on Cloud Computing (CLOUD), 2011, p.364–371
- Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S., "A Survey on Security Issues in Cloud Computing", 2011
- Behl, A., & Behl, K., "An analysis of Cloud Computing security issues", World Congress on Information and Communication Technologies (WICT), 2012, p.109–114
- Bhopale, S.D., "Cloud Migration Benefits and Its Challenges Issue", IOSR Journal of Computer Engineering (IOSR-JCE), 2013, p.40-45
- Carroll, M., Van der Merwe, A., & Kotze, P., "Secure Cloud Computing: Benefits, risks and controls", Information Security South Africa (ISSA), 2011, p.1–9
- CFR 228.12 [Title 12 -- Banks and Banking; Chapter II -- Federal Reserve System; Subchapter A -- Board of Governors of the Federal Reserve System Part 228 -- Community Reinvestment (Regulation Bb); Subpart A – General]
- Chaput, S. R., & Ringwood, K., "Cloud Compliance: A Framework for Using Cloud Computing in a Regulated World", Cloud Computing, 2010, p.241–255
- Chen, Z., & Yoon, J., "IT Auditing to Assure a Secure Cloud Computing", Proceedings of the 2010 6th World Congress on Services, p.253–259
- Cloud Consumer Banking Point of View, Institute for Business Value, IBM, 2014
- Dahbur, K., Mohammad, B., & Tarakji, A. B., "A survey of risks, threats and vulnerabilities in Cloud Computing", Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, p.12:1–12:6
- ENISA, "Cloud Computing - Benefits, risks and recommendations for information security", 28 December 2009
- Erbes, J., Motahari Nezhad, H. R., Graupner, S., "The Future of Enterprise IT in the Cloud", Computer, 45(5), p.66–72
- Fan, C. K., Chiang, C.-M. F., & Kao, T. L., "Risk Management Strategies for the Use of Cloud Computing", International Journal of Computer Network and Information Security(IJCNIS), April 2012, p.50.
- Guo, Z., Song, M., & Song, J., "A Governance Model for Cloud Computing", International Conference on Management and Service Science (MASS), Aug 2010, p.1–6
- Huang, C.-C., & Hsieh, C.-C., "Does Cloud Computing Matter?", Networking IT and Services Value in Organizations, 2011, p.75–80
- Khajeh-Hosseini, A., Greenwood, D., Smith, J.W., Sommerville, I. "The Cloud Adoption Toolkit: supporting Cloud adoption decisions in the enterprise", Software: Practice and Experience, 42(4), 2012, p.447–465
- Khajeh-Hosseini, A., Sommerville, I., Bogaerts, J., & Teregowda, P., "Decision Support Tools for Cloud Migration in the Enterprise", IEEE International Conference on Cloud Computing (CLOUD), 2011, p.541–548

- Knode, R., “BP Fuels Cloud Computing Interest”, whitepaper, 2009 (http://www.trustedCloudservices.com/Individual-Case-Studies/bp-fuels-Cloud-computing-interest)
- Koning, E., Brink, M. ten, Baveco, M., Presentation DNB self-assessment results 2013 on seminar “Security: the next level ...", 30 January 2014, p.13
- Maurya, B. K., “Cloud Computing: Exploring the scope”, 11 May 2010
- (http://arxiv.org/ftp/arxiv/papers/1005/1005.1904.pdf)
- Mell, P., Grance, T., “The NIST Definition of Cloud Computing – Recommendations of the National Institute of Standards and Technology”, National Institute of Standards of Technology, U.S. Department of Commerce, special publication 800-145 (http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf)
- Office of the Privacy Commissioner of Canada, Introduction to Cloud Computing, fact sheet (https://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf)
- Olson B., Lacey C., Almad A. “Banking’s ‘Sweet Spot’ in the Cloud” BAI Banking Strategies
- Sultan, N., Van de Bunt-Kokhuis, S., “Organisational culture and Cloud Computing: coping with a disruptive innovation”, Technology Analysis & Strategic Management, 24(2), 2012 p.167–179
- Vohradsky, D., “Cloud Risk – 10 Principles and a Framework for Assessment”, ISACA Journal “Privacy and the Cloud”, volume 5, 2012, p.31–41
- Yin, R.K., (2009), Case Study Research Design and Methods
- Zabalza, J., Rio-Belver, R., Cilleruelo, E., Garechana, G., Gavilanes-Trapote, J., “Benefits Related to Cloud Computing in the SMEs”, 6th International Conference on Industrial Engineering and Industrial Management, 2012, p.637–644

Websites

- http://about.bloomberglaw.com/practitioner-contributions/are-financial-institutions-ready-for-Cloud-computing/
- http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.231.6718&rep=rep1&type=pdf
- https://cloudsecurityalliance.org/media/news/csa-releases-new-ccm-caiq-v3-0-1/
- http://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-internal-audit-and-risk-of-Cloud-computing-022614.pdf
- http://www935.ibm.com/services/multimedia/Cloud_Computing_for_Banking__Janvier_2013.pdf
- http://www.aitegroup.com/
- http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-New-Era-Banking-Cloud-Computing-Changes-Game.pdf
- http://www.accenture.com/us-en/outlook/Pages/outlook-online-2011-business-impact-Cloud-computing.aspx
- http://www.capgemini.com/resource-file-access/resource/pdf/Cloud_Computing_in_Banking.pdf
- http://www.compact.nl/en/articles/C-2013-4-Derksen.htm

Jaarrekening assurance bij materiele gebreken in onvervangbare IT Controles

André Sanders

Van origine registeraccountant, met werkervaring bij KPMG in audit en bij General Electric in Finance, sloot ik me enige jaren gelden aan bij de schare van studenten voor de IT Audit opleiding aan de VU, om me ook op dit vakgebied bij te laten spijkeren. Na studieafronding is mijn band met de VU intact gebleven, en verleen ik met enige regelmaat hand -en spandiensten aan Abbas en zijn team. Ik werk als docent aan de Arnhem Business School van de Hogeschool van Arnhem en Nijmegen.

1 Aanleiding

We schrijven het jaar 1995. De internet revolutie is nog niet uitgebroken. Financiële verantwoordingen zijn nog het product van mainframes met grootboekpakketten die in isolatie van de primaire processen van het bedrijf opereren en nog op grote schaal (semi-) handmatig gevoed worden. De IT audit heette nog EDP audit. De accountant controleert de mechaniek en de inhoud van het grootboeksysteem, als zelfstandig controle object. Parafenlijsten en facturen zijn nog belangrijke controlebronnen.
In deze omgeving brengt het NIVRA (de voorloper van het NBA) dat jaar geschrift 64 uit met als titel: "Electronic Data Interchange, beheersing en controle". Het is de controleerbaarheid van de geautomatiseerde gegevensverwerking, de audit trail, die het NIVRA in dit geschrift aanspreekt, en waarbij de accountant wordt aangewezen bij een combinatie van:

- ontoereikendheid van de onvervangbare interne “EDI” controles en
- materieel belang voor de jaarrekening

dwingende conclusies te verbinden aan de strekking van de controleverklaring.

Het toereikend zijn van de controleerbaarheid van de geautomatiseerde gegevensverwerking wordt verbonden met de werking van onvervangbare interne “EDI” controles. Deze onvervangbare “EDI” controles vormen klaarblijkelijk een ondergrens voor de controleerbaarheid van een jaarrekening. Duidelijk toch ? …

Sinds het verschijnen van NIVRA geschrift 64 … is IT steeds meer een onvervangbaar element van de accountantscontrole geworden:

- de fysieke wereld van parafenlijsten en afgetekende facturen is nu onderdeel van een virtuele, papierarme wereld,
- waarin naast werknemers ook externe stakeholders via openbaar toegankelijk internet inloggen op een gedistribueerde IT infrastructuur van het bedrijf,
- met in het systeem verankerde authenticatie en functiescheiding toegang krijgen tot de applicaties en data,
- van met elkaar geïntegreerde primaire bedrijfsprocessen,
- waar via geautomatiseerde IT controles (betaal)fiattering van kritische transactiestromen met hoge volumes gebeurt,
- en waarvan de financiële mutaties rechtstreeks het grootboek inlopen.

Er is de afgelopen 20 jaar dus nogal wat veranderd. De IT afhankelijkheid van bedrijven is enorm gestegen en daarmee is, ook voor de accountant, het belang van adequaat werkende IT controles sterk toegenomen. Daarbij zijn de elementen van onvervangbare interne controle in hoofdlijnen nog dezelfde, te weten: audit trail van primaire vastleggingen van transacties naar de financiële verantwoording, handhaving van functiescheidingen in de meest materiële transactiestromen, randvoorwaarden voor de volledigheid van contractuele rechten en verplichtingen, bewaring van de “kroonjuwelen”, waarborgen voor de continuïteit. Hun toepassing is nu echter in de IT wereld verankerd en dient door werkende IT controles gewaarborgd te worden.

2 Probleemstelling en onderzoeksvraag

Gegeven de toegenomen relevantie van IT voor de controle van de jaarrekening mag verondersteld worden, dat de accountant en de IT auditor normen(kaders) of richtlijnen zijn aangereikt die verduidelijken hoe een (minimale) ondergrens voor de werking van onvervangbare IT controles als basis voor een deugdelijke grondslag kan worden bepaald.
Dit is echter niet het geval:

- niet over consequenties van niet werkende onvervangbare controles
- niet over onvervangbare controles in het algemeen en

- ook niet voor de verbijzonderde vorm van onvervangbare IT controles.

De NV COS en andere bronnen zoals het recente studierapport van NBA, NOREA en TUACC "Jaarrekening controle in het MKB: IT audit geïntegreerd in de controle-aanpak"[34], en publicaties van de AFM[35], PCAOB[36] en ITGI[37] beschrijven uit te voeren IT controles maar geven geen ondergrens in de werking aan, laat staan mogelijke gevolgen voor de oordeelsvorming.

Formulering onderzoeksvraag

Het kennelijk ontbreken van normen of richtlijnen voor het omgaan met jaarrekening assurance bij materiele gebreken in onvervangbare IT controles leidt tot de volgende probleemstelling:

> *Welke onvervangbare IT controles dienen minimaal adequaat te werken om een hieruit resulterende beperking in de verklaring bij de jaarrekening (van een willekeurige onderneming) te vermijden, en hoe kan de IT auditor in dit kader bijdragen aan reductie van het audit risico?*

Voor een adequate beantwoording van de onderzoeksvraag zijn de volgende deelvragen geformuleerd:

1 Wat zijn onvervangbare IT controles en hoe kritisch zijn gebreken in hun werking ?
2 Welke IT controles dienen uit assurance oogpunt minimaal adequaat te werken?
3 Hoe kan de IT Auditor de bijdrage aan het reduceren van het audit risico verbeteren?

De eerste deelvraag is inventariserend, de beide anderen zijn analyserend van aard.

Methode van onderzoek

De munitie voor het onderzoek komt voort uit uitgebreide literatuurstudie en gesprekken met ITACA docenten. Hiervan uit heb ik een eerste versie van de scriptie geschreven met daarin een initiële beantwoording van de onderzoeksvraag met conclusies en aanbevelingen.
De uitkomsten van de literatuurstudie heb ik uitgewerkt met behulp van de onderzoekaanpak van Yin[38], en in de vorm van een enquête aan een 20-tal experts (RA 's en RE 's) voorgelegd. De enquête resultaten zijn vervolgens geanalyseerd en aan de experts teruggekoppeld, en op individuele basis zijn de conclusies via korte interviews geverifieerd.

Afbakening en definities

Waar in deze afstudeeropdracht wordt gesproken over de accountant wordt bedoeld: een registeraccountant, in de functie van openbaar accountant. Waar in deze afstudeeropdracht wordt gesproken over de IT auditor wordt bedoeld: een register EDP-auditor ingeschreven bij de beroepsorganisatie NOREA.
Centraal in het onderzoek staat de IT auditor als de deskundige op het vakgebied en in die hoedanigheid wordt ingehuurd door de accountant. Hun gezamenlijk object van onderzoek is de controle van de jaarrekening van een willekeurige onderneming.
Het jaarrekening audit risico of controlerisico "is het risico dat een accountant een onjuist oordeel tot uitdrukking brengt wanneer de financiële overzichten een afwijking van het materieel belang bevatten. Controlerisico is een functie van de risico's op een afwijking van materieel belang en het ontdekkingsrisico[39]". De accountant past risicoanalyse toe om dit audit of controlerisico te mitigeren, waarbij ik opteer voor een controleaanpak die maximaal gebruik maakt van effectieve maatregelen van interne beheersing.
Tot de maatregelen van interne beheersing behoort een stelsel van IT controles gericht op het inperken van de inherente IT risico 's van de onderneming:

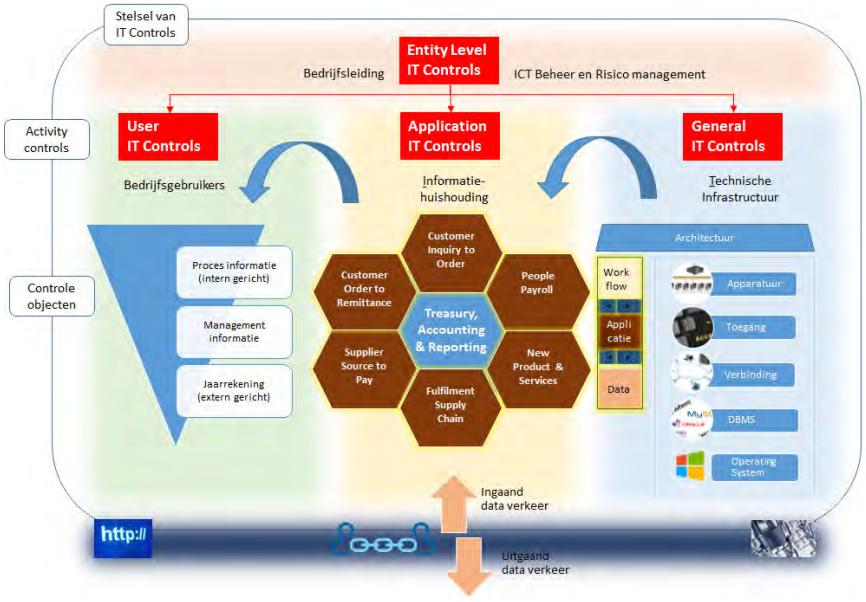
[34] Schellevis en Van Dijk - "Jaarrekening controle in het MKB: IT audit geïntegreerd in de controle-aanpak", april 2014
[35] AFM - Uitkomsten onderzoek kwaliteit wettelijke controles Big 4-accountantsorganisaties, sept 2014
[36] PCAOB Staff Audit Practice Alert No. 11, October 2013
[37] ITGI - IT Control Objectives for Sarbanes Oxley, 2nd Edition, 2006
[38] Robert K. Yin – "Case study research, design and methods", 4th edition 2009
[39] NBA – "HRA"- NV COS Begrippenlijst, januari 2014

- IT Entity Level controles = door het management geïnstitutionaliseerde vormen van aansturing en bijsturing van strategische IT doelen, vooral gericht op het optimaliseren van business alignment, veranderprojecten en GRC
- IT General controles & Application controles = IT controles gericht op de beheersing van de reguliere procesuitvoering (tactisch/operationeel) op de kwaliteitsaspecten exclusiviteit, integriteit, controleerbaarheid en continuïteit
- IT User controles = Gedocumenteerde gebruikerscontroles op de IT output, veelal in de vorm van cijferanalyse op financiële informatie. Cijferanalyse omvat de controlemiddelen cijferbeoordeling, verbandscontrole en toetsing aan normatieve gegevens.

De interne beheersing van een onderneming bestaat – uit optiek van de accountant - uit maatregelen van vervangbare en onvervangbare interne controle. Onvervangbare interne controle betreft maatregelen van interne controle die de accountant niet door eigen actie kan controleren en niet – door gegevensgerichte controle – kan vervangen.
De hiertoe behorende onvervangbare IT controles worden in deze afstudeeropdracht alleen op hun vermijdbare gebreken onderzocht.

3 Deelvraag 1: Wat zijn onvervangbare IT controles en hoe kritisch zijn gebreken in hun werking?

Aan de basis staat een model dat het stelsel van IT controles verbindt met controle objecten van de jaarrekening audit. De IT controles zijn daarbij analoog de ruime interpretatie van ISACA/ITGI[40] onderverdeeld in Entity Level en Activity controls:

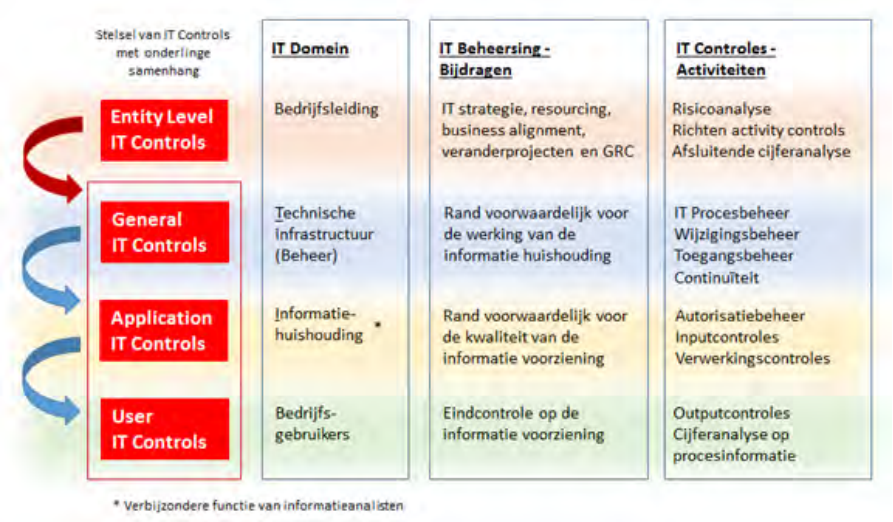


De controleobjecten van de jaarrekening zijn opgedeeld naar bedrijfsdomeinen:
- De bedrijfsgebruikers (groene kolom) ontvangen vooraf overeengekomen procesinformatie uit de informatiehuishouding (gele kolom), waaruit voor interne doeleinden op periodieke en ad-hoc basis

[40] ITGI - IT Control Objectives for Sarbanes Oxley, blz 56, 2nd Edition, 2006

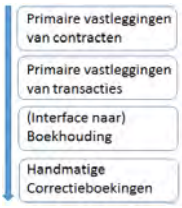
management informatie wordt samengesteld. Conform geldende regelgeving, verantwoordt het bedrijf periodiek externe financiële en overige bedrijfsinformatie, waaronder de jaarrekening;
- In de informatiehuishouding (gele kolom) zijn de bedrijfsprocessen in ERP modules (in bruin) organisatie-breed gestandaardiseerd en in vergaande mate met de "boekhouding" (in blauw; "Treasury, Accounting & Reporting") geïntegreerd;
- De technische infrastructuur (blauwe kolom) dient met technisch beheer de betrouwbaarheid van applicaties, data en workflows te waarborgen.

De bedrijfsdomeinen staan -voor wat betreft het product jaarrekening- met elkaar in een klant-aanbieder relatie. De kwaliteit van hun dienstverlening is sterk afhankelijk van een goed werkende IT voorziening. Die hangt op zijn beurt af van de werking van IT controles die de betrouwbaarheid van financiële data moeten waarborgen.
De -voor de jaarrekening relevante- IT controles vormen op hun beurt een stelsel van IT controles, met hieronder weergegeven onderlinge samenhang:



Wat geldt voor het interne beheersingsproces dat de kwaliteit van een jaarrekening moet waarborgen, geldt evenzo voor de jaarrekening audit die op de werking van de interne beheersing steunt. Hiermee is het belang van de werking van IT controles voor de jaarrekening audit geïllustreerd.

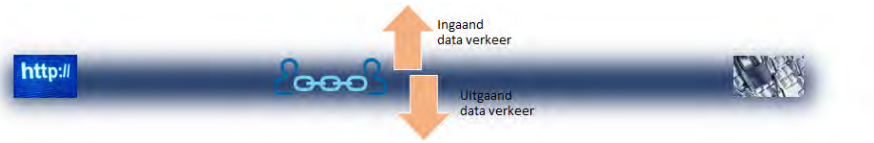
Waar de accountant in het verleden een keuze had een jaarrekening "om de computer heen" (gegevensgericht) en "door de computer" (systeemgericht) te controleren, was "om de computer" heen controleren op een zeker moment (door het gebrek aan fysiek bewijs, in de keten) geen optie meer[41]. Voorheen werd de financiële informatie voor een jaarrekening uit afzonderlijke bronnen samengesteld, zoals hiernaast getoond. Tegenwoordig zijn een groot deel, zo niet alle bronnen, geïntegreerd in één informatiesysteem, één controleobject.



De accountant moet daarom met zijn controlemix van maatregelen dóór de computer, waarbij een adequate beoordeling van het interne beheersingsbeleid gericht op de werking van IT controles kritisch is.

[41] Gerritse - "IT-ontwikkelingen en de IT-auditfunctie" – De IT-Auditor nummer 4 2013

Het model “Stelsel van IT controles” bevat aan de onderkant de volgende toevoeging die refereert naar de relatie naar het ingaande en uitgaande dataverkeer met stakeholders van het bedrijf, inclusief werknemers die via vaste of mobiele datalijnen toegang willen krijgen tot applicaties en data:



Onder invloed van internet technologie en andere IT innovaties (outsourcing middels cloud computing, BYOD) is het dataverkeer van bedrijven met de buitenwereld sterk toegenomen en zijn informatiesystemen steeds meer gedeeld/gekoppeld. Het inherent hogere risico van misbruik van applicaties en data door derden moet via IT controles worden voorkomen.

Ook binnen de virtuele muren van het bedrijf is sprake van meer IT afhankelijkheid. Onder invloed van digitalisering, procesintegratie, ketensamenwerking en virtualisatie is de invloed van IT op de inhoud van primaire bedrijfsprocessen, en daarmee ook op de jaarrekening, veranderd van een ondersteunende naar een primaire, bepalende rol.

Ondanks de groeiende verwachtingskloof tussen business vraagzijde en IT aanbodzijde, zijn wezenlijke IT veranderingen gerealiseerd, waardoor het relatieve belang van interne beheersing van IT processen sterk is toegenomen; een verder te definiëren fundament van interne controle verankerd in IT systemen en processen is tegenwoordig een onvervangbaar onderdeel van de interne beheersing, dat de accountant op werking dient te controleren.

Welke zekerheden/mogelijkheden biedt de toegenomen IT voor de jaarrekeningcontrole ?
- Wat is onder invloed van toegenomen automatisering gebeurt met de IT controles zelf ? Geautomatiseerde controles in robuuste ERP applicaties kunnen sterk bijdragen aan effectieve interne beheersing van processen, op voorwaarde dat de ondersteunende beheersorganisatie op orde is … want een keten is zo sterk als zijn zwakste schakel;
- Hoe verhoudt zich de gestegen effectiviteit van vooral IT Application controles tot de dynamiek in de te controleren processen ? Deze vraag kan alleen situationeel -van case tot case specifiek- worden beantwoord, maar dezelfde basisvoorwaarde geldt;
- Biedt de inzet van data-analyse om kwalitatieve IT audit bevindingen, vooral op het gebied van functiescheidingen, met behulp van event logs van het ERP systeem te vertalen naar kwantitatieve/financiële verschillen, een “remedie” zodat de accountant met een volledig gegevensgerichte controleaanpak de jaarrekening kan controleren ?

Het antwoord daarop is nee, gezien de navolgende belangrijke beperkingen:
- Voorlopig staan nieuwe data-analyse technieken nog in hun kinderschoenen, zijn in financieel opzicht te duur, en is de business case is (nog) niet goed genoeg
- Van groter belang is: data-analyse is zo goed als de kwaliteit van de brondata:
    - bij de ontwikkeling van standaardprogrammatuur, en nog meer bij maatwerk, krijgt het aspect controleerbaarheid in vergelijking met de andere kwaliteitsaspecten minder prioriteit[42]. Gevolg is dat event logs vaak nog van onvoldoende kwaliteit zijn: onvolledig, onjuist en in opzet niet gedocumenteerd;

[42] Haasnoot-Bezverhaya - "Controleerbaarheid en kwaliteit van event logs", De IT-Auditor nummer 2 2013

- de integriteit van de brondata is alleen bij werkende onvervangbare IT controles gewaarborgd, uitzonderingssituaties daargelaten waarin de accountant/IT auditor het restrisico moet meewegen in de bewijskracht die aan de data-analyse wordt ontleend.

De bestudeerde literatuur bevat slechts in beperkte mate specifiek onderzoek van en directe verwijzingen naar onvervangbare IT controles, en biedt dan in het algemeen weinig informatie over gevolgen voor de aanpak en de conclusie van de jaarrekening audit, enkele uitzonderingen daargelaten die dan ook de relevantie van het probleem bevestigen.[43] [44] [45] In het recente studierapport van NBA, NOREA en TUACC[46] worden compenserende maatregelen voor gebreken in IT controles benoemd, duidelijk wordt dat compensatie niet altijd mogelijk is = IT controles onvervangbaar zijn, maar de gevolgen voor de audit zijn niet verder uitgewerkt; alsof het een hete aardappel is … ?

> "Een minimale set IT General controles is nodig om de toegangsbeheersing, het change management en het slechts met corporate applicaties aan de corporate database kunnen toevoegen van data, te realiseren … de logische toegangsbeheersing is ingericht op het niveau van IT General controles en van IT Application controles …De accountant moet toetsen op afwijking …**Onder negatieve gevolgen valt bij de jaarrekening-controle vooral te denken aan beperkingen van de controleerbaarheid**. [10] "

Recente kwaliteitsonderzoeken van AFM naar jaarrekeningcontroles wijzen op lacunes in de controle van de interne beheersing en daarin opgenomen IT controles; er bestaan generieke gebreken in controles van functiescheidingen (autorisatie) en op door IT gegenereerde data, en specifieke ses[47] roepen een beeld op van een accountant die het relatieve belang van IT audit en van werkende IT controles onderschat. [48]

> "-De accountant heeft onvoldoende kennis van IT om de organisatie goed te kunnen controleren, maar past het controleteam daar niet op aan
> -De AFM vindt dat het stelsel van kwaliteitsbeheersing meer moet afdwingen dat externe accountants, indien nodig, IT-deskundigen inzetten voor hun accountantscontrole; dit geldt zowel voor deskundigen die binnen de accountantsorganisatie aanwezig zijn als voor externe deskundigen.
> -De accountant heeft onvoldoende de beheersingsomgeving van organisatie in kaart gebracht, inclusief de relevante informatiesystemen, onderliggende infrastructuur en IT beheersprocessen
> -De accountant kiest daarom soms ten onrechte een sterk gegevensgerichte aanpak
> -In deze aanpak wordt wel impliciet gesteund op beheersingsmaatregelen in de informatiesystemen, zonder dat deze getest zijn"27

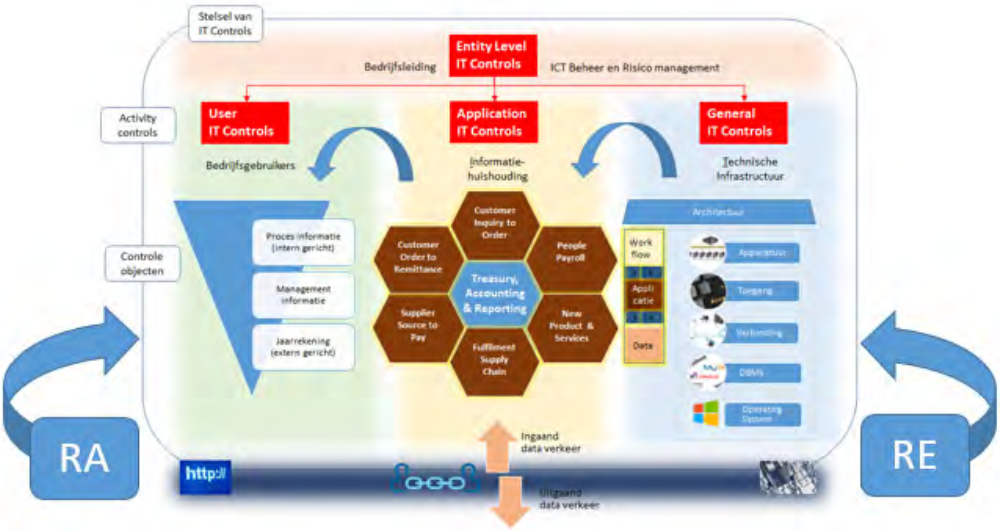
Daarmee is de jaarrekening assurance in een gevaarzone beland, want:

[43] Kloosterman en Snoeker - "Informatietechnologie en interne beheersing", De IT-Auditor nummer 2 2013
[44] Van Bommel, Van Goor, Peek en Winterink - "De betekenis van IT-auditing voor de jaarrekeningcontrole ontrafeld!", MAB oktober 2006
[45] Rabe en Johan - "IT-audit en MKB-controle", Accountancynieuws nr. 20, november 2010
[46] Schellevis en Van Dijk - "Jaarrekening controle in het MKB: IT audit geïntegreerd in de controle-aanpak", april 2014, tabellen 4 t/m 6 op pagina's 44 t/m 46
[47] AFM - Uitkomsten onderzoek kwaliteit wettelijke controles Big 4-accountantsorganisaties, september 2014: voorbeeld van controle cliënt H, pagina 73/74
[48] Schellevis - "Financial Audit Support: integrated auditaanpak"- NOREA symposium mei 2014

- de accountant die materiële gebreken in onvervangbare IT controles niet ontdekt, geeft mogelijkerwijs een onjuiste verklaring af bij een niet controleerbare verantwoording;
- de accountant die materiële gebreken in onvervangbare IT controles onderkent maar "compenseert" met aanvullende gegevensgerichte maatregelen, verleent met een goedkeurende verklaring mogelijkerwijs schijnzekerheid aan gebruikers van de jaarrekening.

4 Deelvraag 2: Welke IT controles dienen uit assurance oogpunt minimaal adequaat te werken?

De IT auditor verifieert opzet, bestaan en werking van het stelsel van IT controles voor zover jaarrekening audit relevant. Uitgangspunt voor de IT auditor is de specifieke inrichting en omgeving van de gecontroleerde en zijn financiële verantwoording; te allen tijde is - in samenspraak met de accountant - maatwerk nodig om een raamwerk van (onvervangbare) IT controles te bepalen dat adequaat de IT gerelateerde bedrijfsrisico 's afdekt die tot materiële fouten in de jaarrekening kunnen leiden.

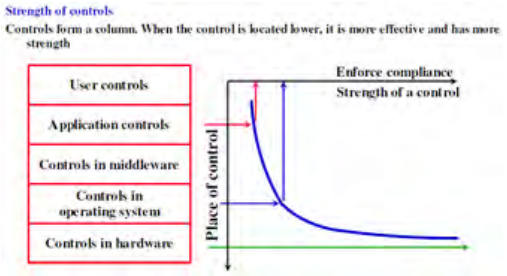


Aan het maatwerk – het IT controleprogramma - gaat een proces van gezamenlijke beoordeling van de ondernemingssituatie vooraf, met volgende complicaties:

1 De accountant en de IT auditor analyseren het stelsel van IT controles vanuit een verschillend perspectief, waaruit een verschil in aanpak resulteert;
   - de accountant komt van links – start met een risicoanalyse vanuit de jaarrekening, werkt dan terug (naar rechts) om met een controlemix van maatregelen, juist voldoende om zekerheid voor een oordeel te bereiken
   - de IT auditor komt van rechts - start bij de beoordeling van de overkoepelende architectuur, werkt dan de lagen van de infrastructuur af (naar links) vanuit het perspectief van een gebruiker die remote inlogt om na het doorlopen van een mix van IT controles toegang tot de applicatie te krijgen en de gekoppelde database te kunnen raadplegen of muteren.

2 De accountant en de IT auditor hebben een andere interpretatie van de sterkte van IT controles, waarmee controlezekerheid te bereiken is;

- de accountant hecht relatief grote waarde aan controlezekerheid uit gebruikerscontroles, uit raadpleging van documentatie en interviews met verantwoordelijke managers, en uit informatie van applicaties die één op één te vertalen zijn naar posten van de jaarrekening. Vanuit deze optiek zijn bevindingen uit IT General controles een “ver van mijn bed show”;
- de IT auditor legt meer nadruk op de rand voorwaardelijke beveiligings- en continuïteitaspecten van de infrastructuur, middels isolatie van domeinen, encryptie van netwerk communicatie, het voorkomen van inbreuk op toegangspaden tot applicaties en data, en ondersteunende maatregelen van IT beheer.[49]



3 De accountant beschikt over een uitgebreidere gereedschapskist aan controlemiddelen, en de IT auditor heeft daar niet altijd zicht op. Het gaat hier om gegevensgerichte maatregelen zoals cijferbeoordeling en verbandscontroles.

4 De accountant controleert met een materialiteitsblik, die voor de IT auditor veelal moeilijk te doorgronden is, omdat 1) de bepaling van een fouttolerantie een subjectief element kent en 2) de fouttolerantie kan variëren naar gelang welke post van de jaarrekening, of welk transactieproces, beoordeeld wordt.

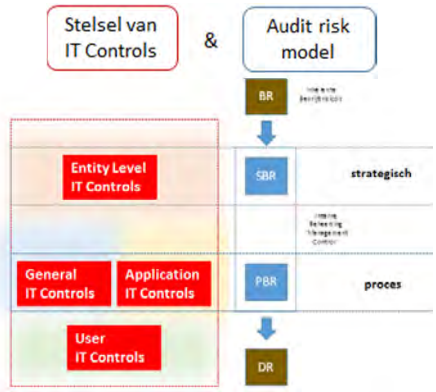
Conclusie:
de accountant en de IT auditor zijn in een jaarrekening audit – gezien de bovenstaande verschillen - geen natuurlijke partners, maar dat laat onverlet dat de accountant IT controles dient af te dekken.
De besluitvorming over het IT controleprogramma zal dan ook een trechtermodel moeten doorlopen, waarbij:

- in de opstartfase (pre-audit) de wederzijds perspectieven en motieven voor geplande maatregelen open uitgewisseld worden
- in alle fasen van de audit, zowel de instelling van de partners als de inhoudelijke uitvoering van de controle principle-based is
- in een zo vroeg mogelijk stadium van de audit overeenstemming wordt bereikt over een minimale set van werkende IT maatregelen, binnen het stelsel van IT controles van de gecontroleerde, zonder welke de accountant geen goedkeurende verklaring bij de jaarrekening kan afgeven.

Op de zoektocht naar mogelijk onvervangbare IT controles is het van belang om aansluiting te houden tussen het stelsel van IT controles en het audit risk model dat aan de basis staat van de controle van de jaarrekening.

Het verband tussen strategische inrichting van de interne beheersing en het controleobject, de jaarrekening, is indirect. Daarentegen hebben proces controles (de General en Application IT controles) een directe relatie met posten van de jaarrekening, hun werking is meer relevant voor het bereiken van de algemene en de IT audit doelstellingen.

[49] Paans - "IT-auditor, repressief of juist preventief optreden?", Presentatie op Vurore Seminar, 18 april 2008



Zijn strategische controles volledig vervangbaar? Voldoen werkende proces controles voor het bereiken van voldoende controlezekerheid ?
Menig accountant zal –indien gedwongen tot een keuze- hierop bevestigend antwoorden, en redeneren dat het merendeel van de controledoelstellingen in theorie kunnen worden bereikt in geval van slechte strategische controles en goede procescontroles[50], maar … dan moeten wel eerst juiste strategische beslissingen zijn genomen over de richting en de inrichting van de interne beheersing en de specifiek daarin opgenomen procescontroles. Daarop zal de IT auditor terecht hameren.

COSO 2013[51], en in het verlengde daarvan COBIT[52], gebruik ik als normenkaders voor de selectie van voor de jaarrekening relevante IT controles, die op mogelijke onvervangbaarheid worden beoordeeld:

Organisatorische basisvoorzieningen in IT: Entity level controls
Entity Level IT controles zijn onderdeel van de algemene beheersactiviteiten voor IT. Deze controles zijn de directe verantwoordelijkheid van het management van de onderneming. Het is cruciaal dat het management hieraan zélf adequaat invulling geeft, en niet naar de CIO of de leiding van de IT Beheer organisatie afschuift.

De navolgende IT basisvoorzieningen zijn naar mijn mening onvervangbaar voor de jaarrekening audit, met volgende motivatie:

- Voorwaarde voor de controleerbaarheid van IT activiteiten is dat het management van de onderneming de IT organisatie richt;

[50] Van Leeuwen & Wallage - "Moderne controle-benaderingen steunen op interne beheersing", MAB maart 2002
[51] Grant Thornton LLP – "New COSO framework links IT and business process", summer 2014
[52] ITGI - IT Control Objectives for Sarbanes Oxley, 2nd Edition, 2006

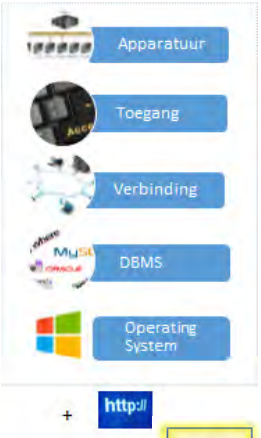
- In de dynamische omgeving van een bedrijf is effectief risicomanagement onvervangbaar; de IT activiteiten en controles zijn tijdig aan te passen aan externe verandereisen en aan interne proceswijzigingen. Zonder deze functie loopt IT achter de feiten aan, is sprake van onvoldoende alignment;
- Omwille van de controleerbaarheid van de jaarrekening, dient de bedrijfsleiding IT kritische processen en functies te monitoren.

Basisvoorzieningen in logische toegangsbeveiliging en wijzigingsbeheer: General IT controls

De General IT controles zijn onderdeel van de procescontroles. Door IT ondersteunde procescontroles zijn van groot belang voor de jaarrekening audit. Daarbij zijn de General IT controles rand voorwaardelijk voor het bestaan, de opzet en de werking van Application IT controles. Dit geeft al een indicatie dat General IT controles onvervangbare elementen van interne beheersing kunnen bevatten.

Op de zoektocht naar mogelijk onvervangbare IT controles voor de jaarrekening audit behandel ik eerst de objecten van de Technische infrastructuur van IT. Daarna ga ik in op de verschillende categorieën van beheersactiviteiten.

De objecten van de Technische Infrastructuur en hun relevantie voor de jaarrekening audit worden hieronder behandeld:



- Het in-en uitgaande verkeer via internet raakt de buitenste schil van de infrastructuur. Bij werkende General IT controles (de binnenste schillen), zal de toegang via internet geen risico voor de jaarrekening inhouden;
- Het operating system voert geen voor de jaarrekening relevante transactie/dataverwerking uit. Windows Active directory is van belang voor de toegangscontrole (met SSO). Bij werkende General IT controles (de binnenste schillen) zal het operating system echter geen direct risico voor de jaarrekening vormen;
- Hardware en netwerk staan relatief ver van de transacties af en vormen bij goedwerkende General IT controles geen direct risico voor de jaarrekening;
- Het DBMS dekt centraal databasebeheer en datacommunicatie af, waarbij te onderzoeken is welke rol het DBMS heeft, welke databestanden voor welke applicaties worden gebruikt, en waar ze opgeslagen worden.

De meest relevante objecten zitten in de binnenste schil, het zijn de toepassingsapplicaties en de data, omdat gebruikers hiermee de transacties genereren die in de jaarrekening uitmonden. Het risicoprofiel van applicaties is hoger bij: 1) maatwerk, versus standaard oplossingen, vanwege het aspect integriteit; 2) uitbesteed, versus in intern beheer, vanwege het aspect controleerbaarheid; 3) shared, versus intern, vanwege het aspect exclusiviteit.

Workflow tools zorgen voor interfaces tussen applicaties, wanneer van een ERP standaard wordt afgeweken. Het risicoprofiel van een workflow is inherent hoog, omdat het maatwerk betreft en vaak grote datahoeveelheden te verwerken zijn.

De navolgende IT basisvoorzieningen zijn naar mijn mening onvervangbaar voor de jaarrekening audit, met volgende motivatie:

- Toepassingsprogramma's en databases (opslag en transport) moeten, individueel en in hun rol/samenspel binnen het informatiesysteem, aan minimumeisen voor IT controles op beveiliging en integriteit voldoen, zodat aan de kwaliteitsaspecten exclusiviteit, integriteit en controleerbaarheid invulling kán worden gegeven;
- De controleerbaarheid van de jaarrekening kan niet voldoen zonder adequaat wijzigingsbeheer op kritische applicaties. Voorbeeld is het behouden van de audit trail (was => wordt) bij de overgang naar een nieuwe programma versie;
- De controleerbaarheid van de jaarrekening kan niet zonder afdoende logische toegangsbeveiliging middels identificatie en authenticatie. Voorbeeld: indien het password beleid binnen een onderne-

ming niet op orde is, kan authenticatie van individuele gebruikers slechts beperkt plaats vinden. Hierdoor is (achteraf) veelal niet meer vast te stellen of functiescheiding heeft gewerkt. Als paswoorden "publiek" bekend zijn, is niet vast te stellen of doorgevoerde mutaties door bevoegde personen zijn gebeurd, en functievermenging tot materiele fouten (en/of waarde onttrekkingen) heeft geleid;
- In voor de jaarrekening kritische (massa)processen zijn goed werkende functiescheidingen onmisbaar om materiële fouten van/door -niet geregistreerde- waarde onttrekkingen te voorkomen.

Onder “Manage data” (COBIT DS11) heeft ITGI enkel IT controles geselecteerd die het kwaliteitsaspect continuïteit afdekken, waarbij het belang van het aspect integriteit van databases mogelijk tekort schiet; de beveiliging van kritische data vereist:
- Data security controles die voorkomen dat databases via ongeautoriseerde paden, om de applicaties heen, benaderd en gemuteerd worden.

Conclusie uit de beoordeling is dat General IT controles onvervangbare elementen van interne beheersing bevatten. Dit heeft tot gevolg dat:
- General IT controles niet enkel rand voorwaardelijk te testen zijn als op de “onderliggende” Application IT controles gesteund wordt, want
- de IT auditor dient in de jaarrekening audit onvervangbare General IT controles dwingend op hun werking te testen !

Werking van IT controles in kritische massa-processen: Application IT controls
De Application IT controles zijn onderdeel van de procescontroles. Door IT ondersteunde procescontroles zijn van groot belang voor de jaarrekening audit. Daarbij zijn de Application IT controles (steunend op werkende IT General controles) rand voorwaardelijk voor User IT dependant manual controles. Dit geeft al een indicatie dat Application IT controles onvervangbare elementen van interne beheersing kunnen bevatten.
Application IT controles bestaan in vele verschijningsvormen, en dekken, elk voor de specifieke applicatie, details van individuele kwaliteitsaspecten van de informatieverwerking af die -op zich staand- grotendeels vervangbaar zijn. Voorbeeld is een Limit check op een debiteurenkrediet, dat de gebruiker ook handmatig kan vaststellen met het huidige debiteurensaldo en het orderbedrag in kwestie.

Een opdeling van Application IT controles naar de fase van informatieverwerking[53] is:
- Input controles: gericht op juiste en volledige invoer in de applicatie; zoals checks op een veld, geldigheid, redelijkheid en teken;
- Verwerkingscontroles: gericht op juiste en volledige verwerking van de input; zoals totaalcontroles (# in = # verwerkt), volledigheidscontrole;
- Output controles: gericht op de juistheid en volledigheid van de output; zoals controle van verbanden, volledigheidscontrole, totaalcontrole;
- Integriteitscontroles: gericht op de blijvende integriteit van een applicatie –zoals preventieve controle op code changes- en/of op applicatie data -monitoring in de verwerking, transport en opslag;
- Audit trail controles: gericht op de controleerbaarheid van verwerkte transacties; zoals logging van transacties, events/verstoringen, toegangsgegevens gebruikers, veranderingen in parameterinstellingen
- & overkoepelend voor alle fasen: controles op de Logische toegangsbeveiliging, indien deze specifiek op applicatie niveau is bepaald.

Application IT controles worden belangrijker voor de controle van de jaarrekening naarmate:

[53] GTAG 8 – Auditing Application Controls, January 2009

- de omvang en de complexiteit van de processen groter wordt, want handmatige controle is dan geen optie meer; te tijdrovend/kostbaar en te grote foutenkans
- de controles kritische controleverbanden afdekken, of totaal omspannend zijn, waarmee een totaal proces op efficiënte en effectieve wijze gecontroleerd of beoordeeld kan worden
- alternatieve controlemiddelen -zoals data analyse- niet beschikbaar of vanwege proces complexiteit niet mogelijk zijn, of niet efficiënt te realiseren zijn.

Deze navolgende IT basisvoorziening kan naar mijn mening onvervangbaar zijn:
- In de procesbeheersing van dynamische massa transactiestromen – vooral in de noodzakelijke verbanden van de geld- en goederenbeweging- kunnen Application IT controles zo kritisch zijn dat gebreken de controleerbaarheid van de jaarrekening kunnen beperken. Voorbeeld: een niet juist werkende 3-way match controle in het inkoopproces van een discount webwinkel – in combinatie met complexe leveringsvoorwaarden, zoals variabele prijsafspraken - kan leiden tot materiele afwijkingen in de hoeveelheden en de inkoopprijzen waartegen de voorraden in de balans gewaardeerd staan.

In navolging van het geconstateerde bij General IT controles, geldt ook voor Application IT controles– indien op applicatie niveau geregeld- dat:
- De jaarrekening niet zonder afdoende logische toegangsbeveiliging van de applicatie middels identificatie en authenticatie kan.

Voor kritische applicaties zijn werkende audit trail controles en de integriteitscontroles van de betreffende applicatie –in aanvulling op de informatie uit het wijzigingsbeheer- onvervangbaar, inclusief hun logging:
- De controleerbaarheid van de jaarrekening kan niet voldoen zonder bewijs van blijvende werking – gedurende de controle periode- van de kritische applicatie.

Conclusie uit de beoordeling is dat Application IT controles onvervangbare elementen van interne beheersing bevatten, met daarbij de kanttekening dat de inrichting van de controle sterk afhankelijk is van de specifieke inrichting en omgeving van de gecontroleerde en zijn financiële verantwoording.

Leidraad voor een controleprogramma van onvervangbare IT controles:
Ik concludeerde aan het einde van het vorige hoofdstuk dat de jaarrekening assurance in een gevaarzone is beland;
- “een verder te definiëren fundament van interne controle verankerd in IT systemen en processen is tegenwoordig een onvervangbaar onderdeel van de interne beheersing, dat de accountant op werking dient te controleren”
- “de accountant die materiële gebreken in onvervangbare IT controles niet ontdekt, geeft mogelijkerwijs een onjuiste verklaring af bij een niet controleerbare verantwoording” óf “de accountant die materiële gebreken in onvervangbare IT controles onderkent maar "compenseert" met aanvullende gegevensgerichte maatregelen, verleent met een goedkeurende verklaring mogelijkerwijs schijnzekerheid aan gebruikers van de jaarrekening”.

Het fundament van IT controles die uit assurance oogpunt minimaal adequaat dienen te werken – de onvervangbare IT controles – is in dit hoofdstuk onderzocht.
COSO 2013, en in het verlengde daarvan COBIT, zijn daarbij als normenkaders gebruikt voor de selectie van voor de jaarrekening relevante basisvoorzieningen in IT.
Resultaat van dit onderzoek is een leidraad voor een controleprogramma van onvervangbare IT controles -verdeeld naar Entity Level IT controles, General IT controles en Application IT controles.

Ik spreek hier over een leidraad, omdat het controleprogramma van onvervangbare IT controles –evenals de overige maatregelen van de controle van een jaarrekening- steeds maatwerk is gebaseerd op de specifieke inrichting en omgeving van de gecontroleerde en zijn financiële verantwoording.

Het opstellen van het controleprogramma is dus een "principle-based job" die niet zonder de expertise en het professional judgement van de IT auditor kan.

Indien bij uitvoering van het controleprogramma materiële gebreken in de onvervangbare IT controles worden vastgesteld, is de controleerbaarheid van -delen van- de financiële verantwoording in geding, en schrijven de controlestandaarden voor dat de accountant geen goedkeurende controleverklaring kan en mag afgeven.

5 Deelvraag 3: Hoe kan de IT Auditor de bijdrage aan het reduceren van het audit risico verbeteren?

IT audit competenties zijn noodzakelijk van om tot een deugdelijke grondslag voor de controleverklaring bij de jaarrekening te komen:

A Niet alleen is de invloed van IT op de inhoud van primaire bedrijfsprocessen, en daarmee ook op de jaarrekening, veranderd van een ondersteunende naar een primaire, bepalende rol, maar zoals hierboven geschetst is IT zelf een risico factor van belang geworden[54], een reden temeer om expertise -van de IT auditor- in te schakelen om het inherent risico van IT voor de jaarrekening te beoordelen

B De IT realiteit is object van de jaarrekening audit geworden, waarbij verificatie van onvervangbare IT controles -onder meer- zekerheid geven over de werking van kritische functiescheidingen

C In haar meest recente audit heeft de AFM[55] met enige regelmaat geconstateerd dat de accountant steken liet vallen in het verkrijgen van een deugdelijke grondslag voor IT audit bewijs. Deze vaststelling is geen verrassing voor de doorsnee IT auditor, en tegelijk ernstig gezien de groeiende relevantie van IT. Hieruit resulteert als verbeteringsvoorstel: => naar mijn mening dient de inschakeling van een IT auditor bij de controle van de jaarrekening van een “IT-afhankelijk” bedrijf niet aan de individuele accountant overgelaten worden, maar dienen verplichte consultatie van een IT auditor en adequate naleving van gemaakte afspraken binnen het stelsel van kwaliteitscontrole door het NBA verplicht te worden vanwege reductie/beheersing van het audit risico.

De bijdrage van de IT auditor heeft naast het aspect van IT expertise en kennisoverdracht ("wat") een belangrijke tactische component ("hoe") die moet voorkomen dat zijn controle bevindingen onvoldoende gelag (met g) vinden. De samenwerking tussen IT auditor en accountant dient in beide opzichten (dus "wat" en "hoe") te verbeteren en dat in combinatie draagt bij aan reductie van het audit risico.

Op zoek naar opties voor verbetering van de samenwerking bestaan twee sporen:

- Focus op hard skills -zoals expertise, procedures, tools- als succesfactoren voor IT audits[56]. Deze benadering sluit aan op de wederzijdse expertise gap.
- Nadruk op soft controls waarbij gedragsverbeteringen van management en medewerkers de belangrijkste succesfactor zijn[57], aansluitend op de vaststelling dat “taal”- en cultuurverschillen aan de basis liggen van soms moeizame samenwerking[58]”. Deze benadering sluit aan op het verschil in perspectief.

[54] Singleton - "The Core of IT Auditing", ISACA Journal Volume 6 2014

[55] AFM - Uitkomsten onderzoek kwaliteit wettelijke controles Big 4-accountantsorganisaties, sept 2014

[56] Havelka, Merhout - "Internal information technology audit process quality: Theory development using structured group processes", International Journal of Accounting Information Systems 14, 2013

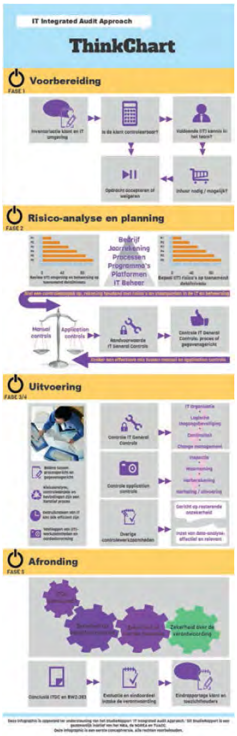
[57] Baarslag – “Soft controls: harde dobber voor IT-managers?”, Tijdschrift Informatie, aug 2013

[58] Bakker - "Venus en Mars", De Accountant juli/augustus 2013

Een combinatie van deze twee sporen -voor de jaarrekening audit- is het doel.
Van belang is te onderkennen dat de samenwerking tussen de accountant en de IT auditor op verschillende niveaus tot stand moet komen, tussen:

- de partners in de jaarrekening audit ("de leiding"): hun samenwerking is rand voorwaardelijk voor de uitvoering. Helaas bestaan op dit niveau ook de meeste blokkades, van politieke, financiële en andere aard. Faciliterende maatregelen vanuit de kwaliteitsbeheersing en-bewaking kunnen hier uitkomst bieden
- hun uitvoerende controleteams ("de uitvoering"): mijn ervaring is dat op dit niveau veel minder blokkades bestaan, en succesvolle samenwerking veel meer afhangt van de kwaliteit van de audit aanpak, lees een goede integratie van IT audit in de jaarrekening audit, en planmatige uitvoering met de juiste processturing.

Een handboek schrijven over het "hoe" van een geoptimaliseerde samenwerking is niet meer nodig; het eerder aangehaalde studierapport van NBA, NOREA en TUACC[59] beschrijft in de vorm van een ThinkChart een proces dat per fase van het audit proces een afstemming tussen de accountant en de IT auditor kent, waarbij mijn stelling is dat:
de kwaliteit van de jaarrekening controle en - als essentieel onderdeel daarvan - de kwaliteit van de samenwerking tussen de IT auditor en de accountant is gebaat bij een geïntegreerd audit proces, waarbij de interactie in de driehoek IT auditor-accountant-klant betere controle-informatie, en daarmee betere controlezekerheid oplevert gedurende en verspreid over het boekjaar. In deze aanpak is IT Audit een geïntegreerd onderdeel van een controle-aanpak, waarbij de IT auditor minimaal de werking van onvervangbare IT controles verifieert.



Een geïntegreerde aanpak van de jaarrekening audit biedt naast kwaliteitsverbetering ook mogelijkheden voor:

- Vernieuwing van de traditionele jaarrekening audit; door middel van het volledig benutten van het potentieel van IT audit, met gebruik van data-analysetechnieken, audit scripts, en het inspelen op continue audit en monitoring technieken;
- Onderzoek naar mogelijke nieuwe vormen van assurance bij de jaarrekening en andere financiële verantwoordingen, die in een maatschappelijke behoefte voorzien.
  Naar het motto: Innovatie is voorsprong.

In een geïntegreerde audit vinden rapportages over IT audit werkzaamheden gedurende iedere fase van de jaarrekening audit plaats. Bij effectieve tussentijdse samenwerking bevat de eindrapportage van de IT auditor geen verrassingen. Die eindrapportage dient dan vooral de documentatie van de deugdelijke grondslag.

Het slotstuk is een schriftelijke rapportage over de IT audit bevindingen –ook in hun onderlinge samenhang- uitmondend in conclusies voor (onderdelen van) de jaarrekening audit.

Om effectief te kunnen zijn, moet deze eindrapportage aan voorwaarden voordoen:

[59] Schellevis en Van Dijk - "Jaarrekening controle in het MKB: IT audit geïntegreerd in de controle-aanpak", april 2014

- Maatwerk; de rapportering moet aansluiten op de overeengekomen scope en specifieke aandachtspunten zoals vooraf en gedurende de audit overeengekomen
- Structuur; de rapportering moet uit voor de accountant herkenbare elementen bestaan, die aansluiten op de overeengekomen risicoanalyse en controle aanpak
- Vertaling; de bevindingen moeten – op basis van overeengekomen criteria - vertaald kunnen worden naar mogelijke gevolgen voor de jaarrekeningaudit
- Eenduidigheid; de conclusie van de IT auditor moet eenduidig en voldoende dwingend zijn, om opvolging door de accountant zeker te stellen.

Hoe kan aan deze rapportagevoorwaarden vorm worden gegeven ?
Het gaat denk ik om het vinden van een goede balans tussen:
- professional judgement als leidraad voor audit beslissingen en
- gedetailleerde IST-SOLL metingen (“niet meten = niet weten”) als beslissingsbasis.

Op die basis kom ik tot het volgende voorstel voor de rapportage van de IT auditor:
De rapportage van de IT auditor aan de accountant dient per primair (sub)proces een kwantitatieve meting van de werking van IT controles te bevatten, waarbij onderscheiden wordt tussen de verwachting – uit de planning fase = de basis voor de overeengekomen controle aanpak (de SOLL positie) – en de feitelijke werking – uit de uitvoering van de audit (de IST positie) - van:
- Als onvervangbaar aangemerkte IT controles (de ondergrens)
- Als vervangbaar aangemerkte IT controles

Een score beneden de ondergrens impliceert dat de IT auditor vanuit zijn oogpunt de controleerbaarheid van - een aspect van - de jaarrekening in twijfel trekt.

Een op deze leest geschoeide, robuuste rapportage met een duidelijk oordeel van de IT auditor - vanuit zijn optiek - legt de bal en de noodzaak van adequate opvolging bij de accountant. Dit kan het duwtje in de rug zijn dat beter waarborgt dat de accountant waar nodig nog aanpassingen in de uitvoering van of de rapportage over de jaarrekening controle doorvoert.

6 Oplossingsvoorstel in samenvatting

Het kennelijk ontbreken van normen of richtlijnen voor het omgaan met jaarrekening assurance bij materiele gebreken in onvervangbare IT controles leidde tot de volgende probleemstelling:

Welke onvervangbare IT controles dienen minimaal adequaat te werken om een hieruit resulterende beperking in de verklaring bij de jaarrekening (van een willekeurige onderneming) te vermijden, en hoe kan de IT auditor in dit kader bijdragen aan reductie van het audit risico?

Kern van de probleemoplossing is een leidraad voor een controleprogramma van onvervangbare IT controles, verdeeld naar Entity Level, General en Application IT controles. Deze leidraad is door de IT auditor - in overleg met de accountant- te vertalen naar de specifieke inrichting en omgeving van de gecontroleerde en zijn financiële verantwoording.

Controleprogramma van onvervangbare IT controles (leidraad)			IT audit doelstelling			
No.	Categorie	Procedures (opzet, bestaan en werking gecombineerd)	Exclusiviteit	Integriteit	Controleerbaarheid	Continuiteit
1	Entity-level	Stel vast dat het management (team) de IT organisatie zodanig gericht heeft dat IT verantwoordelijkheden juist afgebakend zijn, recht wordt gedaan aan eisen van functiescheiding (inclusief scheiding tussen ontwikkeling en productie), en kritische beheersfuncties adequaat zijn bemand	X	X	X	X
2	Entity-level	Beoordeel de inrichting van IT governance op geadresseerde IT risico 's uit de interne en externe omgeving, de tijdigheid van daarop aansluitende risico mitigatie planning, en toets de effectiviteit van gedane interventies	X	X	X	X
3	Entity-level	Toets de adequate monitoring van kritische IT processen en functies door een controlefunctie die namens het management periodieke audits uitvoert, en de effectiviteit van gedane interventies	X	X	X	X
4	General	Stel vast dat kritische componenten van de IT architectuur - waaronder toepassingsprogramma's en databases- aan minimum eisen van beveiliging, integriteit en controleerbaarheid voldoen	X	X	X	
5	General	Controleer de effectiviteit van wijzigingsbeheer -inclusief de naleving van vastgestelde procedures- op belangrijke veranderingen in de productie omgeving		X	X	
6	General	Verifieer de effectiviteit van identificatie en authenticatie procedures voor de logische toegangsbeveiliging op kritische toepassingsprogramma's en databases	X	X	X	
7	General	Stel de werking van procedures vast die voorkomen dat kritische databases via ongeautoriseerde paden, om de applicaties heen, benaderd en gemuteerd worden.		X	X	
8	General	Controleer procedures gericht op de handhaving van kritische functiescheidingen	X	X	X	
9	Applicatie	Stel (na een change) de werking vast van voor de jaarrekening relevante geprogrammeerde controles in massa transactiestromen		X	X	
10	Applicatie	Beoordeel de uitkomsten van audit trail -en de integriteitscontroles gericht op de blijvende werking van kritische applicaties		X	X	

Tabel: Controleprogramma van onvervangbare IT controles

Naast de vakinhoudelijke component is verbetering van de samenwerking tussen de accountant en de IT auditor een belangrijk verbeterpunt, met een "wat" en een "hoe" component. De IT auditor dient hier zélf aan bij te dragen, meer invloed uit te oefenen, maar kan niet zonder actieve ondersteuning van de beroepsorganisaties.

De beroepsorganisaties NBA en NOREA moeten gezamenlijk inhoud geven aan een twee sporenbeleid gericht op verbetering van de samenwerking tussen de accountant en de IT auditor, dit beleid is rand voorwaardelijk voor verbetering van de uitvoering. Dit beleid adresseert zowel harde als zachte elementen van de samenwerking, waarbij onder meer de volgende oplossingselementen aan de orde komen:

1 Verduidelijking van de toepassing van controlestandaarden bij vaststelling van materiële gebreken in de onvervangbare IT controles, inclusief de gevolgen daarvan voor de strekking van de controleverklaring bij de jaarrekening;
2 Invoering van verplichte consultatie van de IT auditor bij de jaarrekening controle van een IT-afhankelijk bedrijf en adequate naleving van gemaakte afspraken binnen een stelsel van kwaliteitscontrole;
3 Regels te stellen aan inhoud en vorm van de jaarrekening audit rapportage door de IT auditor aan de accountant, en voor adequate opvolging door de accountant;

4 Voortgezette educatie te organiseren die elke accountant op een basisniveau van IT expertise brengt en die ieder van de samenwerkende partijen helpt hun culturele verschillen beter te begrijpen en daarmee te kunnen overbruggen;
5 Sturend en ondersteund beleid te maken gericht op het wegnemen van belemmeringen in de onderlinge samenwerking;
6 Vaktechnische vernieuwing van de jaarrekening audit op weg te brengen met een sterke, geïntegreerde IT audit component.

Deze rand voorwaardelijke beleidsmaatregelen scheppen een kader waarin de positie van de IT Auditor wordt versterkt en omzetting zal bijdragen tot reductie van het audit risico in de controle van de jaarrekening.

Machine Learning in the Audit
An Automatic Review of the Debtors List

Ludy Rohling

Ludy heeft Artificial Intelligence (A.I) gestudeerd aan de VU te Amsterdam. In 2014 is zij afgestudeerd met als scriptie onderwerp 'Spatial Crime Prediction'. Daarna is zij begonnen als Data Analist bij de Risk Assuance afdeling van PwC. Naast het werk binnen Risk Assuance is Ludy deels werkzaam binnen het Experience Center van PwC waarin zij de mogelijkheid heeft om te onderzoeken hoe A.I verder kan worden ingezet binnen het vakgebied van de accountancy, maar ook breder binnen PwC.

1 Introduction

A financial audit is conducted to provide a reasonable assurance that the financial statements truthfully represent a company's financial situation. During the execution of the financial audit, the auditors will identify risks and establish whether or not sufficient controls are in place.
Part of the financial audit is the review of the debtors list of the company. An auditor will establish that the debtors in the year-end balance sheet actually exists and will be recorded with the correct balance. Currently, the auditor reviews the debtors list manually and takes the following items into account:

- Credit Balances
- Significantly past due balances
- Account Receivables replaced with notes receivable
- Intercompany and/or related party balances
- Foreign currency balances

Besides the listed items, an auditor will check remarkable transactions, e.g. transactions with consecutive numbers (12345,67), equal numbers (555,55) or round numbers (600,00), and mark these for further investigation on accuracy and whether those are material, i.e. those debtors significantly influence the debtors result.
The manual review of the debtors list is depends on the auditor's interpretation of the rules, which could lead to misinterpretations of the rules and/or disparities in the review of the transactions. By automating the review of the debtors list, misinterpretation is no longer possible. The review of the transactions will have a higher quality and will take less time, because the auditor no longer needs to go through the list manually. But is it really possible to automate the review of the debtors list?

1.1 Machine Learning

To automate the review of the debtors list, a computer must learn which rules must be applied and which characteristics are important. Machine Leaning is a technique within the field of Artificial Intelligence, where an algorithm is able to recognize patterns in large datasets. Due to pattern recognition, the required rules do not have to be explicitly programmed, because the algorithm will recognize the patterns based on the characteristics of the dataset.
According to Phil Simon, machine learning is a "*Field of study that gives computers the ability to learn without being explicitly programmed*" [15]. As with humans, there are 3 different learning methods with specified algorithms.

Supervised Learning - Task Driven, Classification

This learning method requires a dataset (input) with the corresponding output. The 'teacher' will provide the input to the algorithm and verifies the output of the algorithm with the expected output. The goal is to learn the mapping (or rule) between the input and output.

Unsupervised Learning - Data Driven, Clustering

This learning method is used in cases where the output is unknown. The input data is given to the algorithm, leaving it on its own to find a structure in the data. This learning method is often applied to find hidden patterns.

Reinforcement Learning - Close to human learning

This learning method does not learn rules, mappings or finds structure in a provided dataset, but will learn a policy how to behave. This could be achieved, for example, by playing a game against other (human) opponents.

To automate the review of the debtors list, both a supervised learning and unsupervised learning method will be applied. A supervised learning algorithm is likely to learn the predefined rules and may find some

unknown patterns based on the input and output. On the other side, an unsupervised learning method does not require an output, which could be useful in case it is a new client. The last learning method, reinforcement learning, is often applied in the robotics field to simulate *human behaviour* and is therefore less applicable to use in this study.

1.2 Research Objectives

This paper will examine whether it is possible to automate the review of the debtors list using machine learning algorithms. This leads to the following research question:

> *To what extent is it possible to review the debtors list automatically by using machine learning algorithms?*

To make it possible to automate the review, there are a number of preconditions. First, the correctness and completeness of the debtors list, which come from ERP systems, needs to be determined. Secondly, a study of the different algorithms is necessary to be able to select an appropriate algorithm to review the debtors list. Last but not least, auditors must have confidence in the automatic review. Therefore, the review must meet a number of requirements before it can be used in practice. This leads to the following sub questions:

- How is the accuracy, completeness and integrity of the debtors lists established?
- Which machine learning algorithms are suitable for reviewing the debtors list?
- Which requirements must be met before the algorithms can be used in practice?

1.3 Outline of the Paper

In section 2 the background information is obtained through a literature study and will contain audit guidelines of the accounts receivable audit and different machine learning algorithms. Based on the literature, different algorithms will be selected and will be built in a tool in order to automate the review of the debtors list. This will be described in section 3. In section 4, the results of the automated review will be presented and in section 5, these results will be questioned and compared with the reviewed debtors list of the auditor. Finally, section 6 will summarizes the main results, answer the research and sub questions and will draw some suggestions for further research.

2 Literature

2.1 Review of the Debtors List

As stated before, one part of the annual control of the financial statements is the review of a company's debtors list. An auditor will verify that each customer actually exists and is recorded for the correct amount. According to the PwC Audit Guide 2017 - Article 5600, an auditor needs to review the following points:

- Credit Balances
- Significantly past due balances
- Account Receivables replaced with notes receivable
- Intercompany and/or related party balances
- Foreign currency balances

The credit balances are not expected on the debtors list and therefore requires further inspection. The significantly past due date analyses provides insight whether sales documents are likely to be paid. For example, when a sales document is not paid after 3 times the payment terms, it is likely that the debtor will not pay at all, i.e. a *doubtful debt*. The debtors list exists of short term payments and the auditor needs to validate the correctness of the debtors. Intercompany or related parties are not allowed on the

debtors list and must be listed separately. The last point is the currency of the amounts, which must be the reporting currency to represent an accurate view of the company's financial situation.
Besides the listed control points, an auditor will review remarkable transactions, e.g. transactions with consecutive numbers (12345,67), equal numbers (555,55) or round numbers (600,00), and mark these for further inspection.

2.2 Determination of Completeness, Integrity and Accuracy

An auditor examines the financial statements to evaluate the presentation of the balance sheet and income statements as well as the disclosures. The IT auditor and auditor cooperate to translate the requirements for the annual audit into specific control objectives and standards. These objectives and standards are based on the automated processing of data relating to the annual audit.
A client's debtors list could be extracted from their ERP system, e.g. SAP. However, an investigation on the IT applications and IT application controls must be made to determine the reliance of the ERP system. The trustworthiness can be tested by using the ITGC. Without effective ITGC, reliance on IT systems may not be possible. According to the PwC Audit Guide 2017 - Article 3300, ITGC include the following 4 domains:

Access to programs and data (security): Policies and procedures that help determine only authorized access is granted to programs and data upon authentication of a user's identity. Controls include the processes used by the entity to add, delete, and change users (both business users and IT personnel) and their related access rights.

Program changes: Policies and procedures that help determine changes to programs are requested, authorized, performed, tested, and implemented to achieve management's application control objectives. Controls are applied consistently to all programs, applications or data that are relevant to the audit.

Computer operations: Procedures or mechanisms are in place to ensure production systems are processed as approved, production problems are corrected and the systems are restarted to ensure errors are not introduced.

Program development: Policies and procedures that help determine applications are developed, configured, and implemented to achieve management's application control objectives. This domain is relevant only where significant development, implementation, or conversion projects exist or are anticipated that will impact the risk of material misstatement to the current year's financial statements.

The first 3 domains apply to the reliance of the system and data, where the fourth domain is not applicable for extracting a client's debtors list. If during the ITGC testing, no issues are found, the completeness, integrity and accuracy of the debtors list is valid.

2.3 Machine Learning Algorithms

Machine Leaning is a technique within the field of *Artificial Intelligence*, where an algorithm is able to recognize patterns based on the characteristics of a dataset. As with humans, there are 3 different learning methods with specific algorithms.

Supervised Learning Task: Driven, Classification. Learning the mapping between an input set and a known output set.
Example: Artificial Neural Networks (ANN), *K*-Nearest Neighbour, Support Vector Machines (SVM)

Unsupervised Learning: Data Driven, Clustering. Learning based on an input set, but without a known output set. Most of the time used to find unknown patterns in the data.
Example: *K*-Means, Decision Trees

Reinforcement Learning: Close to human learning. The algorithm learns a policy of how to act instead of rules.
Example: Evolutionary Algorithms (EA)

For the automatic review of the debtors list, 2 different learning algorithms are selected for further research, 1 supervised algorithm and 1 unsupervised algorithm. The third learning type, reinforcement learning, is often applied in the robotics field to simulate *human behaviour* and is less suitable to automatically review the debtors list. As supervised learning algorithm, the Artificial Neural Network (ANN) is selected for further inspection. The ANN is widely used for classification and prediction problems. On the other hand, an unsupervised algorithms is selected because those algorithms do not require training. Therefore *K-Means* is selected, because *K*-Means has the advantage of being a simple algorithm which is able to cluster data into groups.

2.3.1 Artificial Neural Network (ANN)

An ANN is a supervised learning algorithm. In general, ANNs are adaptive non-linear models that provide answers to a problem after they have been trained for similar problems. ANNs are inspired by biological neurons in the brain [4][12]. A multi-layer perceptron is a type of feed-forward ANN and is fully connected. As a result, each node in a current layer is connected to every node in the next layer, although there is no connection between the output and input layer to form a directed cycle or loop [3].

An ANN consists of 3 parts; an input, a hidden and an output layer, see also figure 1 for an example. The *input layer* represents data that is used to make predictions. The *hidden layer* contains nodes that are unobservable (a black box). It is used to increase a network's expressiveness due to the fact that the hidden layer allows a network to represent more complex models than without one. Non-linear dependencies are, for example, unsolvable without a hidden layer [12]. The hidden layer in figure 1 shows one hidden layer with 4 nodes. However, this layer may consist of serval layers with each a different number of nodes. The final and third part of the ANN is the *output layer*, which shows the output of the network.

Each layer, except the input layer, consists of neurons, or nodes, that are connected by synaptic weights. Each node has a non-linear activation function that maps the weighted sum of the input vectors to the output of the neuron (which is the input value for the next layer) [3][4][12]. An ANN uses different activation functions for the hidden and output layer. The hidden layer uses a hyperbolic tangent activation function, which produce numbers between -1 and 1. For the output layer the *softmax* function is used, which maps a real valued vector to a range between 0 and 1 and sum to 1[60].

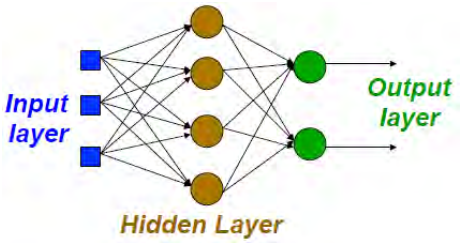


Figure 1: *A multi-layer perceptron with 3 inputs, 1 hidden layer and 2 outputs*

Training Before the ANN can be used to make predictions, the network must learn to make predictions by using a training set with known outcomes (i.e. supervised learning). Learning occurs by applying a back propagation algorithm [3], which searches for weights that minimize the error. The error is the difference of the network's output, $\varphi(net)$, and known or desired output, d_n.

Back propagation is a two-step process: 1) calculating the error and 2) updating the weights. To calculate the error, a network evaluates the data of the training set one by one. This error is then used to update the synaptic weights. A learning rate, η, indicates the proportion of the error by updating the values of the

[60] IBM SPSS Neural Networks 19, https://www.csun.edu/sites/ default/files/neural-network19.pdf

weights. If the learning rate is too high, the network is likely to jump over the global minima and if it is too low, training will take a long time [3]. A weight *w* is updated with the value of *Δw*. A summary of the training process of a multi-layer perceptron is shown in algorithm 1[61].

Testing After training the network and establishing a small enough error, the network can be tested by using a test set. The test set contains data that was not used for training and therefore is allowed for measuring the performance of the network. This measure indicates whether the network was trained sufficiently and is not overfitting the training data.

Algorithm 1 Multi-layer perceptron learning algorithm in pseudo code

time step $t = 0$
initialize: synaptic weights $w_n(t = 0)$
for all *training examples* **do**
  activation: present a training example x_n and desired output d_n
  error calculation: $E = \frac{1}{2}(d_n - y_n)^2$, where $y_n = \varphi(net)$
  update weights: $w_n(t+1) = w_n(t) + \Delta w$, where $\Delta w = \eta(d - \varphi(net))\varphi'(net)x$
  $t = t + 1$
end for

2.3.2 *K*-Means

The *unsupervised* algorithm *K*-Means [10] is an algorithm used for clustering to discover meaningful groups in a dataset based the characteristics [7][9]. It does not have to be trained and it does not require labelled data.
The *K*-Means algorithm is an iterative method to partition a given dataset into a user specified number of K clusters. Each cluster is represented by a centroid, a point defined as the mean of the data instances belonging to the cluster [6]. The clustering needs to be done in such a way that

1. Similarity between instances in the same cluster is *maximised*
2. Similarity between instances in different clusters is *minimised*
3. The number of clusters is *minimised*

After deciding how many clusters are necessary, the *K*-Means algorithm initializes centroids randomly. These are the initial clusters of the data points. After the initialisation, the distance between the data points and the centroids are often calculated with the *Euclidean Distance* function [6][7][9]. Based on distance value, the data point is added to their closest cluster centroid. After adding a data point to a cluster, the *mean* of the centroid is recalculated before another data point is added. The pseudo code of the *K*-Means algorithm is given in algorithm 2.
K-Means is a relatively simple algorithm to apply, but is sensitive to the initialisation of the centroids. Therefore, the *K*-Means algorithm will converge to a local optimum and not to a global optimum [6][7][9].

Algorithm 2 K-Means algorithm in pseudo code

data points x
initialize: *K* centroids at random $C_k(t = 0)$
for all *data points* **do**
  activation: present a data point x_n
  distance calculation: $d = \sqrt{\sum (C_n - x_n)^2}$, where C_n = *centroid* and x_n = *data point*
  cluster assignment: *Add the data point to the cluster where the distance is shortest*
  update centroids: $C_k(t+1)$ = *average of data points in cluster*
  next data point
end for

[61] Based on the Perceptron Convergence Theorem of Haykin [4]

K value

The most optimal K value is the value which divides the data in K clusters in such a way that there is a balance between the maximum error (all data points in one cluster) and zero error (all data points are a cluster). Finding the optimal *K* value is the most difficult part and could be done by trial and error or using an algorithm. The *Elbow* and *Silhouette* method will be discussed to find the most optimal *K* value, but other algorithms are available.

The **silhouette** method will focus on how well a data point fits in a particular cluster. This is done by calculating the fit of the data point with, for example, the *Euclidean* or *Manhattan* distance [6][14]. The **elbow** method will show the minimal number of clusters that are necessary to model the variance of the data [8][16]. In other words, when will the added value of an additional cluster be negligible.

3 Method

The literature describes the way the auditor reviews the debtors list, how the auditor will feel comfortable about the completeness, integrity and accuracy of the data and some machine learning algorithms. However, the reliability of the data is not enough to apply one of the algorithms. The performance of the algorithms is affected by the quality of the data. This section will describe the used data, the selected algorithms and how to measure the performance to make a comparison.

3.1 Data inspection

The auditor receives a debtors list from the client. This list is not received in a predefined format. Therefore, the used debtors list in this thesis is extracted from a client's SAP system to ensure the format of the received data. The reliability of the specific SAP system is not part of this thesis, therefore we assume the SAP system is trustworthy. After the data extraction, the data is checked on the *Completeness*, *Integrity* and *Accuracy* as described in section 2.

3.1.1 Data overview

After the determination of the reliability of the data, the data itself is examined. In total, 19 fields are selected and extracted from the system (see table 1). Inspection of the data shows that the *company code*, *customer number*, *financial year*, *accounting document number* and *accounting document line* cannot be zero. Besides the data types, the data scale should also be taken into account. It is, for example, not possible to compare document numbers, these are only an indication of the sequence.

Table 1: *Overview of the extracted data field and data types*

Field Name	Data Type	Data Scale
Company Code	Varchar	Nominal
Customer Number	Varchar	Ordinal
Customer Name	Varchar	Nominal
Clearing Date	Datetime	Interval (Cyclic)
Clearing Document Number	Varchar	Ordinal
Financial Year	Int	Ratio
Period	Int	Interval (Cyclic)
Accounting Document Number	Varchar	Ordinal
Document Line	Int	Ordinal
Posting date	Datetime	Interval (Cyclic)
Document Date	Datetime	Interval (Cyclic)
Currency	Varchar	Nominal
Document Type	Varchar	Nominal
Posting Key	Varchar	Nominal
Local Currency	Decimal	Ratio
G/L Account Number	Varchar	Ordinal
Terms of Payment	Varchar	Nominal
Baseline Date for Due Date Calculation	Datetime	Interval (Cyclic)

3.1.2 Data Statistics

After the inspection of the data types and scales, a more in depth analysis is performed. In case of the nominal and ordinal values, it is not possible to calculate a meaningful average. Therefore it is inspected how many unique data values occur how many times.

In total there are 88,377 lines in the debtors list of *2014*. These could be divided in 2 unique company codes. The first company code has 10,502 lines and the second 77,875. On average there are 7,365 line item payments each month with the highest number in April. There are 3 G/L accounts used, which are Account Receivable Trade accounts; Unaffiliated - 81,146 lines, Affiliated - 7,011 lines and Intercompany - 220 lines. It is noteworthy that there are more unique customer numbers then unique customer names. This could indicate that a customer has multiple customer numbers.

There are 8 different document types used and 99.8% of the documents are *Commissionaire Documents* or *Billing Document Transfers*. Furthermore, it is remarkable that 38.2% of the debtor bookings are posted with a credit memo key. However, further inspection shows that 94.7% of the credit memos are related to commissionaire documents.

A closer look at the 2 date time variables, posting and clearing date, shows that the most posting lines are made in 1st of April 2014 and most document lines are cleared at 29th of June 2014. An overview of the statistics of the posting and clearing dates is given in example 1. Last but not least, the reporting amount shows that most values are in the range of -385,240 and 443,570. The most common amount is 380.01 which occurs 347 times. More statistics are given in example 2.

Example 1: Summary of Date Statistics 2014

Posting Date		**Clearing Date**	
Minimal Value	01-01-2014	Minimal Value	01-01-2014
1st Quarter	26-03-2014	1st Quarter	06-04-2014
Median	16-06-2014	Median	26-06-2014
3rd Quarter	23-09-2014	3rd Quarter	08-10-2014
Maximum Value	31-12-2014	Maximum Value	04-03-2015
Modus	01-04-2014	Modus	29-07-2014

Example 2: Summary of Currency Statistics 2014

Amount in Local Currency	
Minimal Value	- 634,628.60
1st Quarter	- 1,377.89
Median	502.92
3rd Quarter	2,221.26
Maximum Value	3,297,748.64
Modus	380.01
Average	1,767.24

The debtors list of *2015* consist of 45,819 lines. These could be divided in 2 unique company codes. The first company code has 10,471 lines and the second company code 35,348. On average there are 3,818 payments each month with the highest number in April. For 2015, the same 3 G/L accounts are used as in 2014; Unaffiliated - 421,569 lines, Affiliated - 3,109 lines and Intercompany - 141 lines. It is noteworthy that there are more unique customer numbers then unique customer names. This could indicate that a customer has several customer
numbers.

There are 8 different document types used and 99.8% of the documents are *Commissionaire Documents* or *Billing Document Transfers*. Furthermore, it is remarkable that 34.1% of the debtor bookings are posted with a credit memo key. However, further inspection shows that 94.4% of the credit memos are related to commissionaire documents.
A closer look at the 2 date time variables, posting and clearing date, shows that the most postings are made on 1st of April 2015 and most documents are cleared at 9th of January 2015. An overview of the statistics of the posting and clearing dates is given in example 3. Last but not least, the reporting amount shows that most values are in the range of -695,997 and 1,914,883. The most common amounts are 666.63 and 726.52 which both occur 98 times in the debtors list. More statistics are given in example 4.

Example 3: Summary of Date Statistics 2015

Posting Date		**Clearing Date**	
Minimal Value	01-01-2015	Minimal Value	02-01-2015
1st Quarter	31-03-2015	1st Quarter	15-04-2015
Median	25-06-2015	Median	10-7-2015
3rd Quarter	29-09-2015	3rd Quarter	15-10-2015
Maximum Value	31-12-2015	Maximum Value	04-03-2016
Modus	01-04-2015	Modus	09-01-2015

Example 4: Summary of Currency Statistics 2015

Amount in Local Currency	
Minimal Value	-7,359,243.62
1st Quarter	-1,419.98
Median	479.67
3rd Quarter	2,254.03
Maximum Value	7,359,243.62
Modus	666.63 and 726.52
Average	2,160.33

3.2 Data Preparation

Before the algorithms of section 2 can be applied on the available data, the data needs to be prepared.

3.2.1 Data Transformation

As described in section 2, most algorithms expect numerical data of the interval or ration scale. However, table 1 shows that most variables are on the nominal and ordinal scale. Therefore, it is necessary to transform the nominal and ordinal data to a (binary) numerical scale.
As shown in table 1, there are 12 variables which are nominal or ordinal, which should be transformed before a distance measure, e.g. Euclidean Distance, is able to calculate the distance between values. However, it is possible that not all variables are necessary as input for the algorithms.
Before the data transformation, four variables are added to the dataset; Credit, Due date, Intercompany and Classification. The variable Credit indicates whether a line item of the debtors list does not have a clearing document number and the amount is negative. The Due date variable indicates that a line item is not cleared and the difference between the posting date and book closure (December 31) is more than 30 days. The intercompany variable indicates debtors that are possibly intercompanies, i.e. they have the client's name in their name or description. Finally, if one of the 3 variables is true, the line item is classified as *should be inspected in more detail by the auditor*.
To explore the possibilities of the machine learning algorithms, 2 datasets will be used (if applicable). The first dataset will only contain the defined variables, Credit, Due date, Intercompany and Classification.

These are all binary data types and therefore not suitable for every algorithm. The correlation between the 3 variables and 2 classes is easy to understand and therefore suitable to get a feeling how the algorithms operate. The second dataset will consist of the original data fields, where it is harder to see a direct correlation. However, not all fields will be used, since a transformation is not always possible, e.g. the client's name.
The following variables are selected and transformed to match the required numerical datatypes; Company Code, Period, Posting date, Clearing data, Amount and Intercompany. The first step is to replace all *not applicable* fields to zero to ensure that calculations can always be done. Secondly, company code, posting date and amount are converted to numerical data. And finally, all the fields are normalised. Please note that the transformed dataset is only used for the algorithms that require numerical data. Other algorithms can still use the original data as represented in table 1.

3.2.2 Training and Test set

Besides the data transformation, a training and test set is necessary for the *supervised learning* algorithms. The *unsupervised learning* algorithms do not need these sets.
The size of the training and test set can be determined in 2 ways. The first method is to use a X% of the total dataset as training set and the remaining data points as test set. A commonly used distribution is 60% as training set and 40% as test set. Another way, is to randomly divide the dataset in X equal groups and select one group as the test set and the other groups as training set. After training, pick another group as test set and the remaining groups as training set and train the algorithm. Repeat this until all the groups are used a test set. This method is called *Leave One Out Cross Validation* (LOOCV) and is mostly used for training predictive models and to prevent the model of overfitting [12]. A graphical overview of the LOOCV is given in figure 2.

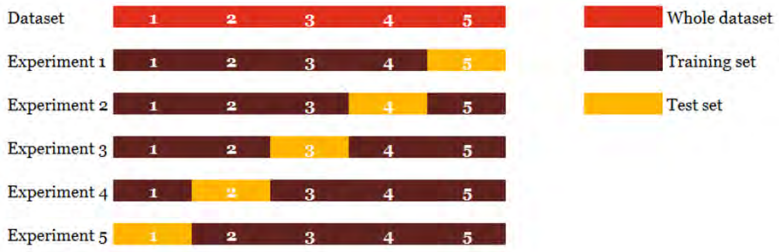


Figure 2: *A graphical overview of the LOOCV method*

3.3 Modelling and Evaluation

3.3.1 Selected Algorithms

Two different algorithms, one supervised (ANN) and one unsupervised learning (*K*-Means) algorithm, are selected for one and the same problem to explore the differences. Whereas the ANN will learn the correlations between the different variables, the *K*-Means algorithm will create clusters, which will indicate which data entries are more or less the same. A big advantage of *K*-Means is that it does not require any training, where an ANN does. On the other hand, an ANN is more robust against outliers and contaminated data.
The selected algorithms require different data sets. Where the ANN is not able to handle nominal and ordinal data, the *K*-Means algorithm faces problems when dealing with binary data. For the ANN a training set is created with numerical data and labelled with a class (see 3.2.1). The labelled data is also useful for *K*-Means, to understand and validate the characteristics of the groups and find the groups with the expected outliers, i.e. data entries that need to be verified by the auditor. However, *K*-Means is not able to handle noise in the data and therefore a related algorithm, *K-Medoids* is used. *K*-Medoids is related to

the *K*-Means algorithm and also attempt to minimize the distance. In contrast to the *K*-Means algorithm, the centre points used by *K*-Medoids are always existing data points, while *K*-Means frequently 'creates' centre points. The centre point of the *K*-Medoids algorithm is defined as the *medoid*, whose average dissimilarity to all the data points is minimal i.e. it is the most centrally located point in the dataset [1][13].

3.3.2 Model Settings

In order to model the selected algorithms, the programming language and software environment for statistical computing and graphics supported by the R Foundation for Statistical Computing is used[62]. R has several packages with predefined models including documentation available on-line.

For modelling the ANN several packages are available and after reading several documentation sets, the *RSNNS* package is selected [2]. There are 6 input parameters (which are normalised) and 1 output parameter. The used ANN model has one hidden layer with 3 hidden nodes, according to rule of thumb *the optimal size of the hidden layer is usually between the size of the input and size of the output layers* [5]. Furthermore, the ANN will use the backpropagation algorithm as a learning function, has an initial learning rate of 0.2 and 0, and will use 15 iteration.

For *K*-Medoids, the R package *PAM* [11] is used to cluster the data into K clusters following the *K*-Medoids approach. Each data point is then assigned to the cluster corresponding with the nearest medoid. The most difficult step is to determine how many clusters should be used. The PAM package includes the *Elbow* and *Silhouette* method to calculate the most optimal number of cluster for this dataset. Both methods test various *K*-values to find the optimal *K*-value.

3.3.3 Performance Measure

After initializing up the models, the performance should be measured. The first measurement is the accuracy of the predictions. In case of the ANN, the predicted output can be compared with the desired output. The type I and II errors can be counted, i.e. false positive results and false negative results. For *K-M*edoids, the performance measure is not that easy. Where the ANN provides an output per line or data entry, *K*-Medoids shows a graphical overview of the results, i.e. clusters of the data point. However, each data point has an ID. With the ID's it is possible to evaluate the characteristics of the data points in a cluster to find out the matching characteristics. Therefore the Type I and Type II error is used to score the accuracy of the predictions and to compare both models. The idea of the Type I and Type II error is illustrated in 2.

Table 2: *Overview of the ANN prediction errors based on the 3 input variables and 1 output variable.*

Observations **Predictions**	**0**	**1**
0	Accurate	Type II
1	Type I	Accurate

4 Results

After setting up the different parameters for the ANN and *K*-Medoids, the models are used to review the debtors list. The datasets consist of the same variables, however, the data types of the variables could differ. This depends on the requirements of the used algorithm.

4.1 Artificial Neural Network Results

As discussed in chapter 3, two models of the ANN are used, the first model to explore the possibilities and accuracy of the ANN and the second model to make predictions on the dataset.

[62] R, The R Project for Statistical Computing, https://www.r-project.org/

The first model used 3 input variables, 3 hidden nodes and 1 output node, with the debit/credit, due date and intercompany indicator as input variables and the predicted classification as output variable. An overview of the error over the iterations is given in figure 3, which shows that 5 iterations is enough for testing with 3 variables.
After training and testing, the model is used to make predictions based on a new dataset of the same client. In this case, financial year 2014 is used for training and testing to make a prediction of the data of the financial year 2015. The predictions are measured by using the confusion matrix as described in section 3.3.3. An overview of the Type I and Type II error is given in table 3. The model predicted 6 data entries as a Type II error, i.e. a *false negative* result.

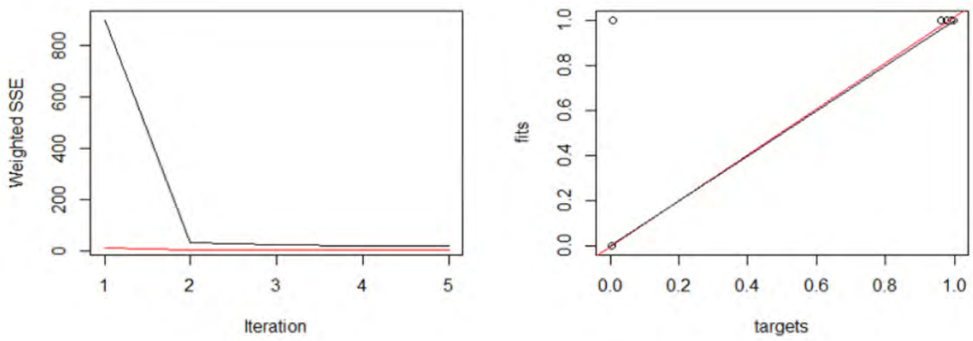


Figure 3: *A graphical overview of the ANN method with 3 input variables and 1 output variable*

Table 3: *The confusion matrix based on the 3 input variables and 1 output variable*

Observations	**0**	**1**
Predictions		
0	42366	6
1	0	3447

The second ANN model does not use the 3 binary input variables, but 6 input variables from the raw dataset. The remaining variables, such as the number of hidden nodes and iterations, is changed. Furthermore, the number of iterations and the learning rate are varied. Based on the experiments, 15 iterations is enough to train the model, see figure 4 for the error per iteration.
After training and testing, the model is applied to the data of the financial year 2015. Comparison of the predicted classes and the real classes resulted in 99.75% correctly classified data entries, 0.25% as a Type I error and 0% as a Type II error. The confusion matrix of this model is given in table 4.

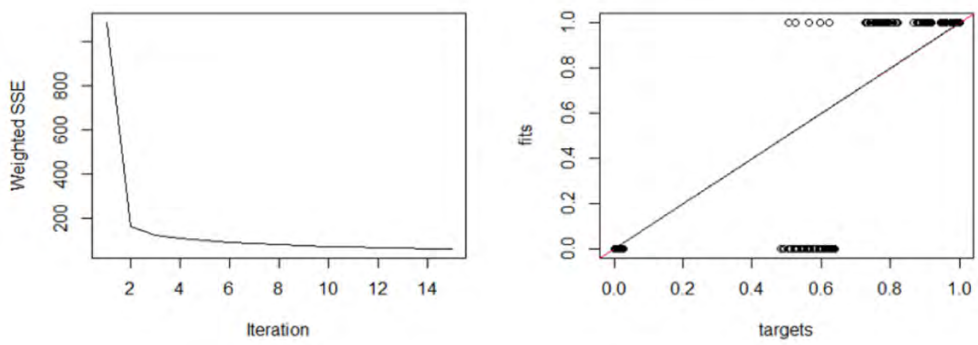


Figure 4: *A graphical overview of the ANN method with 3 input variables and 1 output variable*

Table 4: *The confusion matrix based on 6 input variables, 1 output variable and 5 iterations*

Observations	**0**	**1**
Predictions		
0	42253	0
1	113	3453

4.2 *K*-Medoids Results

As described in chapter 3, it is necessary for the *K*-Medoids method to determine the number of clusters and both the Elbow and Silhouette method are used. In figure 5, a graphical overview is given of different number of clusters. The dashed lined indicates which K-value should give the most optimal results.

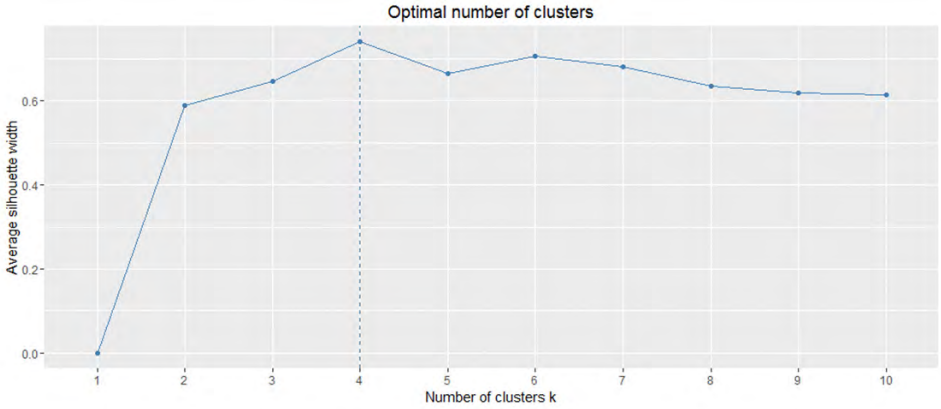


Figure 5: *A graphical overview of different K values for K-Medoids*

The figure shows that the most optimal number of clusters for this dataset is 4 clusters. More than 4 is possible, but the picture shows that the difference between the groups is not significant, i.e. the *elbow* is only present at K = 4. The results with using K = 4 are given in figure 6. To compare the optimal number of clusters, 2 other K-values are used, e.g. K = 3 and K = 5, which do not show a significant different result.

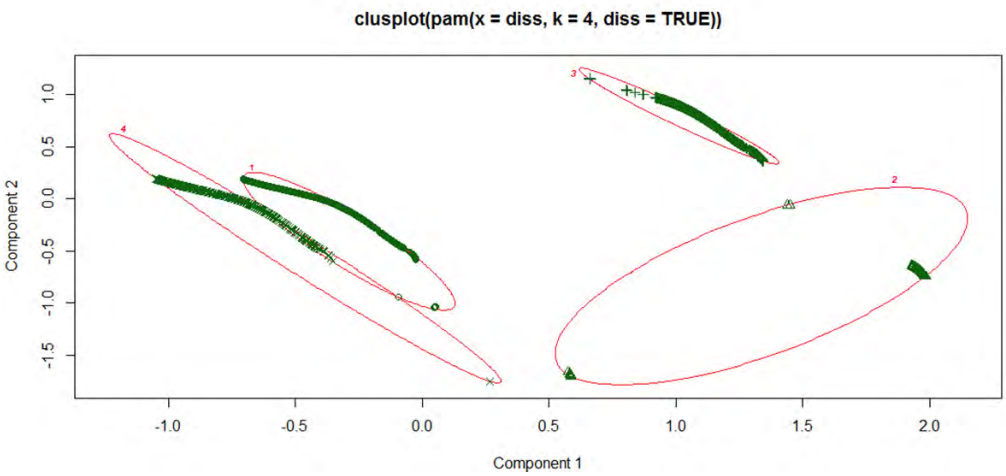


Figure 6: A graphical overview of the data by using 4 clusters

Figure 6 shows that cluster number 2 is very big with a low density, where cluster numbers 1 and 4 are smaller with a higher density. Cluster number 3 is the smallest ellipse with the highest density. The density indicates the similarity of the data points, i.e. cluster 2 has the least similar and cluster 3 has the most similar data points. Further inspection shows that cluster 2 only exists of data points classified as 1, where cluster 4 only has data points with classification 0 (and one data point classified as 1). Cluster 1 has 146 data points classified as 1 where the remaining points are classified as 0. The same is valid for cluster 3, where 80 data points are classified as 1. The results are summarized in confusion matrices per cluster, see table 5, 6, 7 and 8.

Table 5: *The confusion matrix of Cluster 1*

Observations / Predictions	0	1
0	14008	146
1	0	0

Table 6: *The confusion matrix of Cluster 2*

Observations / Predictions	0	1
0	0	0
1	0	3226

Table 7: *The confusion matrix of Cluster 3*

Observations / Predictions	0	1
0	14071	80
1	0	0

Table 8: *The confusion matrix of Cluster 4*

Observations / Predictions	0	1
0	14287	1
1	0	0

4.3 Comparing Results

The results of both models (i.e. the ANN and *K*-Medoids) are measured by means of a confusion matrix. The ANN classifies a data entry (i.e. debtor) to a class, which can be easily compared with the actual class of the data entry. *K*-Medoids is not assigning a class to a data entry, but clusters data points based on characteristics. Because every data point has an ID and the classes are known, it is possible to identify which data points are in an unexpected cluster.

For comparison, the confusion matrices of *K*-Medoids are be summed up. This resulted in a total 45,592 correctly clustered data points and 227 incorrectly clustered data points (Type II error). For the ANN, a total of 45,706 data points are correctly classified and 113 data points are incorrectly classified (Type I

error). See the confusion matrix of table 9 for the results of *K*-Medoids and table 4 for the confusion matrix of the ANN.

Table 9: *Summed confusion matrix of K-Medoids*

Observations / Predictions	0	1
0	42366	227
1	0	3226

Further inspection of the *K*-Medoids Type II error shows that most data points have a due date greater than 30 days. Those data points occur during the whole year with most posting dates in period 11. The remaining Type II error data points are credit amounts. Those data points are mainly posted in period 5, 6, 7 and 12 and none of the documents are cleared. Further inspection shows that 32 out of 41 are commissionaire documents and the remaining 9 documents are billing transfer documents.
Looking at the specific misclassified data points of the ANN data shows that all sales documents do miss a clearance document. Besides the outstanding sales documents, the total amount is immaterial. For the misclassified *K*-Medoids data points, all 227 documents are not cleared and occur during the whole financial year 2015. The total amount of all 227 items shows that the amount is immaterial and therefore do not affect the accounts receivables.

5 Discussion

5.1 Performance Results

As shown in table 4, the ANN misclassified 0.25% of the items (113 out of 45,819). All 113 cases are a Type I error which leads to manually reviewing 113 unnecessary cases. Table 9 shows the confusion matrix of the *K*-Medoids method. *K*-Medoids misclassified 0.50% of the items (227 out of 45,819). All those 227 items are a Type II error which leads to missing 227 items for the manual review of the auditor.
Further inspection of the misclassified ANN data shows that the sales documents exists of 3 types, 57 billing documents, 55 commissionaire documents and 1 accounting document. All sales documents have a document date of December 2015 and do miss a clearance document. Besides the outstanding sales documents, the total amount is immaterial. Further inspection of the *K*-Medoids results shows that 130 out of 227 items are commissionaire documents, 94 items are billing documents and 4 items are accounting documents. All the documents are not cleared and occur during the whole financial year 2015. Finally, the total amount of all 227 items are immaterial and therefore do not need a manual control of the auditor.
According to the client file, the auditor did a manual check of the debtors list. They did find some exceptions, however further follow up was is not necessary since the total amount is immaterial. A scan of the debtors list regarding unusual items did not lead to items for follow up and a reconciliation of the debtors list with the trail balance shows that no differences are noted.

5.2 Algorithms and Performance Measurement

As has been described in section 3, two algorithms are used for the automatic review of the debtors list. The first method is a supervised algorithm: the ANN. The second an unsupervised algorithm: *K*-Medoids. The ANN must be trained before the debtors list can be reviewed. The *K*-Medoids method does not need any training, but the K-value should be defined beforehand.
The two algorithms, besides being in different categories, both require some initial settings. In case of *K*-Medoids, this is the K-value, which is determined by the elbow and silhouette function. The ANN has several initial settings, e.g. learning rate, initial weights, iterations, nodes, layers. The optimal settings are unknown and the current settings are chosen based on rule of thumb and trial and error. A more in depth research into the 'most optimal' initial settings would probably lead to better results.

Apart from the initialisation, the output of both algorithms is different and a performance measure is introduced, see section 3.3.3. This measurement shows the Type I and II error in a confusion matrix. For the ANN it is easy to determine whether a debtor is correctly classified or not. For the *K*-Medoids method it is not, because the algorithm creates clusters. Therefore inspection of the data points per cluster was necessary and showed that based on the characteristics, some data points were expected to be found in another cluster. Those data points are marked as misclassified. The error definition of *K*-Medoids is done manually. It is be possible that another performance measurement requires less interpretation and is more suitable for the *K*-Medoids method.

5.3 Applying Techniques in the Audit

The applied techniques, a supervised learning and unsupervised learning algorithm, gave some interesting and promising results. However, this is only possible when ITGC are in place, i.e. the auditor is able to rely on the system. The IT auditor reviews that the controls are in place in the 4 domains *Access to programs and data, Program Changes, Computer Operations* and *Program Development* (see 2.2). The first 3 domains apply to the reliance of the system and data, where the fourth domain is not applicable for extracting a client's debtors list. During ITGC testing no issues were found and therefore the completeness, integrity and accuracy of the debtors list is valid.

Besides testing the ITGC, the IT auditor will be more involved in the annual control. The IT auditor will extract the debtors list and runs the algorithm to review the debtors list automatically. This ensures the reliance of the debtors list, sufficient comfort is gathered with the ITGC testing. However, the IT auditor is unable to verify the outcomes of the automatic review and therefore, needs to share the used debtors list and outcome with the auditor.

Comparison of the findings between the two algorithms and manual control of the auditor did lead to the same results, no material differences were noted. However, the IT audit is unable to determine the materiality level. Therefore an account should always decide if the results need further inspection. Despite the outcome of the algorithms, the auditors should trust the outcome of algorithms.

First of all, an auditor must rely that the automatic review resulted in a valid and correct result before the technique can be applied during the audit as a valid method. The reliability of the output could be obtain via a review of the used algorithm, which could be done via custom made ITGC and code reviews. Besides a theoretical control, it is necessary to compare the manual review with the automatic review of the debtors list. When differences between the results exists, the ideally case would be that the algorithm finds items which the auditor has missed for further inspection. The auditor needs to be convinced that the algorithm marks at least the same items as a manual review.

To gain some confidence, more test runs should be done with machine learning algorithms to improve the results. Besides the results themselves, confidence is gained by understanding the correctness of the results. An auditor is only likely to trust an automatic reviews if (s)he is able to follow the way an algorithm assigns a certain class to an item. It is interesting to know why one item needs a follow up and the other item does not. And if the auditor has a different view, is (s)he able to understand the processing steps of the algorithm and is this a valid difference?

6 Conclusion

The auditor provides reasonable assurance that the financial statements truthfully represents the company's financial situation at each year-end. Part of the financial audit is the validation of the debtors list. Currently, the debtors list is reviewed manually, but with the current techniques, i.e. Machine Learning, it could be possible to automate this review. This research has investigated the research question: "*To what extent is it possible to review the debtors list automatically by using machine learning algorithms?*"

6.1 Artificial Neural Network versus *K*-Medoids

Machine Learning is a technique within the field of Artificial Intelligence and gives computers the ability to learn without explicitly programmed [15]. There are three different learning types, *supervised learning, unsupervised learning* and *reinforcement learning.* This research focused on the first two, *supervised learning* and *unsupervised learning*, since the review of the debtors list could be seen as a classification or clustering problem. The third learning type is often applied in the robotics field to simulate human behaviour and is less suitable in this study. Research indicates that an ANN was the most suitable supervised learning algorithm, where *K*-Medoids was the best choice as unsupervised algorithm.

The ANN was used to classify each item on the debtors list. The actual class and predicted class were compared and the results were measured by using a confusion matrix, which indicated the different types of errors. In case of the ANN, only Type I errors (false positives) occurred for 113 out of 45,819 items. Further inspections shows that all sales documents are from the last period (December 2015) and are missing a clearance document. Another finding was the presence of commissionaire documents. However, further manual inspection was not necessary since the total amount of the 113 items were immaterial.

The *K*-Medoids method was used to cluster the data. Instead of assigning a class to debtor, the method groups data points together based on the characteristics, i.e. clustering. After conducting a small research, 4 clusters gave the most optimal result for this dataset. The results were measured by inspecting each data point's characteristics and the characteristics of the whole cluster to identify unexpected data points in a cluster. Those findings were measured by using a confusion matrix (per cluster and altogether). Results showed that only Type II errors (i.e. false negatives) occurred for 227 out of 45,819 items. Further inspection shows that all sales documents occurred during the whole year and were not cleared. However, further manual inspection was not necessary since the total amount of the 227 items were immaterial.

Based on the results of the confusion matrices (see table 4 and 9), the ANN outperformed *K*-Medoids. Not because of the small deviation of misclassified items but due to the nature of the error type (false positive versus false negative). Comparing the results of the algorithms with the results of a manual control performed by an auditor, the conclusion is the same. Limitations weren't found because the total amount of error was immaterial.

6.2 IT Auditor and Machine Learning in the Audit

Unless the promising results conducted with this research, it is not possible to apply this technique in every audit. Besides some technical difficulties, the algorithms used data from an ERP system, i.e. SAP. Before the debtors list can be used, the *Completeness, Integrity* and *Accuracy* of the list must be determined. Since the list was extracted from an ERP system, the whole ERP system must have be tested with ITGC by an IT-auditor. Reliance of the system, and debtors list, is not possible without an effective ITGC's. See section 2.2 for more information.

When machine learning algorithms are applied in the audit, an auditor needs confidence that the algorithm does what is expected. The role for the IT-auditor will be expanded with ensuring the working and reliance of those algorithms. However, how do you audit an self-learning algorithm?

6.3 Further Research

This first test did show that it could be possible to automatically review the debtors list by using machine learning algorithms. However, more pilots are needed to improve the initialisation of the algorithms itself, but also to add (more) value for the auditor. An auditor must be able to understand why certain items needs further manual inspection where another items do not. Only after gaining confidence of the trustworthiness of these kind of learning algorithms, an automatic review could be possible.

The trust of such algorithms could be guaranteed by IT-auditors. Currently, it is unknown how to audit machine learning algorithms. A framework with guidelines does not exist. Is it possible to test that the algorithm does what it should do? And how can we reperform the learning steps? The work of the IT-auditor will change if machine learning algorithms are used by auditing financial statements.

Besides the audit related questions, further research is necessary to optimize the learning algorithms. In case of the ANN, more research should be done to the initial settings of the variables, e.g. learning rate, weights, number of layers. For the *K*-Medoids algorithm, more research is necessary to indicate which variables should be taken into account and which method is best to use to indicate the *K* value. Another addition is the use of text-mining to search into text to determine whether or not intercompanies are present in the debtors list, but also to scan the descriptions of the sales documents.
Last point is used data. In this research the debtors information form a client's ERP system was used. Further research could extend the debtors information with external data. Do all Dutch companies on the list have a Chamber of Commerce number? The sector in which the customers operate might be interesting to group the customers.

7 References

[1] Adluni, N. Fraud detection in financial statements: Improving fraud detection in an audit of financial statements using data mining and statistics-based techniques. Master thesis, VU University Amsterdam, 2015.

[2] Bergmeir, C., and Benítez, J. M. Neural networks in R using the stuttgart neural network simulator: RSNNS. Journal of Statistical Software 46, 7 (2012), 1–26.

[3] Gardner, M., and Dorling, S. Artificial neural networks (the multilayer perceptron) - a review of applications in the atmospheric sciences. Atmospheric environment 32, 14-15 (1998), 2627–2636.

[4] Haykin, S. S. Neural Networks and Learning Machines, vol. 3. Pearson Education Upper Saddle River, 2009.

[5] Heaton, J. Introduction to Neural Networks with Java. Heaton Research, Inc., 2008.

[6] Hennig, C., and de Amorim, R. C. Recovering the number of clusters in data sets with noise features using feature rescaling factors. Information Sciences 324 (2015), 126–145.

[7] Jain, A. K. Data clustering: 50 years beyond k-means. Pattern recognition letters 31, 8 (2010), 651–666.

[8] Ketchen, D. J., and Shook, C. L. The application of cluster analysis in strategic management research: an analysis and critique. Strategic management journal 17, 6 (1996), 441–458.

[9] Likas, A., Vlassis, N., and Verbeek, J. J. The global K-Means clustering algorithm. Pattern recognition 36, 2 (2003), 451–461.

[10] MacQueen, J., et al. Some methods for classification and analysis of multivariate observations. In Proceedings of the fifth Berkeley symposium on mathematical statistics and probability (1967), vol. 1, Oakland, CA, USA., pp. 281–297.

[11] Maechler, M., Rousseeuw, P., Struyf, A., Hubert, M., and Hornik, K. Cluster: Cluster Analysis Basics and Extensions, 2016. R package version 2.0.5 — For new features, see the 'Changelog' file (in the package source).

[12] Mitchell, T. Machine Learning. McGraw Hill, 1997.

[13] Pratap, R., Vani, K. S., Devi, J. R., and Rao, D. K. N. An efficient density based improved k-medoids clustering algorithm. IJACSA) International Journal of Advanced Computer Science and Applications 2, 6 (2011).

[14] Rousseeuw, P. J. Silhouettes: A graphical aid to the interpretation and validation of cluster analysis. Journal of Computational and Applied Mathematics 20 (1987), 53–65.

[15] Simon, P. Too Big to Ignore: The Business Case for Big Data, vol. 72. John Wiley & Sons, 2013.

[16] Thorndike, R. L. Who belongs in the family? Psychometrika 18, 4 (1953), 267–276.

Toetsing Scrum in het kader van de jaarrekeningcontrole

Toetsen van change management volgens de SCRUM methodiek in het kader van de jaarrekening-controle

Arriën van Deursen MSc RE

In 2011, Arriën van Deursen graduated with a master degree at the VU University, Amsterdam with a specialization in management consultancy firms
In the same year, he started working at EY as an IT auditor within the financial services sector. During his employment at EY, he finalized the postgraduate master IT auditing at the VU University, Amsterdam in 2015 on the topic of auditing SCRUM based change management processes
In 2018, Arriën started working at the Dutch Central Bank (DNB) as financial market infrastructures supervisor.

1 Aanleiding

Om in het kader van de jaarrekeningcontrole te kunnen steunen op geautomatiseerde systeemcontroles en gebruik te kunnen maken van systeem-gegenereerd lijstwerk (electronic audit evidence), moeten de IT General Controls (ITGC's, randvoorwaardelijke beheersingsmaatregelen) getoetst worden (Schellevis en Van Dijk, 2014), waarbij de IT auditor zich voornamelijk richt op change management, logische toegangsbeveiliging en continuïteitsbeheer van de relevante componenten van de IT omgeving.

Het normenkader wat de IT auditor hanteert ten aanzien van change management (softwareontwikkeling en -onderhoud) in het kader van de jaarrekeningcontrole, is ontwikkeld op basis van en gericht op de traditionele watervalmethode. Binnen deze methode is er in het ontwikkelproces een duidelijke fasering aangebracht tussen ontwerp, ontwikkeling, testen, goedkeuring en onderhoud van applicaties (Strode, 2012; Collyer en Manzano, 2013; Trijsenaar en Zalm, 2013; Martens et al., 2014).

In toenemende mate wordt binnen organisaties gebruik gemaakt van de SCRUM methodiek in de ontwikkeling en het onderhoud van (bedrijfs-kritische) applicaties (Kim et al., 2013; Trijsenaar en Zalm, 2013; Martens et al., 2014; Westerveld, 2014). Deze methode is gericht op een snelle ontwikkeling van software en kenmerkt zich door de aanpak waarbij in multidisciplinaire teams deelprojecten van de systeemontwikkeling worden aangepakt.

Het huidige normenkader, dat door de IT auditor wordt gehanteerd in het kader van de jaarrekeningcontrole om change management (software onderhoud) te toetsen om een uitspraak te doen over de geautomatiseerde gegevensverwerking, lijkt niet toepasbaar in een omgeving waarin de SCRUM methodiek wordt gehanteerd (Barlow et al., 2011). Omdat de relevante kenmerken van de SCRUM methodiek afwijken van de watervalmethode, moet er een normenkader worden ontwikkeld om de IT auditor handvatten te bieden om in het kader van de jaarrekeningcontrole zijn werkzaamheden uit te voeren en om een uitspraak te kunnen doen over de betrouwbaarheid van de geautomatiseerde gegevensverwerking.

2 Onderzoeksonderwerp

Op basis van de beschreven aanleiding van het onderzoek, is de volgende onderzoeksvraag geformuleerd:

Hoe kan change management (softwareontwikkeling en -onderhoud) volgens de SCRUM methodiek getoetst worden in het kader van de jaarrekeningcontrole teneinde een uitspraak te kunnen doen over de betrouwbaarheid van de geautomatiseerde gegevensverwerking?

Het beantwoorden van de onderzoeksvraag heeft enkel betrekking op het toetsen van change management volgens de SCRUM methodiek in het kader van de jaarrekeningcontrole door de IT auditor om uiteindelijk een uitspraak te kunnen doen over de betrouwbaarheid (voornamelijk juistheid en volledigheid) van de geautomatiseerde gegevensverwerking (geautomatiseerde systeemcontroles en systeemgegenereerd lijstwerk). Met change management wordt in dit onderzoek verwezen naar het proces van ontwikkelen (en onderhouden naar aanleiding van gebruikerswensen) van software, maar niet naar het proces van installeren van standaard updates, patches en fixes. Het eindresultaat is een normenkader dat door de IT auditor tijdens de jaarrekeningcontrole kan worden gebruikt en zal derhalve niet volledig van toepassing zijn voor andersoortige controlewerkzaamheden die worden uitgevoerd door de IT auditor.

De toepasbaarheid van het ontwikkelde normenkader zal worden gevalideerd aan de hand van verschillende interviews met subject-matter experts die werkzaam zijn binnen de financiële sector en ervaring

hebben met het toetsen van change management volgens de SCRUM methodiek binnen deze sector (banken, vermogensbeheerders, verzekeraars).

3 Onderzoeksmethode

Om een normenkader te ontwikkelen om change management volgens de SCRUM methodiek te toetsen in het kader van de jaarrekeningcontrole, dient SCRUM nader te worden gedefinieerd. Het literatuuronderzoek was tweeledig Enerzijds zijn de gehanteerde definities, uitgangspunten en 'leading practices' van de SCRUM ontwikkelmethodiek uitgewerkt. Anderzijds zijn de variabelen en normenkaders, die zijn voorgesteld om deze methodiek te beoordelen, behandeld.

Nadat vanuit de literatuur SCRUM is gedefinieerd, zijn vanuit het huidige normenkader de toetspunten geïdentificeerd die de IT auditor hanteert ten aanzien van change management in de jaarrekeningcontrole. Door middel van een kritische beschouwing van dit normenkader en de theoretische uiteenzetting van SCRUM uit eerdere hoofdstukken wordt duidelijk dat het huidige normenkader niet voldoet en wordt inzichtelijk welke 'gaps' moeten worden aangevuld in het nieuwe normenkader.

Het nieuwe normenkader bevat een beschrijving van het normenkader voor het toetsen van change management volgens de SCRUM methodiek. Het ontwikkelde normenkader is gebaseerd op het bestaande normenkader en aanvullingen voor de geïdentificeerde 'gaps'. De praktische toepasbaarheid van het ontwikkelde normenkader wordt behandeld in een discussie die wordt gevoed door vijf uitgevoerde interviews met subject-matter experts.

4 Literatuurstudie

4.1 Scrum: Definities en uitgangspunten

Om een normenkader te ontwikkelen om change management volgens de SCRUM methodiek te toetsen in het kader van de jaarrekeningcontrole, dient SCRUM te worden gedefinieerd. SCRUM wordt beschouwd als een van de meest voorkomende agile software ontwikkelmethodieken. Dit hoofdstuk bevat een uiteenzetting van gehanteerde definities en kernbegrippen van agile software ontwikkelmethodieken in het algemeen en van SCRUM in het bijzonder.

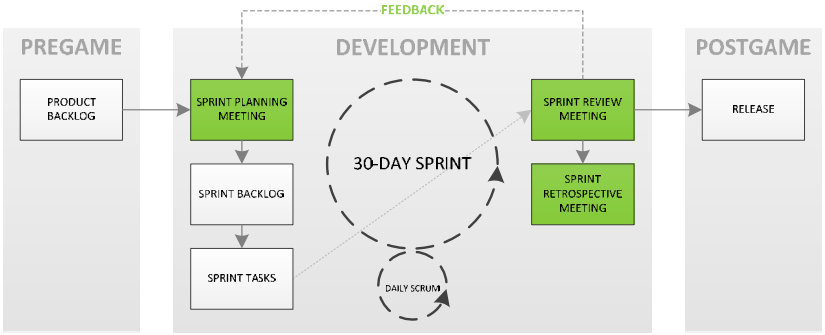
Volgens Strode (2005, 2012) zijn agile methodieken een groep van systeem ontwikkelmethodieken die in eerste instantie niet gericht zijn op een vooraf uitgevoerde analyse, een vooraf opgesteld ontwerp of een vooraf gedefinieerd object. Dit contrasteert met de uitgangspunten van de klassiekere watervalmethode, waarin deze zaken wel een prominente rol innemen in het ontwikkelproces (Trijsenaar en Zalm, 2013).

Strode (2006) stelt dat een agile software ontwikkelmethodiek ontworpen is voor het management en de ondersteuning van een iteratief en incrementeel ontwikkelproces van business systemen, in omgevingen waar verandering constant is, waarbij in kleine teams software wordt geproduceerd door communicatie, feedback, leerervaringen en frequente meetings en waarbij modelleren en documentatie niet een voornaam belang hebben.

SCRUM wordt voor het eerst benoemd door Takeuchi en Nonaka (1986), maar volgens Strode (2005) is SCRUM als software ontwikkelmethodiek geïntroduceerd en uitgewerkt door Beedle et al. (1999) en Schwaber en Beedle (2002). Beedle et al. (1999) definiëren SCRUM als ontwikkelmethodiek door de technieken te beschrijven waarmee de ontwikkelaars de chaos en de complexiteit van de veranderende omgeving kunnen pareren. Een belangrijke methode om de voortgang in het ontwikkelproces in een continu

veranderende omgeving te waarborgen, is het betrekken van het management door middel van frequente besprekingen omtrent tekorten en belemmeringen (Abrahamsson et al., 2003).

SCRUM wijkt voornamelijk af van de andere agile methodieken door de unieke procesgang. Zie hieronder voor een schematische weergave van het SCRUM ontwikkelproces, gebaseerd op verschillende (grafische) beschrijvingen van het proces (Abrahamsson et al., 2002; Highsmit, 2002; Strode, 2005; Mahnic en Vrana, 2007; Mahnic en Zabkar, 2007; Collyer en Manzano, 2013):



Figuur 1: Schematische weergave SCRUM ontwikkelproces

Het product backlog is een lijst van wensen en eisen, afkomstig van verschillende stakeholders (Abrahamsson, 2002). Tijdens de sprint planning meeting wordt door de product eigenaar een prioritering gemaakt van items die in de eerstvolgende sprint meegenomen moeten worden, waarna het ontwikkelteam hiervoor de bijbehorende taken en een inschatting van de benodigde tijd maakt. Op basis van het overleg binnen de sprint planning meeting wordt de sprint backlog opgesteld (Mahnic en Zabkar, 2007) als input voor de eerstvolgende sprint. Highway (2002) benadrukt het belang van een sprint goal om te voorkomen dat het SCRUM team zich verliest in de details van de afzonderlijke taken.

In een sprint worden verschillende taken uitgevoerd die zijn opgenomen in de sprint backlog. Binnen de sprint is er geen sprake van een vooraf gedefinieerd proces (Beedle et al., 1999). De lengte van een sprint varieert tot maximaal 1 kalendermaand (Beedle et al., 1999; Abrahamsson et al., 2002, Highway, 2002). Om de voortgang te bewaken, wordt dagelijks een 15-minuten durende SCRUM meeting gehouden waarin ieder lid van het SCRUM team antwoord geeft op de vragen ‘wat heb je gedaan sinds de laatste dagelijkse SCRUM meeting’, ‘wat ga je doen voor de volgende SCRUM meeting’ en ‘zijn er belemmeringen in het ontwikkelproces’ (Mahnic en Zabkar, 2008).

Aan het eind van de sprint vindt een sprint review meeting plaats waarin de voortgang wordt besproken en een demonstratie van het eindresultaat wordt gegeven aan de klant (Highway, 2002). Het testen van een redelijk gedeelte van de ontwikkelde software is volgens Beedle et al. (1999) ook onderdeel van de sprint review meeting. Feedback vanuit de sprint review meeting wordt besproken in de sprint planning meeting voor de eerstvolgende sprint. In een aantal beschrijvingen van het SCRUM proces wordt ook een sprint retrospective meeting benoemd (Mahnic en Vrana, 2007) die plaatsvindt tussen de sprint review meeting en de volgende sprint planning meeting om het SCRUM team opties tot verbetering aan te laten dragen.

Indien er als gevolg van een sprint of een iteratie van sprints een onderdeel van de software is die in productie kan worden genomen, wordt deze in productie genomen. Abrahamsson et al. (2002) onderschei-

den een post-ontwikkelfase waarin ruimte is voor de voorbereiding van de in-productie name van de software door het uitvoeren van integratie- en systeemtesten.
In de onderstaande tabel zijn de belangrijkste stakeholders binnen het SCRUM proces weergegeven inclusief taken, verantwoordelijkheden en belangen. Deze tabel is ontstaan door de beschrijving van Abrahamsson et al. (2002), Mahnic en Vrana (2007) en Mahnic en Zabkar (2007, 2008) te combineren:

STAKEHOLDER	VERANTWOORDELIJKHEDEN	BELANGEN
(IT) Management	Verantwoordelijk van het kiezen van de product owner; Opstellen van de product backlog;	Timely Information on Project Performance; Quality Improvement;
Product Owner / Customer	Bewaken eindresultaat van het SCRUM proces; Opstellen van de product backlog;	Customer Satisfaction;
Scrum Master	Bewaken van SCRUM waardes en principes; Bewaken voortgang vs. planning; Oplossen belemmeringen tijdens SCRUM proces;	Efficient Impediments Resolution;
Team Members	Ontwikkelen software; Samenstellen sprint backlog;	Job Satisfaction;

Tabel 1: Stakeholders in SCRUM ontwikkelproces: verantwoordelijkheden en belangen

4.2 Scrum: Meetbaar en toetsbaar

Het doel om uiteindelijk een normenkader te ontwikkelen om de SCRUM methodiek te toetsen in het kader van de jaarrekeningcontrole, impliceert dat de procesgang van de SCRUM ontwikkelmethodiek toetsbaar en meetbaar is. Dit hoofdstuk bevat zowel een introductie van modellen die bedacht zijn om dit proces meetbaar te maken zonder afbreuk te doen aan de principes van agile en SCRUM als een uitwerking van de normenkaders die zijn opgesteld door Collyer en Manzano (2013), Kim et al. (2013) en Trijsenaar en Zalm (2013). In deze scriptie zullen deze modellen als input dienen voor het concept normenkader wat de IT auditor kan gebruiken in het kader van het toetsen van de geautomatiseerde gegevensverwerking door applicaties die volgens de SCRUM methodiek ontwikkeld worden.

Het ontbreken van meeteenheden in het SCRUM proces is voor Mahnic en Vrana (2007) en Mahnic en Zabkar (2007, 2008) aanleiding geweest om een model op te stellen waarmee het software ontwikkelproces kan worden gemonitord en verbeterd rekening houdend met de verschillende stakeholders.

Mahnic en Zabkar (2007, 2008) hebben getracht om de meeteenheden in het AGIT (AGIle software developmenT) model aan de hand van ITGI COBIT (2007) en ISACA (2008) te koppelen aan het COBIT model (versie 4.1). Met deze mapping hebben Mahnic en Zabkar (2007, 2008) willen aantonen dat het AGIT model voldoende waarborgen biedt om te voldoen aan de algemene auditcriteria die gelden voor informatiesystemen, zoals deze zijn verwerkt in het COBIT model. Het AGIT model biedt handvatten, die gebruikt kunnen worden voor het opstellen van een concept normenkader.

Hieronder worden drie normenkaders behandeld, die in verschillende mate zijn aangepast aan de specifieke kenmerken van SCRUM.

Collyer en Manzano (2013) komen tot de conclusie dat er in feite twee conflicten ontstaan. Ten eerste, in de agile ontwikkelmethodiek worden tijdens de ontwikkeling nieuwe vereisten en wensen verwerkt in de software. Ten tweede, bij agile ontwikkelmethodieken wordt minimale aandacht besteed aan vastlegging

van uitgevoerde testwerkzaamheden. Zij stellen dat het eerste conflict opgelost kan worden door voldoende diepgang te betrachten in de set van vereisten aan het begin van het ontwikkelproces. De auteurs merken op dat het niet zinvol is om het SCRUM team naar eigen inzicht functionaliteiten van de software te laten ontwikkelen. Op basis van de uitgebreide product backlog kan, parallel aan het ontwikkelproces, een hoogover testplan worden opgesteld. Het tweede conflict wordt ondervangen door bij elke release een 'verharde' sprint uit te voeren waarbij ervoor wordt gekozen om voor deze sprint de vereisten, testverslagen en akkoorden wel uitvoerig vast te leggen.

Waar Collyer en Manzano (2013) het huidige normenkader ongewijzigd laten en voorstellen om op onderdelen de SCRUM methodiek aan te passen, stellen Kim et al. (2013) een driedimensionaal audit model voor, waar 'audit point', 'audit domain' en 'audit viewpoint' centraal staan. Het resultaat van hun analyse is een checklist, waarin enkel de dimensie 'audit point' wordt meegenomen. Het 'audit domain' heeft betrekking op het audit object, dat in deze context het change management proces is, en het 'audit viewpoint' beschrijft het niveau waarop de audit wordt uitgevoerd (proces, product of performance).

In tegenstelling tot de normenkaders van Collyer en Manzano (2013) en Kim et al. (2013), hebben Trijsenaar en Zalm (2013) geen gebruik gemaakt van een bestaand normenkader. Zij concluderen over de wijze waarop agile methodieken in het algemeen en SCRUM in het bijzonder ge-audit kunnen worden, met de stelling: 'met een auditwerkwijze die aansluit op de controleerbare objecten die in Agile-methoden worden gerealiseerd, zoals Agile-ontwikkeldocumentatie (use cases en burndown charts), de werking van het Agile-proces en de bijbehorende randvoorwaarden en andere projectstuurparameters, kan Agile-softwareontwikkeling goed ge-audit worden'. Hieronder zijn deze vier elementen en de bijbehorende toetsbare items in een tabelvorm weergegeven om inzicht te verschaffen in het normenkader wat Trijsenaar en Zalm (2013) voorstellen:

ELEMENT	TOETSBAAR ITEM
Agile-ontwikkeldocumentatie	Use cases (aanwezigheid / accordering / format)
	Burndown chart
Werking Agile-proces	Sprint planning meeting
	Sprint backlogs
	Sprint retrospective meeting
Randvoorwaarden Agile-proces	SCRUM team (samenstelling / ervaring)
	Product owner (senioriteit business vertegenwoordiging)
	Communicatie SCRUM team en product owner
Projectstuurparameters	Functionaliteit
	Kwaliteit

Tabel 2: Agile Audit Model Trijsenaar en Zalm (2013) (in tabelvorm)

De auteurs van de drie behandelde normenkaders hebben in onvoldoende mate gespecificeerd in welke context en met welk doel deze modellen gehanteerd kunnen worden en daarom verschillen de modellen in de mate waarin deze zijn aangepast aan de specifieke kenmerken van SCRUM. Deze scriptie heeft als doel om een normenkader te ontwikkelen wat door de IT auditor gebruikt kan worden in het kader van de jaarrekeningcontrole om change management volgens de SCRUM methodiek te toetsen. In de praktische toetsing wordt eerst aangetoond op welke onderdelen het huidige normenkader niet voldoet en vervolgens wordt een concept normenkader voorgesteld en wordt waar mogelijk gebruik gemaakt van bestaande auditmodellen om de geïdentificeerde 'gaps' te dichten.

5 Praktische toetsing

5.1 Toetspunten Change Management

Hieronder staat de analyse aan de hand van eerder uiteengezette definities van SCRUM om te bepalen in welke mate het huidige normenkader, dat is gericht op de traditionele watervalmethode, kan worden toegepast op een change management proces dat is ingericht volgens de SCRUM methodiek.

Voor deze scriptie is als 'huidig normenkader' de set gebruikt, die door een van de BIG-4 kantoren wordt voorgeschreven in de audit methodologie en wordt gebruikt in de jaarrekeningcontrole voor het uitvoeren van controlewerkzaamheden inzake change management. De ITGC's uit deze set zullen in de onderstaande analyse dienen als leidraad. De normen en de bijbehorende, traditionele controle procedures worden beschreven en door middel van ontleding van de procedures wordt beoordeeld in hoeverre deze kunnen worden uitgevoerd om change management volgens SCRUM te toetsen. Aan de hand hiervan zijn de 'gaps' in het huidige normenkader geïdentificeerd.

Aan de hand van de theoretische uiteenzetting van de definities, het SCRUM proces en de bijbehorende stakeholders en aan de hand van het traditionele normenkader is een analyse uitgevoerd om te beoordelen in welke mate de traditionele controle procedures toepasbaar zijn op een change management proces wat volgens de SCRUM methodiek is ingericht.

Uit de analyse van de verschillende ITGC's en de controle procedures blijkt dat het huidige normenkader dat gericht is op traditionele ontwikkelmethodieken niet toereikend is om te worden toegepast op change management volgens de SCRUM methodiek. De analyse toont de volgende 'gaps' aan:

- Indien er geen system-generated change log kan worden uitgelezen, kan de volledigheid van de lijst van changes, die in productie zijn genomen in een bepaalde periode, niet worden bepaald aan de hand van de change registratie (deze problematiek bestaat ook in de traditionele aanpak, maar deze 'gap' is hier expliciet opgenomen omdat bij de toepassing van de SCRUM ontwikkelmethodiek de volledigheid van de lijst van changes nog moeilijker is vast te stellen en een directe impact heeft op de manier waarop selecties voor de testwerkzaamheden dienen te worden bepaald);
- De vastlegging van autorisaties van changes, de uitvoering van testwerkzaamheden en het monitoren van het change management proces ontbreken;
- In de beschrijving van de SCRUM modellen wordt onvoldoende aandacht besteed aan het uitvoeren van regressietesten;
- De scheiding van taken en verantwoordelijkheden binnen het change management proces kan niet worden aangetoond;

5.2 Concept normenkader Scrum door IT Auditor

Hierboven is aangetoond dat het huidige normenkader niet toereikend is om toe te passen op een change management proces dat is ingericht volgens de SCRUM principes. Hieronder wordt een concept normenkader voorgesteld, waarmee de IT auditor in het kader van de jaarrekeningcontrole een uitspraak kan doen over de effectiviteit van het change management proces volgens de SCRUM methodiek. Het voorgestelde concept normenkader in Tabel 3 is opgesteld aan de hand van de geïdentificeerde 'gaps' en aan de hand van de in de literatuur aangereikte meeteenheden en modellen. Voor iedere controle procedure in het voorgestelde concept normenkader is een toelichting opgenomen. De praktische toepassing van dit voorgestelde concept normenkader, wordt ten slotte behandeld aan de hand van de vijf uitgevoerde interviews met subject-matter experts.

ITGC	CONTROLE PROCEDURES (TRADITIONEEL)	CONTROLE PROCEDURE (CONCEPT)	TOELICHTING
MC-START: Bepaal de populatie van changes en selecteer een geschikt sample	A. Verzamel een complete lijst (populatie) van changes op relevante componenten uit de IT omgeving voor de periode van het begin van de audit periode tot en met de testdatum door: Uitlezen van een system-generated change log; Opvragen registratie changes;	A. Verzamel een complete lijst (populatie) van sprints (en bijbehorende changes) op relevante componenten uit de IT omgeving voor de periode van het begin van de audit periode tot en met de testdatum door: Uitlezen van een system-generated change log en het maken van een indeling van changes per sprint; Opvragen lijst van alle releases, product backlogs, sprint backlogs en tussentijdse changes en na te gaan of alle changes via sprints in productie zijn genomen;	Waar in de traditionele software ontwikkelmethodiek per change een nieuw stuk software/nieuwe functionaliteit in productie wordt genomen, gebeurt dit bij de SCRUM ontwikkelmethodiek per sprint. Er zijn twee manieren om de definitieve lijst van sprints (en bijbehorende changes) te bepalen. De eerste methode betreft het uitlezen van een system-generated change log. Op basis van deze lijst kan inzichtelijk worden gemaakt welke changes in welke sprint in productie zijn genomen. De tweede methode betreft het opvragen van alle releases (die beschreven zijn in de product backlogs), die in nader detail zijn uitgewerkt in de sprint backlogs. Indien de IT auditor kan vaststellen dat er geen changes buiten de sprints in productie zijn genomen, bevat de lijst van sprints alle onderliggende changes.
	B. Selecteer een geschikt sample.	B. Selecteer een geschikt sample uit de populatie van sprints.	Aan de hand van de populatie sprints, die is verzameld in controle procedure 'MC-START' A, kan een geschikt sample worden bepaald. Hierbij worden 10% van de populatie van sprints geselecteerd met een minimum van 5 sprints en een maximum van 25 sprints.
MC-1: Changes worden geautoriseerd	A. Stel voor de geselecteerde changes vast dat deze op een geschikte manier zijn geautoriseerd.	A. Stel voor de geselecteerde sprints vast dat deze tijdens de sprint planning meeting zijn geaccordeerd.	Aan de hand van de notulen van de sprint planning meeting en de sprint backlogs moet worden vastgesteld dat de sprint is geautoriseerd. Deze controle procedure is o.a. gebaseerd op Trijsenaar en Zalm (2013), die verwijzen naar de toetsbare items om de werking van het Agile proces aan te tonen.
	B. Let op: afhankelijk van het beleid van de	B. Let op: afhankelijk van het beleid van de	Tijdens de sprint kunnen changes worden toegevoegd aan het sprint

ITGC	CONTROLE PROCEDURES (TRADITIONEEL)	CONTROLE PROCEDURE (CONCEPT)	TOELICHTING
	organisatie kunnen in bepaalde situaties autorisaties niet vereist zijn (bijv. minor change).	methodiek kunnen gedurende de sprints specifieke changes, worden toegevoegd aan de sprint backlog zonder expliciete autorisatie.	backlog. Deze changes worden in het overleg tussen de product owner en het SCRUM team toegevoegd, waarbij de SCRUM master toezicht houdt op het SCRUM proces. Gezien het beleid van de SCRUM methodiek en de samenstelling van het SCRUM team (zie ook de controle procedures onder MC-5) hoeven dergelijke changes niet expliciet separaat te worden geautoriseerd.
MC-2: Changes worden getest	A. Stel voor de geselecteerde changes vast dat deze op een geschikte manier zijn getest met als doel om te bevestigen dat de change werkt zoals oorspronkelijk bedoeld.	A. Stel voor de geselecteerde sprints vast dat een eindgebruiker (met voldoende senioriteit) deel uitmaakt van het SCRUM team.	Aan de hand van de notulen van de sprint planning meeting en de sprint review meeting moet worden vastgesteld of een eindgebruiker (met voldoende senioriteit) deel uit heeft gemaakt van het SCRUM team. De belangrijkste taak en verantwoordelijkheid van de eindgebruiker is om tijdens de sprints de acceptatietesten uit te voeren. Indien de gebruiker zijn akkoord geeft tijdens de sprint review meeting, betekent dit dat de testen zijn uitgevoerd.
		B. Stel voor de geselecteerde sprints vast dat bij in-productie name controlewerkzaam-heden zijn uitgevoerd om de werking van de kernfunctionaliteiten aan te tonen.	De organisatie zal aan de hand van een risicoanalyse de kernfunctionaliteiten van de geautomatiseerde gegevensverwerking in kaart moeten brengen. Bij in-productie name van de software moet bijvoorbeeld een (geautomatiseerd) regressietestscript worden gedraaid.
MC-3: Changes worden goedgekeurd	A. Stel voor de geselecteerde changes vast dat deze zijn goedgekeurd voordat deze in productie worden genomen.	A. Stel voor de geselecteerde sprints vast dat deze tijdens de sprint review meeting zijn geaccordeerd.	Aan de hand van de notulen van de sprint review meeting moet worden vastgesteld dat de sprint is geaccordeerd. Deze controle procedure is o.a. gebaseerd op Trijsenaar en Zalm (2013), die verwijzen naar de toetsbare items om de werking van het Agile proces aan te tonen.
MC-4: Changes worden gemonitord	A. Verzamel documentatie waaruit blijkt dat het change management proces periodiek wordt ge-	A. Stel vast dat IT management periodiek wordt geïnformeerd over: Kwaliteit van het	Aan de hand van de door Mahnic en Vrana (2007) en Mahnic en Zabkar (2007, 2008, 2008) geïdentificeerde variabelen omtrent de kwaliteit en de voortgang van het SCRUM proces, kan

ITGC	CONTROLE PROCEDURES (TRADITIONEEL)	CONTROLE PROCEDURE (CONCEPT)	TOELICHTING
	monitord (periodiek change overleg / periodiek review van in productie genomen changes).	SCRUM proces (error density / cost of rework / fulfilment of scope); Voortgang (work effectiveness / schedule performance index / cost performance index of labor) costs;	het IT management periodiek worden geïnformeerd en kan het IT management op basis van deze stuurinformatie het SCRUM proces monitoren.
		B. Stel voor de geselecteerde sprints vast dat IT management aanwezig is bij de sprint planning meeting en de sprint review meeting.	Aan de hand van de notulen van de sprint planning en review meeting kan worden aangetoond dat IT management aanwezig is en betrokken is bij het ontwikkelproces. Omdat IT management de functie heeft om het change management proces van een hoger niveau te monitoren, kunnen zij in dergelijke meetings relevante informatie leveren.
MC-5: Er is voldoende functiescheiding ingericht in het change management proces	A. Stel vast dat, zowel organisatorisch als logisch, verschillende personen de volgende taken binnen het change management proces uitvoeren: Aanvragen / autoriseren van een change; Ontwikkelen van een change; In-productie nemen van ontwikkelde changes; Monitoren van changes;	A. Stel vast voor de geselecteerde sprints dat de verschillende rollen binnen het SCRUM proces (IT management / product owner / SCRUM master / SCRUM team) zijn ingevuld door de juiste personen: Stel vast dat de SCRUM master gecertificeerd is; Stel vast dat het SCRUM team op een juiste manier is samengesteld en over voldoende senioriteit beschikken; Stel vast dat het SCRUM proces volgens de juiste principes is uitgevoerd (dagelijkse meeting á 5 minuten);	De norm 'MC-5: Er is voldoende functiescheiding ingericht in het change management proces' is opgesteld om het risico af te dekken dat een change door eenzelfde persoon wordt ontwikkeld en in productie kan worden genomen. Aan de hand van de notulen van de sprint planning meeting en de sprint review meeting kan voor de geselecteerde sprints de samenstelling van het SCRUM team en de SCRUM master worden achterhaald. Op deze manier kan worden vastgesteld of de individuen in het SCRUM team over voldoende senioriteit beschikken. Deze controle procedure is o.a. gebaseerd op Trijsenaar en Zalm (2013), die verwijzen naar de toetsbare items om de werking van het Agile proces aan te tonen. Aan de hand van interviews met de SCRUM master en individuen uit het SCRUM team van de geselecteerde

ITGC	CONTROLE PROCEDURES (TRADITIONEEL)	CONTROLE PROCEDURE (CONCEPT)	TOELICHTING
			sprints kan worden vastgesteld in welke mate de principes van het SCRUM proces zijn gevolgd, omdat deze principes het toezicht en de communicatie tussen de verschillende teamleden waarborgt.
		B. Stel vast dat personen uit het SCRUM team de ontwikkelde software niet in productie kunnen nemen.	Indien individuen uit het SCRUM team geen mogelijkheid hebben om software in productie te nemen, is er sprake van een duidelijke scheiding tussen de ontwikkelomgeving en de productieomgeving.

Tabel 3: Voorgestelde concept normenkader

5.3 Validatie normenkader Scrum voor IT Auditor

Het voorgestelde concept normenkader dat hierboven is gepresenteerd, is gebaseerd op een theoretische analyse van het huidige normenkaders met de 'traditionele' controle procedures enerzijds en een uiteenzetting van de SCRUM principes en methodieken anderzijds. De doelstelling van het onderzoek, namelijk om een normenkader op te stellen dat de IT auditor kan hanteren om change management volgens de SCRUM methodiek te toetsen in het kader van de jaarrekeningcontrole, vereist dat het voorgestelde concept normenkader wordt geconfronteerd met de auditpraktijk. Voor dit onderzoek zijn vijf subject-matter experts geïnterviewd.

De subject-matter experts hebben allemaal minimaal 3 jaar IT audit ervaring en zijn allemaal werkzaam binnen de financiële sector. Voor dit onderzoek zijn drie IT auditors geïnterviewd die geen relevante ervaring hebben binnen de financiële auditpraktijk (type 1). In deze interviews is ten eerste aandacht besteed aan de casi waarin de geïnterviewden controlewerkzaamheden hebben uitgevoerd om change management volgens de SCRUM methodiek te toetsen in het kader van de jaarrekeningcontrole, de door hen in deze casi toegepaste normenkaders en de bijbehorende issues. Ten tweede is het concept normenkader besproken, waarbij voornamelijk aandacht is besteed aan de vaktechnische vereisten en de praktische toepasbaarheid van de voorgestelde concept controle procedures. Daarnaast zijn er twee IT auditors geïnterviewd die wel relevante ervaring hebben binnen de financiële audit praktijk (type 2). De opbouw van de interviews met deze IT auditors heeft zich voornamelijk gericht op de vaktechnische vereisten van de controle procedures, uitgevoerd door de IT auditor, vanuit het perspectief van de financiële auditpraktijk. Voor dit onderzoek zijn deze auditors geselecteerd vanwege hun relevante werkervaring binnen zowel de financiële auditpraktijk en de IT audit praktijk, omdat zij de impact van de controle procedures van de IT auditor op de jaarrekeningcontrole het beste kunnen inschatten.

Aan de hand van de confrontatie tussen het voorgestelde concept normenkader, de discussies omtrent de verschillende praktijk casi en de vaktechnische vereisten van uitgevoerde controle procedures is het eindproduct van dit onderzoek tot stand gekomen. Om het proces van de totstandkoming van dit eindproduct inzichtelijk te maken, is er voor gekozen om de verschillende normen uit
Tabel *3* te hanteren. Naar aanleiding van de interviews is hier een behandeling omtrent de context aan toegevoegd.

5.3.1 Type organisatie en applicatie (MC-Context)

Zowel het traditionele normenkader als het voorgestelde concept normenkader is ontwikkeld in de veronderstelling dat er sprake kan zijn van een generiek toepasbaar normenkader. Echter, in theorie zou elk normenkader toegespitst moeten worden op de change management procedure die door een gebruikersorganisatie op basis van een gedegen risicoanalyse is opgesteld. Uit de interviews bleek bijvoorbeeld dat organisaties vaak een tussenvorm hanteren, waarbij SCRUM principes zijn geïntegreerd in de bestaande change management processen. De IT auditor moet daarom een beoordeling uitvoeren van de opzet van het change management proces en hierbij de volgende drie elementen ten minste in acht te nemen: de context van het 'type organisatie', het 'type applicatie' en de 'werkwijze en diepgang van documentatie' die de organisatie hanteert.

In toenemende mate wordt binnen organisaties gebruik gemaakt van de SCRUM methodiek in het change management proces. Een IT auditor dient in eerste instantie vast te stellen of de gehanteerde change management procedure in opzet de specifieke risico's van de betreffende organisatie afdekken. De organisatie-specifieke risico's worden onder andere bepaald door de aard van het 'type organisatie'.

Uit de interviews blijkt dat dat niet de afzonderlijke elementen 'type organisatie', 'type applicatie' en 'documentatie' bepalen of SCRUM toepasbaar is in een bepaalde context, maar dat juist de samenhang tussen deze elementen bepalend is voor de beoordeling van de opzet van proces.
In het algemeen zijn de geïnterviewden het er over eens dat het 'type applicatie' mede bepaald of SCRUM wel of niet kan worden gehanteerd in de ontwikkeling en het onderhoud van deze applicaties.

Ten slotte, in het voorgestelde concept normenkader is het uitgangspunt dat er vastlegging plaatsvindt van de product backlogs, de sprint backlogs, de notulen van de sprint planning meetings en de sprint review meetings. Hoewel dit niet volledig volgens de agile principes is, vergt het daarom inzet van organisaties die de SCRUM methodiek toepassen in het onderhoud van de kritische applicaties. De IT auditor zal moeten bepalen of er handvatten zijn om überhaupt een beoordeling te kunnen uitvoeren.

In het traditionele normenkader en in het voorgestelde concept normenkader zijn geen separate normen of controle procedures opgenomen, die er toe leiden om de opzet van het change management proces kritisch te beoordelen aan de hand van de context. Derhalve is in het eindproduct van dit onderzoek de norm 'MC-CONTEXT' expliciet opgenomen met de bijbehorende controle procedures:

ITGC	CONTROLE PROCEDURE (DEFINITIEF)
MC-CONTEXT	A. Voer een beoordeling uit van de opzet van het change management proces en besteed hierbij specifieke aandacht aan: Type organisatie; Type applicatie; Werkwijze en diepgang documentatie; Samenhang tussen hierboven genoemde elementen;

Tabel 4: Definitief normenkader 'MC-CONTEXT'

5.3.2 Populatie en sample (MC-Start)

In dit onderzoek is gekozen om de controle procedures, die betrekking hebben op het verzamelen van de populatie en het bepalen van een geschikt sample, te combineren in de stap 'MC-START'.

In de controle procedures volgens het traditionele normenkader, vormt de IT auditor een oordeel over de effectieve werking van het change management proces op basis van een willekeurige selectie van changes

uit de populatie van changes uit de betreffende audit periode. In het voorgestelde concept normenkader zijn twee manieren geopperd om de populatie te bepalen: de populatie kan worden bepaald aan de hand van een system-generated log of aan de hand van een lijst van alle sprints. In aanvulling hierop werd door de geïnterviewden met een financial audit achtergrond (type 2) geopperd om de populatie op te bouwen aan de hand van programmaplan / changeplan voor het betreffende jaar. Deze drie verschillende manieren van het bepalen van de populatie zijn terug te herleiden naar de manier waarop een change wordt gedefinieerd, namelijk respectievelijk als system change, sprint en projectchange. Hieronder wordt eerst elk van deze werkwijzen behandeld en wordt ten slotte een kritische beschouwing gegeven van de sample selectie voorschriften.

Ten eerste, het bepalen van de populatie via een system-generated log is in een beperkt aantal situaties toepasbaar. Zelfs indien het praktisch mogelijk is om zo'n lijst te genereren en de betrouwbaarheid hiervan vast te stellen, zal er een extra slag moeten worden gemaakt om voor elk van de items in het log te herleiden in welke sprint deze is ontwikkeld, is getest en in productie is genomen.

Een tweede manier om de populatie van changes te bepalen is aan de hand van een lijst van sprints die door de organisatie zijn uitgevoerd en die hebben geleid tot de in productie name van nieuwe of bijgewerkte software.

Waar het bij de eerste en de tweede methode van belang is dat er sprake is van een volledige populatie, zodat middels een willekeurige selectie kan worden bepaald dat er sprake is van een uniforme werkwijze voor alle typen wijzigingen (groot, klein en spoed), is de derde methode (programmaplan / changeplan) gebaseerd op een risicoperspectief, waarbij er wellicht minder wordt gefocust op het aspect volledigheid.

Uiteindelijk zijn alle werkzaamheden die in het kader van de jaarrekeningcontrole uitgevoerd worden en de hierbij gehanteerde strategie en aanpak gericht op de vraag: bevat de jaarrekening een afwijking van materieel belang? De derde aanpak ligt in lijn met deze houding. Echter, om tegemoet te komen aan het volledigheidsaspect en het risico ten aanzien van relatief kleine wijzigingen af te dekken, kan er aanvullend een hygiëne check worden uitgevoerd.

De controle procedure voor het bepalen van de populatie van changes is gelinkt aan het bepalen van de sample selectie. De eerste twee werkwijzen zijn gericht op de volledigheid van en de uniformiteit binnen de populatie van changes. Om een oordeel te geven over de werking van het change management proces, is het logisch om een willekeurig sample te selecteren met behulp van een random generator en voor de geselecteerde items te bepalen of deze conform de change management procedure in productie zijn genomen. Echter, men zou kunnen beweren dat het toetsen van het change management proces op die manier een doel op zich is geworden en ook in een context, anders dan de jaarrekeningcontrole, gehanteerd kan worden. Daarentegen, de laatste werkwijze is gebaseerd op een risicoanalyse en lijkt derhalve meer geschikt voor de jaarrekeningcontrole. Ten eerste, de selectie is gericht op de key-items en ten tweede, de selectie is erop gericht om te beoordelen of de kernfunctionaliteiten (application controls) van de geautomatiseerde gegevensverwerking ongewijzigd zijn gebleven.

In het voorgestelde concept normenkader zijn slechts twee methodes opgenomen om de populatie van changes te bepalen en is de aanname dat de huidige sample selectie voorschriften nog steeds gebruikt kunnen worden. Naar aanleiding van de interviews is er een derde werkwijze voor de populatie bepaling opgenomen en is de koppeling met de controle procedure voor sample selectie aangescherpt:

ITGC	CONTROLE PROCEDURE (DEFINITIEF)
MC-START: Bepaal de populatie van changes en selecteer een geschikt sample	A. Verzamel een complete lijst (populatie) van sprints (en bijbehorende changes) op relevante componenten uit de IT omgeving voor de periode van het begin van de audit periode tot en met de testdatum door het: Uitlezen van een system-generated change log en het maken van een indeling van changes per sprint; Opvragen lijst van alle releases, product backlogs, sprint backlogs en tussentijdse changes en nagaan of alle changes via sprints in productie zijn genomen; Opvragen programma changes e.d. en nagaan welke grote programma-changes in productie zijn genomen via SCRUM trajecten;
	B. Selecteer een geschikt sample uit de populatie van sprints: Indien de populatie tot stand komt door middel van system-generated log of lijst van sprints, bepaal een willekeurig sample volgens traditionele voorschriften; Indien de populatie tot stand komt door middel van een risicoanalyse, bepaal een sample op basis van key-item testing en selecteer daarnaast items t.b.v. hygiene testing;

Tabel 5: Definitief normenkader 'MC-START'

5.3.3 Autoriseren van changes (MC-1)

In de traditionele watervalmethodiek heeft het autoriseren van changes betrekking op de expliciete goedkeuring door management om geld en resources toe te wijzen aan een bepaald ontwikkeltraject en op het vertalen en vastleggen van de vereisten van de gebruikersorganisatie in een ontwerp. Hieronder worden beide aspecten in relatie tot het SCRUM proces behandeld en worden ten slotte de verschillende visies belicht met betrekking tot de autorisatie van sprints in het SCRUM proces.

Ten aanzien van de goedkeuring van management, het is niet de primaire taak van een IT auditor om in het kader van de jaarrekeningcontrole een uitspraak te doen over de (effectieve) urenbesteding van het SCRUM team van ontwikkelaars. Echter, aan de hand van de goedkeuring van budgetten kan worden vastgesteld dat er een bepaalde mate van support is vanuit management voor de ontwikkeltrajecten.

Het niveau van goedkeuring door management zal veelal op een hoger niveau plaatsvinden en zal niet expliciet worden gegeven voor individuele ontwikkeltrajecten of sprints. In feite moet de IT auditor voor de in stap 'MC-START' geselecteerde sprints vaststellen of deze onderdeel uitmaken van een door management goedgekeurd programma, project of andersoortig traject.

De vastlegging van de vereisten liggen in de SCRUM methodiek niet vast door middel van een formeel uitgewerkt ontwerp, maar is zichtbaar in het wensenlijstje wat door van de gebruikersorganisatie kenbaar wordt gemaakt aan het SCRUM team in de product backlog en de hiervan afgeleide sprint backlog. Indien er formele vastlegging plaatsvindt van de sprint planning meetings kan hiermee de autorisatie van de geselecteerde sprint worden vastgesteld, omdat de sprint backlog tijdens deze meeting wordt bepaald. Het is hierbij voornamelijk van belang om vast te stellen dat de product owner aanwezig is geweest bij de sprint planning meeting.

De visie van de verschillende geïnterviewden ten aanzien van de autorisatie van sprints, lopen uiteen. Hieronder zijn twee uitersten van het spectrum beschreven. De ene geïnterviewde vindt de toetsing van de autorisatie van sprints door de IT auditor niet relevant en neemt MC-1 niet mee in een normenkader voor SCRUM. Deze zienswijze is gebaseerd op de assumptie dat de werkzaamheden die een IT auditor uitvoert voor MC-2 en MC-3 voldoende waarborgen bieden om een oordeel te kunnen geven. De andere geïnterviewde pleit ervoor dat de IT auditor niet enkel toetst of de originele sprint backlog is geautori-

seerd, maar ook vaststelt dat de afwijkingen ten opzichte van de originele backlog (achteraf) zijn geautoriseerd. Deze zienswijze is gebaseerd op het feit dat MC-1 wel noodzakelijk is om een oordeel te kunnen geven. Door te kiezen voor een tussenvorm (tussen SCRUM en waterval) wordt ook aan de vereisten van MC-1 voldaan.

De discussie met de geïnterviewden omtrent autorisatie van sprints heeft geleid tot een aantal aanpassingen in het normenkader. Ten eerste, er is een splitsing aangebracht in de soorten autorisatie die een IT auditor kan beoordelen en ten tweede is er op basis van de tegenstrijdige zienswijzen een nuancering aangebracht. Indien voor een geselecteerde sprint niet kan worden vastgesteld of deze is geautoriseerd, hoeft dit niet te betekenen dat de ontwikkelde programmatuur onbetrouwbaar is. Immers, er kan worden vastgesteld of nieuwe software is getest en goedgekeurd voor productie:

ITGC	CONTROLE PROCEDURE (DEFINITIEF)
MC-1: Changes worden geautoriseerd	A. Stel voor de geselecteerde sprints vast dat deze zijn geautoriseerd door: Vast te stellen dat de sprint onderdeel uitmaakt van een door management goedgekeurd programma, project of andersoortig traject; Vast te stellen dat in overleg met de product owner (vertegenwoordiger van de gebruikersorganisatie) en het SCRUM team een sprint backlog is gedefinieerd (op basis van het product backlog);
	B. Let op: afhankelijk van het beleid / change management procedure van een organisatie kan de expliciete autorisatie voor een sprint backlog ontbreken. Dit hoeft niet per definitie te betekenen dat er sprake is van een ineffectief change management proces. Afhankelijk van MC-2 en MC-3 kan worden vastgesteld dat enkel betrouwbare software in productie wordt genomen;

Tabel 6: Definitief normenkader 'MC-1'

5.3.4 Testen van changes (MC-2)

Hoewel er in het huidige normenkader geen onderscheid wordt gemaakt in verschillende soorten testen, wordt hieronder een onderscheid gemaakt tussen enerzijds functionele testen en anderzijds regressietesten, omdat dit onderscheid in het concept normenkader is geïntroduceerd. De twee typen testen worden hieronder behandeld en leiden ieder tot een aparte bijdrage tot het definitieve normenkader voor het toetsen van SCRUM in het kader van de jaarrekening.

In de beschrijving van de SCRUM ontwikkelmethodiek is reeds duidelijk geworden dat het testen van de ontwikkelde software geen aparte stap in het SCRUM proces is en dat in de theorie minimaal aandacht wordt besteed aan het testen van de ontwikkelde software. Uit de interviews bleek dat ook in de praktijk de testwerkzaamheden en -documentatie niet altijd op het gewenste niveau worden uitgevoerd en vastgelegd.

Om alsnog te kunnen vaststellen dat de testwerkzaamheden die worden uitgevoerd in een van de geselecteerde sprints voldoende diepgang hebben, was in het concept normenkader voorgesteld om vast te stellen dat een eindgebruiker met voldoende senioriteit deel uitmaakt van het SCRUM team. De interviews wezen uit er bezwaren zijn tegen een dergelijke controle aanpak van de IT auditor. Ten eerste, in veel gevallen maken eindgebruikers geen deel uit van het SCRUM team, waardoor het uitvoeren van deze controle procedure niet mogelijk is. Ten tweede, indien de IT auditor wel kan vaststellen dat er een eindgebruiker onderdeel is van het SCRUM team, is dit nog geen garantie voor succes.

Om een bepaalde mate van zekerheid te verkrijgen over de vraag of een geselecteerde sprint is getest, is het dus onvoldoende om achteraf vast te stellen dat een eindgebruiker deel uitmaakte van het SCRUM team. Een oplossing zou kunnen zijn om als auditor deel te nemen aan bepaalde sprint meetings om vast te stellen wat de impact is van de aanwezigheid van een senior eindgebruiker.

Eerder is gesproken over een organisatie waar gekozen is voor een tussenvorm van SCRUM en watervalmethodiek. Hierbij is er aan het eind van iedere sprint een formele gebruikersacceptatietest, waarin de ontwikkelde functionaliteiten worden getest.

Uit
Figuur 1 blijkt dat ook in een change management proces waar SCRUM wordt gehanteerd als ontwikkelmethodiek sprake is van een 'postgame' fase. Hierin wordt de software naar productie gebracht en wordt er een akkoord gegeven. Echter, het is nagenoeg onmogelijk om een onderbouwd akkoord te geven om software in productie te nemen, zonder dat is aangetoond dat de functionaliteit werkt.

ITGC	CONTROLE PROCEDURE (DEFINITIEF)
MC-2: Changes worden getest	A. Stel voor de geselecteerde sprints vast dat de werking van de ontwikkelde functionaliteit is aangetoond door: Vast te stellen of een eindgebruiker (met voldoende senioriteit) deel heeft uitgemaakt van het SCRUM team (hierbij zal de IT auditor een inschatting moeten maken of de eindgebruiker voldoende inspraak heeft gehad: dit zou kunnen door als IT auditor actief deel te nemen aan het SCRUM proces); Te beoordelen op basis waarvan uiteindelijk is besloten om de ontwikkelde software naar productie te nemen (indien ontwikkelde software zonder onderbouwing naar productie wordt genomen, is er sprake van een ineffectief change management proces);

Tabel 7: Definitief normenkader 'MC-2 (FUNCTIONEEL)'

In de beschrijving van de controle procedures voor het bepalen van het sample ten behoeve van het definitieve normenkader is reeds benoemd dat de werkzaamheden die een IT auditor in het kader van de jaarrekening uitvoert ten aanzien van het change management proces uiteindelijk erop gericht zijn om te kunnen vaststellen dat de kernfunctionaliteiten (application controls) van de geautomatiseerde gegevensverwerking ongewijzigd zijn gebleven. Waar in de vorige paragraaf de nadruk vooral lag op de testwerkzaamheden die door een organisatie worden uitgevoerd om vast te stellen dat de nieuwe functionaliteiten in de ontwikkelde software op een juiste manier werken, is deze paragraaf gericht op de testwerkzaamheden die door een organisatie worden uitgevoerd om aan te tonen dat de bestaande kernfunctionaliteiten (application controls) niet worden aangetast door de ontwikkelde software.

Tijdens de interviews zijn er verschillende methodes besproken, die door organisaties worden gehanteerd om dergelijke regressietesten uit te voeren.

De scope van de IT auditor die werkzaamheden uitvoert ten aanzien van het change management proces, is in feite zeer beperkt. Indien de IT auditor kan vaststellen dat de regressietest de effectieve werking van de kernfunctionaliteit (application controls) aantoont en indien het mogelijk is om voor de software die is ontwikkeld in de geselecteerde sprints vast te stellen dat de regressietest is uitgevoerd, dan is het zelfs van ondergeschikt belang of de functionele test uit de vorige paragraaf wordt uitgevoerd. Echter, het uitvoeren van een integrale regressietest is een tijdrovende activiteit voor de organisatie en derhalve zal per sprint moeten worden beoordeeld of het nodig is om een dergelijke test uit te voeren.

Naar aanleiding van de interviews zijn er een aantal aanpassing gemaakt aan de controle procedures in het definitieve normenkader. Ten eerste, het is cruciaal dat de IT auditor vaststelt dat voor alle kernfunctionaliteiten (application controls) die kritisch zijn vanuit de controle van de jaarrekening, er testgevallen zijn gedefinieerd in de regressietest en dat de testgevallen de risico's omtrent de kernfunctionaliteit in voldoende mate afdekken. Ten tweede, (voornamelijk als de regressietest handmatig wordt uitgevoerd) voor organisaties kan het een intensieve activiteit zijn om een integrale regressietest uit te voeren, waardoor dit niet voor alle geselecteerde sprints wordt uitgevoerd. In deze gevallen dient de IT auditor te beoordelen in hoeverre er een risico-inschatting is gemaakt door de organisatie.

ITGC	CONTROLE PROCEDURE (DEFINITIEF)
MC-2: Changes worden getest	B1. Stel vast dat de door de organisatie gehanteerde regressietest en de uitgevoerde testgevallen de risico's ten aanzien van de kernfunctionaliteit (application controls) in voldoende mate afdekken; B2. Stel vast voor de geselecteerde sprints dat bij in-productie name een regressietest is uitgevoerd. Indien een dergelijke test niet is uitgevoerd, stel vast in welke mate de ontwikkelde software een impact heeft op de bestaande kernfunctionaliteiten (bij voorkeur op basis van een door de organisatie opgestelde risico-inschatting);

Tabel 8: Definitief normenkader 'MC-2 (REGRESSIE)'

5.3.5 Goedkeuren van changes (MC-3)

In de 'postgame' fase vindt de daadwerkelijke in productie name plaats. Alle geïnterviewden hebben benadrukt dat de goedkeuring van de in-productie name van nieuw ontwikkelde software ook met SCRUM vereist is.

De vorm en de frequentie van de accordering is afhankelijk van de manier waarop het SCRUM proces exact is gedefinieerd. Het akkoord voor in-productie name kan plaatsvinden aan het eind van een iteratie van sprints of per sprint en kan worden vastgelegd middels e-mail of middels een change registratietool.
In feite zijn de controle procedures die een IT auditor uitvoert voor MC-3 binnen een SCRUM proces niet wezenlijk anders dan hij uitvoert binnen een change management proces volgens de watervalmethodiek. Naar aanleiding van de interviews zijn de controle procedures verruimd: in de praktijk wordt het akkoord niet altijd gegeven binnen de sprint review meeting, maar ook wel in de 'postgame' fase.

ITGC	CONTROLE PROCEDURE (DEFINITIEF)
MC-3: Changes worden goedgekeurd	A. Stel voor de geselecteerde sprints vast dat de hierin ontwikkelde software is goedgekeurd, voordat deze in productie is genomen door: Akkoord in de notulen van de sprint review meeting terug te vinden; Akkoord in een e-mail terug te vinden; Akkoord in change registratie tool terug te vinden;

Tabel 9: Definitief normenkader 'MC-3'

5.3.6 Monitoren van changes (MC-4)

In de praktijk komt het voor dat binnen een organisatie geen expliciete ITGC's is ingericht die betrekking heeft op het monitoren van het change management proces. Desondanks kan in dergelijke gevallen toch worden geconcludeerd dat er 'gesteund' kan worden op het change management proces in het kader van de jaarrekeningcontrole. Niet alle ITGC's in het huidige door de IT auditor gehanteerde normenkader lijken dus even zwaar mee te wegen in het eindoordeel over de effectieve werking van het change ma-

nagement proces. Het is voor de IT auditor niet essentieel of een dergelijke control is ingericht, zolang hij kan vaststellen dat er vanuit (IT) management voldoende aandacht is voor (de context van) het change management proces. Deels heeft dit te maken met de behandelde stap 'MC-CONTEXT'.

In de concept controle procedures die zijn voorgesteld in het normenkader zijn een aantal meeteenheden voorgesteld die de IT auditor kan hanteren om vast te stellen dat er periodiek wordt gerapporteerd over de kwaliteit en de voortgang van het SCRUM proces. Hoewel uit de interviews niet naar voren is gekomen dat deze meeteenheden in de praktijk worden gebruikt, zijn ze wel in het definitieve normenkader opgenomen als handreiking voor de IT auditor.

Om vast te stellen dat het (IT) management in voldoende mate is betrokken bij het SCRUM ontwikkelproces, was voorgesteld om voor de geselecteerde sprints vast te stellen dat IT management betrokken is bij de sprint review meeting. Echter, verschillende geïnterviewden wezen erop, dat meer nog dan formeel vast te stellen dat IT management aanwezig is, het belangrijk is om een beeld te vormen van de interactie met (IT) management.

Zoals beschreven, is het eerste gedeelte van het concept normenkader voor MC-4 ongewijzigd gebleven. Op basis van de interviews is het tweede gedeelte genuanceerd en is een overweging voor de IT auditor opgenomen om bij het SCRUM proces aanwezig te zijn om op die manier vast te stellen op welke manier (IT) management betrokken is bij het ontwikkelproces:

ITGC	CONTROLE PROCEDURE (DEFINITIEF)
MC-4: Changes worden gemonitored	A. Stel vast dat IT management periodiek wordt geïnformeerd over: Kwaliteit van het SCRUM proces (error density / cost of rework / fulfilment of scope); Voortgang (work effectiveness / schedule performance index / cost performance index of labor costs);
	B. Stel voor de geselecteerde sprints vast dat (een vertegenwoordiger van (IT)) management aanwezig is bij de sprint planning meeting en de sprint review meeting. Voor deze controle procedure kan het noodzakelijk zijn om waarneming ter plaatse toe te passen, in plaats van inspectie van documentatie achteraf.

Tabel 10: Definitief normenkader 'MC-4'

5.3.7 Functiescheiding Change Management proces (MC-5)

Volgens het traditionele normenkader dient de IT auditor vast te stellen dat er voldoende functiescheiding is ingericht in het change proces. Hierbij wordt specifieke aandacht besteed aan enerzijds de functiescheiding tussen autoriseren en ontwikkeling van software en anderzijds de ontwikkeling en in-productie name. Zoals besproken is het eerste type functiescheiding vervaagd. Hierdoor komt de nadruk verder te liggen op de functiescheiding tussen ontwikkeling en productie.

In het concept normenkader waren een aantal controle procedures opgesteld, waarbij minder tastbare toetsingselementen met betrekking tot functiescheiding waren besproken, zoals de certificering van de SCRUM master, de samenstelling van het SCRUM team en de mate waarin de principes van SCRUM volgens de SCRUM procesbeschrijvingen werden gevolgd. Uit de interviews kwam naar voren dat deze handvatten niet toereikend zijn om een uitspraak te kunnen doen over de functiescheiding binnen het change management proces.

Daarnaast is in het concept normenkader een controle procedure opgenomen om op technisch niveau vast te stellen dat ontwikkelaars geen toegang hebben tot de productie-omgeving. De geïnterviewden zijn het er unaniem over eens dat een dergelijke strikte scheiding noodzakelijk is.

Uiteindelijk is in het definitieve normenkader voor SCRUM de eerste stap met de 'softere' controls niet verwijderd, maar is er bewust voor gekozen om de volgorde van de controle procedures om te draaien, om het kritische karakter van de eerste controle procedure te benadrukken.

ITGC	CONTROLE PROCEDURE (DEFINITIEF)
MC-5: Er is voldoende functiescheiding ingericht in het change management proces	A. Stel vast dat personen uit het SCRUM team de ontwikkelde software geen toegang hebben tot de productieomgeving en dus niet in staat zijn om de software in gebruik te nemen. Stel voor de geselecteerde sprints vast dat deze in productie zijn genomen door personen die niet in het SCRUM team zitten.
	B. Indien mogelijk, stel vast voor de geselecteerde sprints dat de verschillende rollen binnen het SCRUM proces (IT management / product owner / SCRUM master / SCRUM team) zijn ingevuld door de juiste personen: Stel vast dat de SCRUM master gecertificeerd is; Stel vast dat het SCRUM team op een juiste manier is samengesteld en over voldoende senioriteit beschikken; Stel vast dat het SCRUM proces volgens de juiste principes is uitgevoerd (dagelijkse meeting á 5 minuten); Voor deze controle procedure kan het noodzakelijk zijn om waarneming ter plaatse toe te passen, in plaats van inspectie van documentatie achteraf.

Tabel 11: Definitief normenkader 'MC-5'

6 Conclusie

Het eindresultaat (de tabellen in hoofdstuk 5) van dit onderzoek dient als leidraad voor de IT auditor, zodat in het kader van de jaarrekening op een gestructureerde wijze werkzaamheden uitgevoerd kunnen worden ten aanzien van het change management proces volgens de SCRUM methodiek. Hieronder zijn de voornaamste verschillen ten opzichte van het traditionele normenkader beschreven.

Ten eerste, in het gevalideerde normenkader is er een additionele stap opgenomen, waarin de IT auditor zichzelf een oordeel dient te vormen over de opzet van het change management proces en daarbij vast te stellen, rekening houdend met het type organisatie, het type applicatie en de werkwijze en de diepgang van documentatie van het SCRUM proces, of de gehanteerde werkwijze inzake het change management proces vanuit een risico perspectief een logische en geschikte werkwijze is.

Ten tweede, de controle aanpak van de jaarrekening controle is gebaseerd op het identificeren van risico's, die mogelijk kunnen leiden tot een materiële fout in de jaarrekening. In de traditionele controle aanpak van change management wordt door de IT auditor een oordeel gegeven over de effectieve werking van het proces door voor een willekeurig bepaald sample vast te stellen dat er sprake is van een uniforme behandeling van changes conform het change management proces. In het gevalideerde normenkader is

er een controle procedure opgenomen, waarbij de IT auditor de meest kritische changes en projecten identificeert en op basis hiervan het sample voor de testwerkzaamheden bepaald.

Ten derde, in het gevalideerde normenkader is een controle procedure opgenomen, die betrekking heeft op regressietesten. In feite is het voor de IT auditor, wanneer hij werkzaamheden uitvoert in het kader van de jaarrekening controle niet relevant om vast te stellen of het SCRUM proces op een juiste manier is ingericht, zolang de organisatie bij de in productie name van nieuwe software aantoonbaar vaststelt dat de kritische kernfunctionaliteiten van de programmatuur ongewijzigd zijn.

Ten slotte, in de traditionele controle aanpak van de IT auditor wordt voornamelijk gebruik gemaakt van inspectie van documentatie om op basis daarvan een oordeel te geven over de effectieve werking van het change management proces. Hoewel de essentie van SCRUM niet inhoudt dat er totaal geen aantoonbare vastlegging is, kan de werkwijze van de organisatie ertoe leiden dat de IT auditor proactief dient aan te haken bij belangrijke meetings in het SCRUM proces.

7 Literatuurlijst

Abrahamsson, P., Salo, O., Ronkainen, J., Warsta, J. (2002) Agile Software Development Methods: Review and Analysis, VIT Publications, 478, pp. 1-107

Abrahamsson, P. Warsta, J. Siponen, M.K., and Ronkainen, J. (2003) New Directions on Agile Methods: A Comparative Analysis, Proceedings of the 25th International Conference on Software Engineering, pp. 244-254

Barlow, J.B., Giboney, J.S., Keith, M.J., Wilson, D.W., Schuetzler, R.M., Lowry, P.B., Vance, A. (2011) Overview and Guidance on Agile Development in Large Organizations, Communications of the Association for Information Systems, 29(2), pp. 25-44

Beedle, M., Devos, M., Sharon, Y., Schwaber, K., Sutherland, J. (1999) Scrum: A pattern language for hyperproductive software development in: Harrison, N. Foote, B., Rohnert H. (eds.) Pattern Languages of Program Design, New York: Addison-Wesley, pp. 637-651

Collyer, K., Manzano, J. (2013) Being Agile While Still Being Compliant: A Practical Approach For Medical Device Manufacturers, IBM Paper, March, pp. 1-14

Highsmit, J. (2002) What is Agile Software Development?, The Journal of Defense Software Engineering, 15(10), pp. 4-9

Highsmith, J. (2002) Agile Software Development Ecosystems, Boston: Addison-Wesley

ISACA (2008) IS Standards, Guidelines and Procedures for Auditing and Control Professionals, Information Systems Audit and Control Association, Rolling Meadows

ITGI (2007) COBIT v4.1, Information Technology Governance Institute, Rolling Meadows

Kim, D.H., Kim, D.S., Koh, C., Kim, H.W. (2013) An Information System Audit Model for Project Quality Improvement by the Agile Methodology, International Journal of Information and Education Technology, 3(3), pp. 295-299

Lee, G., Xia W. (2010) Toward Agile: An Integrated Analysis of Quantitative and Qualitative Field Data on Software Development Agility, MIS Quarterly, 34(1), pp. 87-114

Mahnic, V., Vrana, I. (2007) Using Stakeholders-drive Process Performance Measurement for Monitoring the Performance of a Scrum-based Software Development process, Electrotechnical Review, 74(5), pp. 241-247

Mahnic, V., Zabkar, N. (2007) Introducing CMMI Measurement and Analysis Practices into Scrum-based Software Development Process, International Journal of Mathematics and Computers in Simulation, 1(1), pp. 65-72

Mahnic, V. Zabkar, N. (2008) Assessing Scrum-based Software Development Process Measurement from COBIT Perspective, 12th WSEAS International Conference on COMPUTERS, Heraklion, Greece, July 23-25, 1(1), pp. 589-594

Mahnic, V., Zabkar, N. (2008) Using COBIT Indicators for Measuring Scrum-based Software Development, Transactions on Computers, 7(10), pp. 1605-1617

Martens, M., Veldhuijs, G., Hulstijn, J. (2014) Agile Systeemontwikkeling: een Studie naar Projectsucces in de Financiële Sector, MCA, 2(1), pp. 30-38

Schellevis, W., Van Dijk, V. (2014) Jaarrekening Controle in het MKB: IT audit Geïntegreerd in de Controle-aanpak, http://www.nba.nl

Schwaber, K., Beedle, M. (2002) Agile Software Development with Scrum, New Jersey: Prentice Hall

Strode, D. (2005) The Agile Methods: An Analytical Comparison of Five Agile Methods and an Investigation of Their Target Environment, Department of Information Systems, Massey University, Palmerstone North, New Zealand

Strode, D. E. (2006) Agile Methods: A Comparative Analysis in: Mann, S., Bridgeman, N. (eds.) Proceedings of the 19th Annual Conference of the National Advisory Committee on Computing Qualifications, pp. 257-264

Strode, D. (2012) A Theory of Coordination in Agile Software Development Projects, Victoria University of Wellington
Takeuchi, H. en Nonaka, I. (1986) The New Product Development Game, Harvard Business Review, Jan/Feb, pp. 137-146
Trijssenaar, M., Zalm, M. van der (2013) Agile-ontwikkelmethoden Auditen, IT Auditor, nr. 3, pp. 10-14
Westerveld, W. (2014) Great engineers attrack great engineers, Informatie, Sept, pp. 34-37
Yup, M. (2006) Value Based Extreme Programming, Proceedings of AGILE 2006 Conference, pp. 175-184

A reconsideration of the Segregation of Duties audit approach

Investigating a data analytics approach for auditing the presence of segregation of duties at organizations using Microsoft Dynamics AX

Wilbert van Leeuwen
Frank Zandhuis

After graduating with a Masters degree in Organization Design & Development in 2013 (Cum Laude), Wilbert started his career as IT Auditor at EY. After three years of conducting IT audits at large national and international organizations, he was promoted to Manager Data Analytics. In this role Wilbert was responsible for all data analytics projects for the south region of The Netherlands (which includes the Eindhoven, Venlo and Maastricht offices).
In July 2017 Wilbert co-founded a new venture: Peacock Insights. The goal of this venture is to deliver reliable, affordable and manageable Business Intelligence solutions to our clients. In order to achieve this, we deliver and implement BI Accelerators, which are out of the box solutions to get organizations started with BI based on best practices.

Frank Zandhuis graduated (Cum Laude) with a master's degree from the University of Groningen in International Business & Management (specialization Business & ICT) in 2014. Since 2011 he has worked at EY, integrating IT audit work and data analytics.
In 2016 he graduated from the VU University Amsterdam, with a postgraduate master's degree in IT audit, Compliance and Advisory. With the thesis topic of integrating data analytics and segregation of duties checks in Microsoft Dynamics AX audits.
In the past few years Frank has published articles regarding the opportunities and risks of cloud computing and data analytics

1 Introduction

During the last decades, the societal relevance of the accountant is compromised by a number of scandals and failures of professional practice within their profession. A lot of these issues have been widely discussed in the media. Ironically, the usefulness and necessity of the accountant is precisely to prevent auditing scandals, such as the Pincoffs scandal in 1879 (De Vries, 1985) which can be seen as a direct reason for the emergence of the accountant.

The first professional organization, the "Nederlandsch Instituut van Accountants" (NIvA), or translated the "Dutch Institute of Accountants", was established in 1895. In the past 120 years the world of institutes and organizations have changed significantly. Continued extensive globalization, rapid technological developments and an increasing interdependence between processes and IT are just a few examples of these changes.

Another important development is the explosive growth of the volume of transactions within organizations. At the birth of the auditing profession, the volume of transactions was relatively low. Because of this, a substantive audit approach was sufficient. Due to the growth of organizations, and the related volume of transactions, the efficiency and quality of the financial audit was strained. This caused the need to make use of the internal control environment of the client's organization. Furthermore, the complexity of organizations is also continuing to increase.

What do these developments mean for the auditing profession? Is the profession able to adapt to these developments quick enough in order to maintain qualitative audits? Of course audit firms and professional organizations have changed and audit methodologies are adapted to the specific situation of the subject of the audit. The emergence of IT audit within the financial audit is more or less an example of the change that audit firms have made in order to adapt to the changing world. Furthermore, much is talked and written about innovation in the audit, tools such as data analytics are seen as options for increasing quality and efficiency of the audit.

In the past decades multiple investigations have been conducted into the cause of the problems within the audit profession. In 2014 the well-known AFM (Netherlands Authority for the Financial Markets) report "Uitkomsten onderzoek kwaliteit wettelijke controles Big 4-accountantsorganisaties", roughly translated as "Investigation results quality statutory audit Big 4 audit firms", was published. In this report the culture and quality of work within the auditing sector was criticized. What followed was a number of promises, sector initiatives and public debates. The results of this investigation do not mean that audit opinions on financial statement have inappropriately been given. However, the results are an indication that the checks and balances have insufficiently worked and that mistakes cannot be ruled out. Recently the risk of shortcomings related to the audit quality has become painfully clear, since the AFM has imposed fines between €845.000,- and €2.230.000,- to all the Big Four audit firms (Accountant, 2016).

1.1 Goal

The need to improve the quality of work of the auditor exists as long as the profession of auditor itself. Quality improvement is a continuous endeavor. Examples of quality measures are demanding education requirements before an accountant is certified, practical training, professional organizations, disciplinary committees, quality reviews and regulators. At the same time there are pricing pressures in the market, which increases the emphasis on efficiency.

The predominating view is that an increase in quality often leads to an increase in cost because more work has to be performed. Mandatory enablers, templates and work papers are to be performed and

recorded in the audit file. The tension between the need for quality increases without this negatively affecting of the (profit) margins is evident. What then can audit firms change in their audit methodologies to improve quality assurance, with the intention to provide reasonable assurance that material misstatements from their financial statement audits are ruled out? This research aims not to expose the roots of the problems in the auditing profession. However, the purpose of this study is to:

Gain insight into the impact of audit methodologies to the quality and efficiency of audit activities.

1.2 Research questions

Following the described goal of this research, a main research question is formulated:
How can the quality and efficiency of auditing segregation of duties related to the financial statement audit at an organization that makes use of DAX 2012 be increased?

In order to support the structure of this research, multiple sub questions are formulated:

- What is the relevance of the financial statement audit?
- What approaches are used in a financial statement audit?
- What entails the constructs of quality and efficiency with respect to the financial statement audit?
- What is the relevance of Segregation of Duties?
- What is the role of IT and ERP, such as DAX 2012 within organizations?

2 Literature

In order to provide an answer to the research question, the body of (scientific) literature is studied. The focus on this literature study on the research questions defined in section
Research questions.

By answering these five research questions based on the existing body of literature, several perspectives towards the object of this research (defining a framework to audit SoDs which are supported in DAX 2012 and relevant to the financial statement audit) are taken into account.

Figure 1 - Visual schematic overview of role of SoD in three intersecting areas.

As shown in the Figure 1 above, the three perspectives (Financial Audit, Organizational Processes and ERP Systems) are key in understanding what a framework for financial audit relevant SoD analysis in DAX 2012 should entail.

2.1 What is the relevance of the financial statement audit?

The financial statement is meant to provide a reliable overview of the performance of an organization. For decades large organizations and multinationals are obligated to communicate with stakeholders about their performance by means of the publication of its financial statement. This financial statement is audited by independent financial auditors, who are responsible to provide reasonable assurance to the financial statement users that the provided information is reliable. The construct of reasonable assurance is directly related to the public responsibility of the auditor.

In essence, the auditor provides reasonable assurance that the financial statement is free from material misstatements due to error or fraud. A material misstatement is defined as a misstatement that influences the decisions of the financial statement users. Materiality also has a direct impact on the effort needed from the auditor to provide reasonable assurance. Since the materiality is determined by the auditor, the concept of materiality presumes that an auditor is able to determine when an error in the financial statement influences the decisions of the financial statement users.

So it is clear that stakeholders and the related concept of materiality are the basis for the relevance of the financial statement, but who are these stakeholders and to which extent are auditors able to determine materiality in a meaningful manner? The most apparent stakeholders of a financial statement are (institutional) investors and creditors. Researchers like Carcello, Hermanson and McGrath (1992) use this group in particular to research the perspective of financial statement users. Of course there are lots of other less direct stakeholders (i.e. employees, vendors, suppliers, governments, tax authorities and NGOs).

2.2 What approaches are used in a financial statement audit?

In conducting an audit of financial statement, the overall objectives of the auditor are to obtain reasonable assurance about whether the financial statement as a whole is free from material misstatements, whether due to fraud or error, and thereby expressing an opinion on whether the financial statement is prepared and presented in all material respects, in accordance with the applicable financial reporting framework. Within the financial statement audit the audit approach therefore defines how the auditor ensures that he or she gathers sufficient audit evidence in order to conclude that the financial statement is free from any material misstatements. In this section the common audit approaches will be briefly introduced, followed by an introduction of the upcoming of data analytics.

2.2.1 Defining the reliance and substantive audit strategies

In order to obtain reasonable assurance, the auditor needs to obtain sufficient appropriate audit evidence in order to draw reasonable conclusions on which to base the audit opinion. The Audit Risk Model provides guidance in determining when an auditor has obtained sufficient appropriate audit evidence. The audit risk model, discussed in Statement on Auditing Standards (SAS) No. 47 (American Institute of Certified Public Accountants, 1983), is stated as follows:

Figure 2 - Visualization of relationship between inherent risk, control risk and detection risk.

Inherent risk and control risk are the risks that an organization faces and exist independently of the audit. They arise from many factors including, but not limited to, the nature of the organization's business and

the strategies that it undertakes. They can be increased or reduced by management's attitude to risk. Some organizations and strategies are inherently more (or less) risky than others and result in higher (or lower) inherent risks that material misstatements of the financial statements may occur. Management can mitigate inherent risk by implementing effective internal controls. Detection risk is the risk that a material misstatement would not be detected by the auditor's substantive audit procedures and can thereby be controlled by the extend of the substantive audit procedures performed by the auditor (Hogan & Wilkins, 2008).

The Audit Risk Model clearly states a relation between the risk related to the nature of the organization, the effectiveness of the internal control environment and the need for audit procedures to detect possible misstatements. Resultant from this relation the audit procedures can be divided into procedures to assess and test the effectiveness of the internal control environment and substantive procedures to detect misstatements. In their resource, Hogan and Wilkins (2008) conclude that there is a relation between audit fees and internal control effectiveness, whereby the audit fee increases when substantial internal control problems were identified because the audit effort increases when the auditor cannot rely on the internal controls.

The research of Hogan and Wilkins (2008) shows that the audit effort and strategy is impacted by the concepts of the Audit Risk Model. Based on this, two audit strategies are defined. The audit in which the auditor relies on the internal control environment or merely relies on their own substantial audit procedures. Hereafter these two approaches will respectively be labelled as a reliance audit strategy and a substantive audit strategy. Since SoD is of critical importance for organizational processes and the internal control environment, it is also important for the financial audit regardless whether the audit uses a reliance audit strategy or a substantive audit strategy.

2.2.2 Data analytics in the financial statement audit

Concluding that substantive procedures increase when the auditor cannot rely (entirely) on the internal control environment suggests that the substantive audit approach is used as a fallback scenario. Developments like the emergence of data analytics, big data and growing interdependency between Organizational processes and Information Technology Systems might result in other considerations to choose for a substantive audit approach. It is not surprising that all Big Four audit firms emphasize the importance of using data analytics in the financial audit in their public communications (EY, 2015; Raphael, 2015; PWC, 2015; KPMG, 2015). The promise of data analytics to improve audit efficiency and quality exists for decades. Of course data analytics can be used by an organization to improve the internal control system. However, when the auditor performs data analytics as an audit procedure, it is a substantive audit procedure that is not directly related to the internal control environment. In other words, there might be other reasons, besides the substantial internal control problems that might occur, for choosing a substantive audit strategy instead of a reliance strategy. For example, when new possibilities like data analytics arise with the potential to improve the audit relevance (EY, 2015). The integration of data analytics in the financial audit might have a disruptive effect on the considerations of the auditor to choose for a reliance or a substantive audit strategy. In a recent article of one of the Big Four audit firms the following statement is made:

“It’s a massive leap to go from traditional audit approaches to one that fully integrates big data and analytics in a seamless manner.” (EY, 2015)

In the article of EY, three barriers and four so-called “Analytics dilemmas” are mentioned. In the first place, it is argued that capturing the data is time consuming, partly because of the confidentiality of the data and the required approvals. The second barrier is the high diversity in used information systems within and among organizations. Each system uses its own table structure and data model. Building useful

generic analyses is therefore more and more complicated. The third and last barrier is a barrier related to the knowledge and skills of the auditor. EY explains that applying data analytics to gather audit evidence is difficult and that "Auditors need to find the appropriate balance between applying auditor judgment and relying on the results of these analytics." (EY, 2015)

The promise of data analytics to improve audit quality, efficiency and relevance, makes it very suitable to the purpose of this study. At the same time the barriers and analytics dilemmas pose some interesting challenges. Therefore, the approach to audit SoD in the case study of this paper will be based on the use of data analytics. In this way it is possible to determine the impact of an audit strategy on the audit quality and efficiency.

2.3 What entails the constructs of quality and efficiency with respect to the financial statement audit?

In order to define a practicable and useful framework, it is of utmost importance to take the impact on the quality and efficiency of the financial statement audit into account. For years the challenge for audit firms seemed to be to reduce costs, while maintain, or even improve, the audit quality. A partner, cited by Fischer (1996), once stated the following about the construct of quality in the marketspace of financial audit firms:

> *"We're in a marketplace where the product quality is unobservable … Now, if you go out and buy a dozen of eggs, and you break them open and they're rotten, you know it right away. If you buy a sub-GAAS audit you may never know it. Because every audit look the same." (Fischer, 1996, p.223)*

This citation makes clear that it is hard to measure audit quality because it is not, or hardly, observable. In one of her well known articles, DeAngelo defines the quality of audit services as:

"the market-assessed joint probability that a given auditor will both (a) discover a breach in the client's accounting system, and (b) report the breach. The probability that a given auditor will discover a breach depends on the auditor's technological capabilities, the audit procedures employed on a given audit, the extent of sampling, etc. The conditional probability of reporting a discovered breach is a measure of an auditor's independence from a given client." (DeAngelo, 1981, p.186)

This definition of audit quality provides a clear view on the preconditions that are needed in order to deliver quality in an audit. On the one hand audit quality is related to the technical capabilities and the used audit procedures and extent of sampling, on the other hand the quality depends on the independence of the auditor.

Especially the needed technical capabilities are expected to be connected to chosen audit strategies and procedures. The efficiency in an audit is a far simpler construct which can be measured by the audit effort which is generally measured in hours.

2.4 What is the relevance of Segregation of Duties?

In this section, the topic of Segregation of Duties, or abbreviated to SoD, is discussed with a focus on the following three questions: 1) What is SoD? 2) What is the importance of SoD? 3) What is the link between SoD and IT (Information Technology)?

2.4.1 What is SoD?

In 1748, French philosopher Montesquieu wrote in his political discourse "De l'esprit des loix" about, among other things, the need for a separation of powers in government. This concept is today better

known as trias politica. The intent of this system is to separate powers in order to protect (political) liberty.

> *"When the legislative and executive powers are united in the same person, or in the same body of magistrates, there can be no liberty; because apprehensions may arise lest the same monarch or senate should enact tyrannical laws, to execute them in a tyrannical manner." (Montesquieu, 1977, p.202)*

The functionality of SoDs extends beyond the protection of (political) liberty and can be utilized by organizations, for example, to safeguard the correct functioning of internal controls, as exemplified by the following quotation:

> *"SoD is a basic internal control that attempts to ensure that no single individual has the authority to execute two or more conflicting sensitive transactions with the potential to impact the financial statements." (Adolphson & Greis, 2009)*

In summary, with SoD one can separate a process in distinct activities for which the individual responsibilities can be given to different people. Whereby not one single individual is responsible for all consecutive tasks within a process. SoD works by creating opposing interests between different people.

For the scope of the conducted research, emphasis it put on the importance of SoDs for processes within organizations and their impact on society in general.

2.4.2 What is the importance of SoD?

Organizational effectiveness can be increased through having the appropriate organizational structure. This effectiveness is the degree to which an organization attains its short-term (ends) and long-term (means) goals (Robbins & Barnwell, 2006).

Whilst trying to achieve the objectives set out by the management of the organization the organization and its constituents, such as employees, are exposed to risks.

SoD is a basic part of internal control important to organizations for reducing the "risk of both erroneous and inappropriate actions" (Yale, 2015). More specifically, SoD has long been regarded as a method for (Ernst & Young, 2010):

- Help preventing fraud;
- Reducing the risk of (human) error;
- Maintaining checks and balances through internal control;
- Improving control over regulatory compliance (Engdahl, 2013).

Based on the work of Starreveld, the idea of incorporating SoD within the administrative organization in order to improve internal control was popularized. Creating opposing interests between multiple actors who are part of an organizational process will reduce the risk of error and fraud (Koot & Schultjens, 2013).

Besides the importance to internal control in order to reduce the risk of erroneous and inappropriate actions, the impact of scandals due to SoD conflicts or ineffective internal control on society in general have had their effect on the laws and regulations organizations have to abide by. These control driven regulations resulted in the need of regulatory compliance within organizations:

> *"Among the different control strategies to have addressed the issue of effective decentralized compliance enforcement is the principle of segregation of duties or the idea that no single individual*

should be left alone handling a work task from start to finish. This approach forms an important element in recent efforts to develop mechanisms of social control that can improve regulatory compliance" (Engdahl, 2013, p.333).

Because SoD is such an effective measure to prevent fraud, material misstatements and financial statement manipulation, its relevance to the financial statement audit is clear. As explained in the previous sections, an effective internal control environment requires less audit effort and is therefore more efficient.

However, given the fact that it's almost an elusive goal to entirely prevent SoD conflicts, additional measures are needed in the internal control environment, but also in the audit strategy. Adolphson and Greis describe a five phase road map in their 2009 paper on a risk-based approach to SoD. They propose remediation as a last phase in which they aim to (permanently) correct the identified SoD conflicts. Although they admit there is no universal solution, they do indicate that such a phase is possible and even necessary. Again the remediation measures within the internal control environment should at least be understood by the auditor in order to be able to evaluate the effectiveness of internal controls.

In order to align organizational processes with regulations, policies for centralizing regulatory enforcement for compliance purposes are seen by organizations as (cost) effective (Ernst & Young, 2014). Regulatory compliance, and internal control for that matter, can be improved by making them an integral part of all employee's daily (organizational) activities (Engdahl, 2013).

2.4.3 What is the link between SoD and IT (Information Technology)?

One way of centralizing regulatory compliance and improving internal control is to integrate these SoDs in the applications and systems through (IT) controls the employee's use as integral part of their daily (organizational) activities. Over the past decades the use of IT within organizations have increased dramatically (Computerworld New Zealand, 2015) and this trend will (most likely) continue over the next years (Allied Market Research, 2015). In this instance having appropriate SoDs designed, formally described in documentation, and in place through authorizations within and among applications, together with appropriate general IT controls as a precondition, can help mitigate risks, help improve internal control and aid in regulatory compliance (Ernst & Young, 2010; Office of the New York State Comptroller, 2010; Institute of Finance & Management, 2012).

"An IT control is a procedure or policy that provides a reasonable assurance that the information technology (IT) used by an organization operates as intended, that data is reliable and that the organization is in compliance with applicable laws and regulations. IT Controls can be categorized as either general controls (ITGC) or application controls (ITAC)" (TechTarget, 2015).

In order to integrate the required SoDs in IT these need to be embedded in, and among, the relevant application(s) through access controls, such as role-based access control (RBAC) (Basin et al., 2009). This embedding should be reflected in both formally described policies (design) and the correct implementations in systems (operation). Effective IT general controls (preventative) as well as monitoring (detective) measures need be designed and in place, in order to further help assure data and information confidentiality, integrity and availability. Although research that has been conducted indicates that SoD enforcement in complex workflow environments is not supported through RBAC (Botha & Eloff, 2001).

"Authority for the decisions which permit users to access resources needs to be considered explicitly and reflected in the policy model. Access control policies define the rules which regulate how people (and programs acting on their behalf) can access resources in a computer system" (Moffet & Sloman, 1988, pp.59).

The guideline for designing access control systems for IT and (relevant) information systems should "mirror the organization's internal control system, based on the delegation of authority" Moffet & Sloman, 1988, pp. 59). Furthermore, user identification and authentication are critical issues for maintaining adequate access control, ensuring that the user is in fact who he or she claims to be.

Preferably, SoD is enforced at the time of the transaction (preventative). Runtime enforcement of segregation of duties, meaning SoD conflicts should be prevented, by appropriated: user identifications, authentications and relevant access controls, at time a specific transaction occurs (Brucker, 2013).

In summary this section explained that:

1 SoD is an important part of the internal control environment aimed at preventing that no single individual has the authority to execute two or more conflicting actions within a process.
2 SoDs are important to an organization's internal control environment and the financial statement audit for its effectiveness measure to prevent fraud, material misstatements and financial statement manipulation.
3 SoD, in these times, is closely related to the IT infrastructure within an organization and therefore requires appropriate designed and operating IT controls.

2.5 What is the role of IT and ERP within organizations?

In his book Post Capitalist Society, management consultant Peter Drucker (1993) states that over the last decades a paradigm shift has taken place whereby the world's most important organizations produce and distribute knowledge and information rather than things.

An information system (IS) is a "computerized or manual system to capture data and transform them into information and/or knowledge" (Chaffey & Wood, 2005, pp.21). Such an IS contains information, which is organized data, that is meaningful and contextually relevant and can be used for decision making. Both information systems and information can be supported by IT (information technology), which includes software applications, computer hardware and networks (Chaffey & Wood, 2005).

An organization's process for creating value can be described through its value chain a process whereby inputs are transformed, using resources, through systems and subsystems to valuable outputs. Resulting products and services can be sold to customers (Porter, 1985). These processes can, and ever increasingly are, supported by IT. IT can even help in redesigning organizational processes to gain even better performance (effectiveness and efficiency) (Hammer, 1990).

Significant advances in IT and communications have reduced cost and improved reliability of investments in IT. The commoditization of IT is allowing smaller companies and start-ups to compete with the largest of the established organizations (Carr, 2003).

> *"IT reinforces the existing structure, as well as allowing new structures to evolve. Although IT can replace much of the routine work in organisations, it need not change the basic reporting relationships of the organisation" (Robbins & Barnwell, 2006, pp. 243).*

Knowledge, information and data are valuable resources for decision making and play important roles in (modern) organizations. Knowledge, a combination of data and information to which an expert adds opinion, skills and experience results into a valuable asset for decision making. Data is described as "discrete, objective facts about events. Data are transformed into information by adding value through context, categorization, calculations, corrections and condensation" (Chaffey & Wood, 2005, pp. 21).

Information can be managed as well as a strategic resource for increase organizational performance and improve organizational decision making. However, the effectiveness of this so-called business information management is dependent on the organization's information quality. (Chaffey & Wood, 2005). Data quality encompasses completeness, accuracy, format and currency / timeliness (Setia et al., 2013).

> *"For information to be effective in supporting organizational processes, its quality, or 'fitness for purpose' is critical. In the context of information quality, 'fitness for purpose' means how well it supports the tasks performed by individuals and the decisions they take. If information quality is poor then tasks will be performed inefficiently, erroneous decisions will be made, or, perhaps worse, information will not be trusted and no decisions will be made" (Chaffey & Wood, 2005, pp. 23).*

However, IT can also be a source of new risks, or it can be (part of) the solution for risk management, by, for example implementing applications for mitigating existing risks. IT as such can also be a source of risks, however, the way how organizations use IT and have created organizational processes that support and make use of IT can lead to new risks. The reliability of automated data processing is important, however, many organizations are having issues with effectively operating IT processes. The use of IT is supporting, and creating, more and more complex IT environments. Globally integrated networks with diverse organizational structures. Furthermore, the volume of (electronic) transactions that is created, as well as recorded with greater granularity, is also increasing.

2.6 Defining hypotheses

In this literature section, attention was paid to the relevance of the financial audit, the different audit strategies, the expected role of data analytics in the financial audit, the concept of SoD, the role of IT in organizations. Based on the literature study, hypotheses are defined in order to test if a new audit approach could improve the audit on SoD within organizations. The hypotheses that will be tested in the case study are defined as follows:

H1 - Auditing SoDs by means of data analytics is possible within a DAX2012 environment
H2 - Auditing SoDs by means of data analytics increases the quality of an audit
H3 - Auditing SoDs by means of data analytics increases the efficiency of an audit

3 Case Study Highlights

For the purpose of this study a case study was conducted in order to test the defined hypotheses. The case study is divided into discrete, but interrelated steps, starting out with scoping and finally presenting the results. In this section we present the highlights related to the process and outcome of the conducted case study.

In the preliminary phase the audit manager acknowledged that the purchase-to-pay process is the most suitable process at this client. Based on the audit files of previous years and the risk assessment of the purchase-to-pay process at the case organization several SoD rules were defined, such as:

1 Purchase invoices above €25.000,- that need manual approval should be approved by the CEO and need approval from at least three different approvers.
2 Purchase invoices above €10.000,- that need manual approval should be approved by the Manager Finance and need approval from at least two different approvers.
3 Purchase requisitions above €10.000,- should be approved by the Manager Finance and need approval from at least two different approvers.

The case study client was enthusiastic and eager to participate, because it would allow them to better leverage their existing IT environment and the data that was recorded. It would also provide them with additional insight in, what they consider, valuable data. Namely an opportunity to optimize their purchasing process to gain better control over the process, as well as make it more efficient where possible.

Based on this initial analysis relevant questions can be answered such as:

- What number of expected authorizations based on the amount (excluding VAT) of the purchasing document?
- Is the purchasing document a normal debit or credit note?
- How many unique users were involved with the authorization process?
- Was the procuration limit of the highest authorized involved individual sufficient for this purchasing document?

The interpretation of the results was much less clear cut than expected. It was difficult to capture a complex process, such as the purchasing process, with many (small) operational exceptions, into a relatively limited number of business rules. The analytics process is inherently iterative, based on conducted validations and analyses, additional insight was gained from the financial auditors and the pilot client. This new information was taken into consideration and translated into business rules that could be applied to the analysis.

In this paper not all details are included, although they might be relevant to the financial audit. However, the main arguments and considerations were included to provide enough (background) information for a structured conclusion with respect to our research question regarding audit quality and efficiency. In our analytics approach we distinguish two steps in the purchase processes, namely the purchase requisition and the purchase invoice. As stated above, SoD rules were identified for both steps, depending on the value of the respective document.

3.1 Purchase invoice related highlights

During the transformation and analysis phase, an exception indicator was added with respect to the sufficiency of the highest authorizer's procuration limit, in regards to the purchase invoice amount. By selecting either or both types (OK or NOK) the user gets an immediate overview of the number of purchase invoices per type (<€100; >=€100; >=€10.000; >=€25.000), as well as the number of distinct approvers and the total number of purchase invoices. In this section the highlights are presented around the above-mentioned SoD rules in the purchase invoice approval process.

Purchase invoices above €25.000,- that need manual approval should be approved by the CEO and need approval from at least three different approvers.
When the user makes the appropriate selection of the purchase invoice status (9. Settled) and those documents that need manual approval, the user can select a purchase invoice document type, based on the amount (excluding VAT) of that invoice.

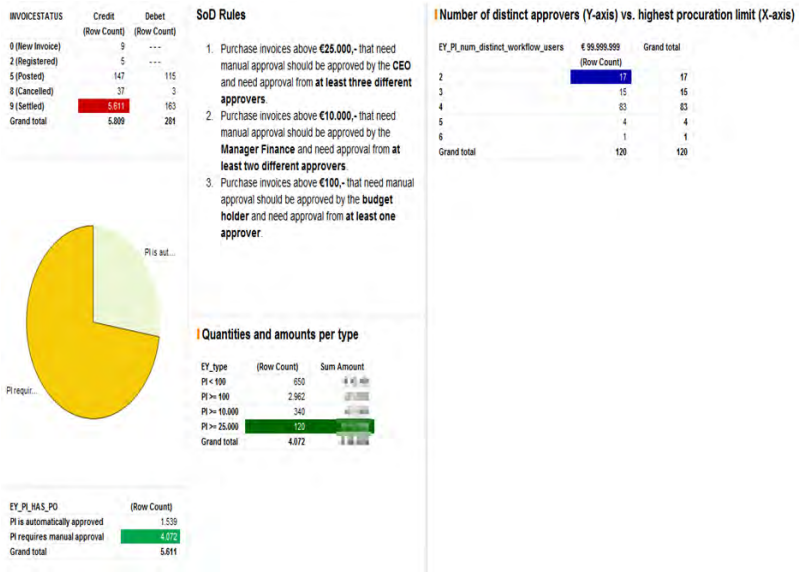


Figure 3 - SoD dashboard for purchase invoices above the €25.000.

Based on the selection, 17 exceptions were identified whereby the approval limit of the highest approver was sufficient for the amount on the purchase invoice document, however, based on the data it was determined that insufficient distinct approvers authorized the purchase invoice document.

- Out of this selection, 15 purchase invoices were authorized twice by the Manager Finance, once as the budget holder of his own purchasing group, and the second time as the Manager Finance due to the purchase invoice amount being greater than €10.000,-.
- One of the purchase invoice document was authorized twice by the CEO, once as budget holder and once as CEO;
- The last exception was caused by the temporary replacement for the Manager Finance during his holiday. In this case this replacement both authorized as the budget holder and the delegated Manager Finance. Please refer to the section below for a more detailed analysis of this phenomenon.

In conclusion, in all these cases at least two distinct people were involved with the purchase invoice approval process, whereby a basic form of SoD was still maintained. However, measured against the client's own standards the SoD for these purchase invoices was insufficient.

Purchase invoices above €10.000,- that need manual approval should be approved by the Manager Finance and need approval from at least two different approvers.
After the user makes the appropriate selections and filters, 18 exceptions were identified with respect to this SoD rule.

Regarding these SoDs we have followed up and investigated these identified exceptions:

- In one exception there was only one distinct approver, namely the Manager Finance, for a purchasing group for which the Manager Finance was also a budget holder;
- The remaining 17 exceptions took place during the summer holiday of 2015 involving the same Manager Finance. During that time his purchase invoice approvals were delegated to his (temporary) replacement, who normally has a lower procurement limit of €10.000. However, for these purchase invoice documents at least two different employees provided approval.

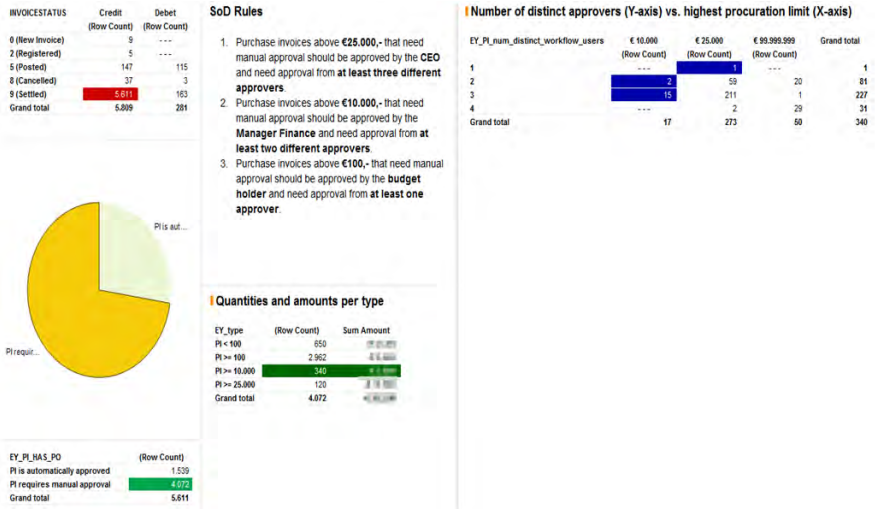


Figure 4 - SoD dashboard for purchase invoices above the €10.000.

Based on a closer examination of the workflow logging table we determined that for weeks 30, 31 and 32 the approval by the delegate fills up the absence left by the Manager Finance. Furthermore, the replacement's quantity of approvals is significantly higher than his average during the year. Please note that the workflow data gets more unreliable near the end of the year, since this period coincides with when we extracted the data used for these analyses.

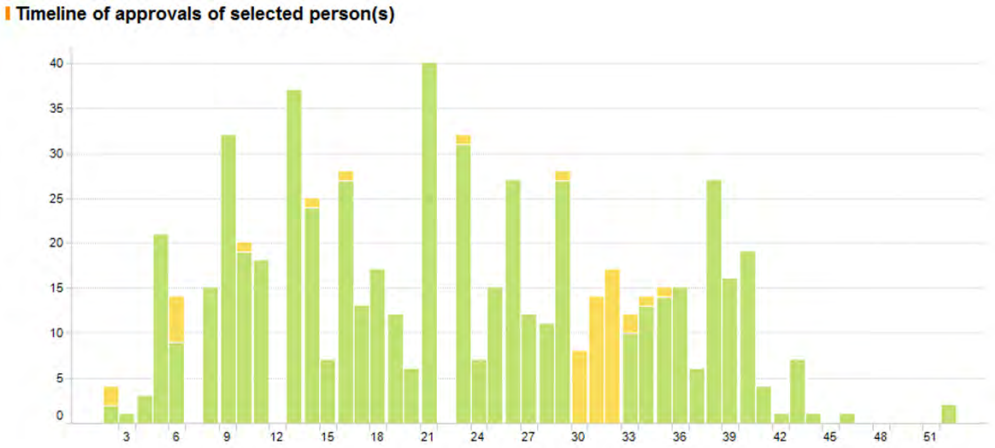


Figure 5 - Timeline of approvals for Manager Finance (green) and his replacement during the summer (yellow).

As can be seen in Figure 5 above, the Manager Finance (in green) has certain weeks during which he doesn't approve purchase invoices. For those three weeks during the summer holiday, the approvals for his replacement (in yellow) are in line with the average purchase invoices during that time.

In conclusion, for all but one case at least two people were involved with the purchase invoice approval process, whereby a basic form of SoD was still maintained. This is a clear deviation against the expected process, since now only one approval was sufficient for this invoice to be settled. However, due to the snapshot approach towards master data, at this moment false positives (17 exceptions) were identified

due to our analysis being unable to properly account for delegation. By highlighting and investigating this issue, additional insight was gained into the process of the client.

3.2 Purchase requisition process

During the transformation and analysis phase, an exception indicator was added with respect to the sufficiency of the highest authorizer's procuration limit, in regards to the purchase requisition amount. By selecting either or both types (OK or NOK) the user gets an immediate overview of the number of purchase invoices per type (<€500; >=€100; >=€10.000; >=€25.000), as well as the number of distinct approvers and the total number of purchase invoices. In this section the highlights are presented around the above-mentioned SoD rules in the purchase requisition approval process.

Purchase requisitions above €10.000,- should be approved by the Manager Finance and need approval from at least two different approvers.
After the user makes the appropriate selections and filters, ten exceptions were identified with respect to this SoD rule.

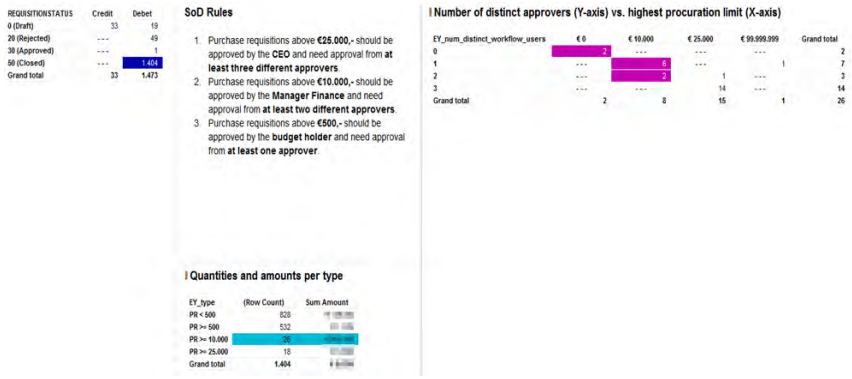


Figure 6 - SoD dashboard for purchase requisitions above the €10.000.

Regarding these SoDs we have followed up and investigated these identified exceptions:

- Two purchase requisitions turn out not to be exceptions because they pertain to fast moving stock goods bought from preferred suppliers. Based on follow-up we learned that, due to the nature of the ordered goods, no approval is required;
- Eight exceptions were identified with insufficient approval, all eight were approved by a budget holder, however, in only two cases a second person approved the purchase requisition. For all eight purchase requisitions, which are above €10.000,-, the approval of the Manager Finance is absent.

In conclusion, two of the ten purchase requisitions pertained to products for which no approval is required. These false positives can be ignored during further analysis and follow-up. However, for eight other purchase requisitions insufficient approval was provided for them to be closed.

4 Conclusion

Based on the findings and the effort that was needed for realizing the analysis a round of interviews with the audit team was organized. This time the goal of the interviews was to evaluate the data analytics approach and its impact on the audit quality and efficiency. The conclusions will be presented per hypothesis as formulated in section 2.6. After describing the conclusions per hypothesis, a brief conclusion will be provided regarding the main research question.

4.1 Auditing SoDs by means of data analytics is possible within a DAX2012 environment

The first hypothesis only states that it is possible to audit SoD by means of data analytics within a DAX2012 environment. In the case study, as described in section 3, it becomes clear that it is indeed possible to audit SoD by means of data analytics within a DAX2012 environment. However, in conducting the case study, there were also some difficulties which will also be evaluated in the hypotheses related to audit quality and audit efficiency.

4.2 Auditing SoDs by means of data analytics increases the quality of an audit

In the evaluation session with the audit team the first point of evaluation is the impact on the audit quality. In order to do so, a comparison was made related to the understanding of the process and the findings of the testing activities. In the testing activities of the financial audit team, no deviations were found and the understanding of the process was documented in a memo. In order to discuss the impact on quality, two main questions were asked.

The first question to the audit manager was if he, after the data analysis, wanted to add or change something in the understanding of the process memo. The audit manager responded that the process was correctly described (high level), but that some relevant details were missing that might be relevant to the understanding of the process. An example of a missing detail is that there was no information added about which employees, in design, had which procuration limit in the purchase-to-pay process. This insight resulted from several questions that were asked during the data analysis phase. It was required to go back to the client to ask questions, rather than gathering the data from the existing audit file.

The second question, which was asked to the entire team, was if they had gained new insights from the data analysis that were relevant to the audit. The main response was that because the analyses were much more thorough, there were also more exceptions noted that had to be evaluated. This enabled them to better understand how the client responded to incidents and deviations. Examples are the holiday of the Manager Finance and related the delegation of his responsibilities, the dual role of the Manager Finance for a number of invoices for which he was both budget holder and the approver for the amount above €10.000,- and the eight purchase requisitions that were not adequately authorized by the Manager Finance. But the most valuable insight that was mentioned by the team members was the impact of the choice to not approve certain fast moving stock goods at preferred suppliers. This choice was evaluated in the audit files, based on the traditional procedures. But the audit team was not able to make a grounded evaluation of the potential risk that arises from this choice. By means of the data analytics they were able to see the potential financial impact and they advised the client to reconsider this part of the process.

Given the abovementioned evaluations we asked the audit manager if he agreed that the data analysis had a positive impact on the audit quality. He responded that the impact was positive and significant.

4.3 Auditing SoDs by means of data analytics increases the efficiency of an audit

The impact on the audit efficiency was evaluated by comparing the required audit effort in order to properly carry out the traditional audit approach and the data analytics approach in a case study. The comparison was made between the hours required for the traditional audit approach, the data analytics approach in an initial year and data analytics approach in a subsequent year. The outcomes were as follows:

Hours required for the traditional approach	20 hours
Hours required for the initial year data analytics approach	130 hours
Hours required for the subsequent year data analytics approach	38 hours

At first glance one would conclude that the data analytics approach is less efficient. However, in the evaluations with the audit team two important remarks were made. The first remark was that the comparison was not entirely fair, since the scope of the traditional approach was broader than the scope of the data analytics approach. The second remark was more formulated as a question. To what extend is an IT audit on the ITGCs still needed, when the controls are tested via data analytics? When the scope of the data analytics approach would be broad enough to cover all relevant automated processes it might result in a saving of 10% to 15% of the audit fee which is used for the IT audit. At the audit of the case study the IT audit budget was 160 hours per year. Therefore, the conclusion of the audit manager regarding the audit efficiency was that as long as data analytics is not integrated to such extend that it could replace IT audit procedures, the data analytics approach would not result in a more efficient audit.

4.4 How can the quality and efficiency of auditing segregation of duties related to the financial statement audit at an organization that makes use of DAX 2012 be increased?

Based on the conducted research, which included both an extensive literature review and a case study, with respect to the hypotheses we have concluded that:

H1: It is possible to audit SoD by means of data analytics within a DAX2012 environment.

H2: Auditing SoDs by means of data analytics increases the quality of an audit.

H3: Auditing SoDs by means of data analytics does not directly lead to more efficiency in an audit.

What do these conclusions mean for our main research question? Both dimensions of quality and efficiency have to be addressed in relationship to the auditing of segregation of duties within an DAX 2012 environment. With respect to dimension of quality, the conclusion of the research reported in this paper is clear that the quality can be improved (significantly) by using data analytics in the financial audit procedures. Certain specific examples are given that clearly indicate the added value of data analytics and improved quality of the financial audit procedures. However, as described in the introduction of this paper, auditors are expected to balance the need to work more efficient, whilst maintaining, and even improving the quality of their work.

Given the conclusion that implementing data analytics in the financial audit procedures does not directly lead to more efficiency, a challenge with respect to balancing these dimensions will remain relevant. However, this research has also suggests that by more drastically reconsidering the role of data analytics in the overall audit approach (broader than SoD), which might lead to eliminating certain traditional (IT) audit activities, efficiency gains can be achieved that (partly) offset the effort required to develop, build and implement (specific) data analytics. This offset reduces the (initial) investment, and therefore benefits efficiency, consequently positively influencing the balance between quality and efficiency, as experienced by many auditors in today's marketplace.

5 References

Accountant. (2016). AFM-boetes big four voor niet naleven zorgplicht. Retrieved March 29, 2016, from https://www.accountant.nl/nieuws/2016/3/hoge-afm-boetes-big-four-voor-niet-naleven-zorgplicht

Adolphson, M., & Greis, J. (2009). Feature A Risk-based Approach to SoD. ISACA Journal, 5, 1–3.

Allied Market Research. (2015). World ERP SOFTWARE Market - Opportunities and Forecasts, 2013 - 2020. Retrieved March 26, 2016, from https://www.alliedmarketresearch.com/erp-market

American Institute of Certified Public Accountants. Accounting and Review Services Committee. (1983). AICPA Professional Standards: Accounting and Review Standards as of June 1, 1983. American Institute of Certified Public Accountants. Retrieved from http://clio.lib.olemiss.edu/cdm/ref/collection/aicpa/id/6954

Basin, D., Burri, S. J., & Karjoth, G. (2009). Dynamic Enforcement of Abstract Separation of Duty Constraints. Computer Security - Esorics 2009, Proceedings, 5789, 250–267. http://doi.org/10.1145/2382448.2382451

Botha, R. A., & Eloff, J. H. P. (2001). Separation of duties for access control enforcement in workflow environments. IBM Systems Journal, 40(3), 666–682.

Brucker, A. D. (2013). Integrating Security Aspects into Business Process Models. Information Technology, 6, 239–246. http://doi.org/10.1524/itit.2013.2004.Abstract

Carcello, J. V, Hermanson, R. H., & McGrath, N. T. (1992). Audit Quality Attributes: The Perceptions of Audit Partners, Preparers, and Financial Statement Users. Auditing: A Journal of Practice & Theory, 11(1), 1–15. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=9703122164&lang=pt-br&site=eds-live

Carr, N. G. (2003). IT Doesn' t Matter. Harvard Business Review, (May 2003), 1–9. http://doi.org/10.1109/EMR.2004.25006

Chaffey, D., & Wood, S. (2005). Business information management: improving performance using information systems. Harlow, England: Prentice Hall/Financial Times.

Computerworld New Zealand. (2001). Making the ERP connection. Retrieved March 26, 2016, from http://www.computerworld.co.nz/article/512814/making_erp_connection/

DeAngelo, L. E. (1981). Auditor size and audit quality. Journal of Accounting and Economics, 3(3), 183–199.

De Vries, J. (1985). Geschiedenis der accountancy in Nederland: aanvang en ontplooiing, 1895-1935. Assen: Van Gorcum. Retrieved from http://imagebase.ubvu.vu.nl/cdm/ref/collection/nib/id/121967

Drucker, P. F. (1993). Post-Capitalist Society. New York. HarperBusiness. Retrieved from http://books.google.com/books?id=dr2QAAAAIAAJ&pgis=1

Engdahl, O. (2013). Ensuring regulatory compliance in banking and finance through effective controls: The principle of duality in the segregation of duties. Regulation and Governance, (April 2013), 332–349. http://doi.org/10.1111/rego.12027

Ernst & Young. (2010). A risk-based approach to segregation of duties. Insights on Governance, Risk and Compliance, (May).

Ernst & Young. (2014). Centralized Operations: The future of operating models for Risk, Control and Compliance functions, (February), 20.

EY. (2015). How big data and analytics are transforming the audit. Retrieved September 15, 2015, from http://www.ey.com/GL/en/Services/Assurance/ey-reporting-issue-9-how-big-data-and-analytics-are-transforming-the-audit

Fischer, M. J. (1996). "Real-izing" the benefits of new technologies as a source of audit evidence: An interpretive field study. Accounting, Organizations and Society, 21, 219–242. http://doi.org/10.1016/0361-3682(95)00005-4

Forbes. (2013). 2013 ERP Market Share Update: SAP Solidifies Market Leadership. Retrieved February 15, 2015, from http://www.forbes.com/sites/louiscolumbus/2013/05/12/2013-erp-market-share-update-sap-solidifies-market-leadership

Gartner. (2014). Gartner Magic Quadrant for Single-Instance ERP for Product-Centric Midmarket Companies. Retrieved October 1, 2015, from https://www.gartner.com/doc/reprints?id=1-25C3331&ct=141201&st=sb

Hammer, M. (1990). Reengineering work: don't automate, obliterate. Harvard Business Review, 68(4), 104–112. http://doi.org/10.1225/90406

Hogan, C. E., & Wilkins, M. S. (2008). Evidence on the audit risk model: Do auditors increase audit fees in the presence of internal control deficiencies? Contemporary Accounting Research, 25(1), 219–+. http://doi.org/10.1506/car.25.1.9

Institute of Finance & Management. (2012). Segregation of Duties is Key to Payroll Control & Compliance, (August).

ISACA. (2015). SOD Remediation Best Practices for ISACA. Retrieved from http://www.isaca.org/Groups/Professional-English/it-audit-guidelines/GroupDocuments/SOD Remediation Best Practices for ISACA.doc

Koot, A., & Stultjens, M. (2013). Starreveld komt weer uit de kast. Informatiebeveiliging, (2), 15–19.

KPMG. (2015). Managen van risico's. Retrieved September 15, 2015, from http://www.kpmg.com/NL/nl/topics/data-en-analytics/Pages/Managen-van-risicos.aspx

Montesquieu. (1977). The Spirit of Laws. Berkeley: University of California Press.

Office of the New York State Comptroller. (2010). The Practice of Internal Controls.

Porter, M. E. (1985). Competitive Advantage. Strategic Management. http://doi.org/10.1108/eb054287

PWC. (2015). Advanced Risk and Compliance Analytics Solutions. Retrieved September 15, 2015, from http://www.pwc.com/us/en/risk-assurance/systems-risk-compliance-and-analytics.html

Raphael, J. (2015). How Artificial Intelligence Can Boost Audit Quality. Retrieved March 29, 2016, from http://ww2.cfo.com/auditing/2015/06/artificial-intelligence-can-boost-audit-quality/

Robbins, S., & Barnwell, N. (2006). Organisation theory: concepts and cases. Frenchs Forest, NSW: Pearson Education Australia.

Setia, P., Venkatesh, V., & Joglekar, S. (2013). Leveraging Digital Technologies: How Information Quality Leads to Localized Capabilities and Customer Service Performance. MIS Quarterly, 37(2), 565–590.

TechTarget. (2015). IT controls. Retrieved October 1, 2015, from http://searchcompliance.techtarget.com/definition/IT-controls

Yale. (2015). Segregation of Duties. Retrieved September 4, 2015, from http://www.yale.edu/auditing/balancing/segregation_duties.html

De IT audit
in een datagedreven accountsantscontrole

Michel Bernsen

Michel Bernsen graduated for the Master Business Administration: Business & ICT at the University of Groningen. He joined Ernst & Young, Risk advisory in Amsterdam and was involved with various audits including financial statement and data analytics.

After five years in the Amsterdam office, he moved the the Sydney office in Australia where he's currently leading the design for a Risk Analytics centre of excellence focusing on delivering Risk Analytics as a service to Advisory clients.

1 Inleiding

De jaarrekening geeft een overzicht van de financiële situatie van een organisatie van een bepaald financieel jaar. De jaarrekening wordt gecontroleerd door de accountant en die geeft – afhankelijk van de opdrachtformulering – een verklaring over de getrouwheid van de gepresenteerde cijfers in de jaarrekening.

De afgelopen jaren is het accountantsberoep onderwerp van discussie, waardoor de uitvoering en verantwoording van de accountantscontrole, waaronder de jaarrekeningcontrole, onderhevig is aan wijzigingen. Dit heeft te maken met:

- Een verhoogde behoefte aan kwaliteit door belanghebbenden;
- Een behoefte aan het verhogen van de informatieve waarde.

Door concurrentie worden budgetten voor een accountantscontrole steeds kleiner (Autoriteit Financiële Markten, 2013). Door kleinere budgetten kiezen accountantskantoren vaak voor een verlaagde bijdrage (in uren) van ervaren personeel of besteden minder tijd aan bepaalde onderwerpen. Dit betekent niet direct dat de kwaliteit van het accountantsberoep hierdoor is verslechterd.

Hogere verwachtingen ten aanzien van de kwaliteit van de jaarrekeningcontrole hebben geleid tot een toenemend aantal kwaliteitsonderzoeken. Uit onderzoek van de Autoriteit Financiële Markten (AFM) blijkt dat significante afwijkingen zijn geconstateerd ten aanzien van de kwaliteit van de jaarrekeningcontroles die door een negental OOB-vergunninghouders wordt uitgevoerd (AFM, 2013). In het rapport spreekt de AFM haar zorgen uit over de kwaliteit van de uitgevoerde accountantscontroles. Vanuit de Nederlandse Beroepsorganisatie van Accountants (NBA) is in 2014 de werkgroep 'toekomst accountantsberoep' gevormd. Zij hebben onderzoek gedaan naar een aantal uitgevoerde accountantscontroles. Zij hebben een rapport gepubliceerd met de titel 'In het publiek belang'. Hierin zijn diverse tekortkomingen geconstateerd. De werkgroep benadrukt dat de kwaliteit van de jaarrekeningcontrole omhoog moet.

De International Auditing and Assurance Standards Board (IAASB) heeft in juli 2013 voorstellen gepresenteerd voor het verhogen van de informatieve waarde van de controleverklaring. Het voorstel is onder meer het vermelden van de belangrijkste bevindingen van de accountant. Dit is eveneens een belangrijke aanbeveling van de werkgroep 'toekomst accountantsberoep'. Tijdens de aandeelhoudersvergadering worden steeds meer vragen gesteld over de jaarrekening en de controlewerkzaamheden (NBA, 2015). Een adequaat inzicht in de organisatie, processen en financiële verslaglegging lijkt derhalve nog belangrijker.

De werkgroep 'toekomst accountantsberoep' beveelt onder andere data analyse aan teneinde de kwaliteit van de accountantscontrole te vergroten. De laatste jaren wordt in toenemende mate data analyse als middel ingezet om zekerheid te krijgen over de financiële situatie van een organisatie. Data analyse biedt de mogelijkheid een post van de jaarrekening integraal (lees: 100%) te beoordelen én bevordert een efficiënte controle. Dit geeft meer inzicht dan de traditioneel uitgevoerde cijferanalyses en deelwaarnemingen.

1.1 Probleemstelling

Hoewel data analyse steeds vaker wordt ingezet tijdens de accountantscontrole, is het methodologisch effect op de controle nog een grijs gebied. Bij de inzet van data analyse is een aantal aandachtsgebieden te onderkennen:

De juistheid en volledigheid van data.

De juistheid en volledigheid van data is vaak onvoldoende beoordeeld. Hiervoor zijn ook onvoldoende richtlijnen vanuit de NBA. Deze schrijft wel voor om de data aan te sluiten met andere bronnen. Echter is dit in sommige gevallen niet mogelijk of niet werkbaar. Deze richtlijn sec is derhalve onvoldoende.

Het afgeven van een in control statement.
Data analyse is een substantieve controlemethode om te controleren wat er over de controleperiode fout gegaan is. Er wordt dan ook niet vastgesteld of controlemaatregelen hebben gewerkt. Er wordt vastgesteld of risico's zich hebben voorgedaan. Er kan derhalve geen oordeel worden gevormd over (bepaalde) interne beheersmaatregelen. Het is niet duidelijk in hoeverre uitspraak gedaan kan worden over het 'in control' zijn.
Een verhoogde mate van steunen op de IT omgeving.
Een aanpak met data analyse vergroot de mate waarin de accountant steunt op de integriteit van de IT omgeving van de klant. Een oordeel over de integriteit van data lijkt derhalve een even groot oordeel als het oordeel over de financiële verslaglegging. Een jaarrekening wordt echter alleen ondertekend door een registeraccountant.

1.2 Onderzoeksvraag

De hoofdvraag van het onderzoek is:

Wat is het effect van een datagerichte controleaanpak op de werkzaamheden van de IT auditor?

Om deze vraag zo goed mogelijk te beantwoorden worden de volgende vragen onderzocht:

1 Welke set aan IT beheersmaatregelen dient geëvalueerd te worden om een oordeel te kunnen vormen over de juistheid en volledigheid van data?
   - A Is er verschil in typen data waardoor gepaste IT beheersmaatregelen van toepassing zijn of is er sprake van een uniform toepasbaar normenkader.
   - B Wat is het effect op de jaarrekeningcontrole als de IT auditor onvoldoende zekerheid kan afgeven over de juistheid en volledigheid van de data?

2 Welke methodologische verschillen brengt de toepassing van data analyse tijdens de jaarrekeningcontrole met zich mee?
   - A Kan de accountant een in control statement ondertekenen of een mening vormen over de continuïteit van de organisatie wanneer een datagerichte aanpak wordt toegepast?
   - B Moet bij een datagerichte aanpak een jaarrekening worden afgetekend door een registeraccountant (RA) alsmede een register EDP-auditor (RE)?

1.3 Doelstelling

De doelstelling van het onderzoek is te onderzoeken welke werkzaamheden anders of extra moeten worden uitgevoerd als data analyse wordt ingezet tijdens de accountantscontrole. Hierbij heeft dit onderzoek als doelstelling duidelijke richtlijnen en randvoorwaarden te presenteren. Ultimo dient het onderzoek bij te dragen aan de ontwikkeling van het beroep en kwaliteitsborging van de accountantscontrole.

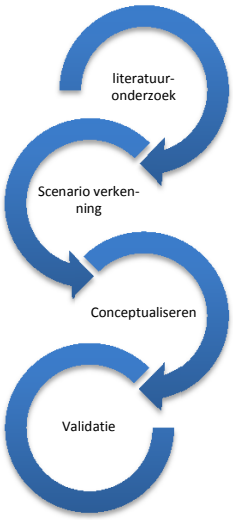
1.4 Afbakening van het onderzoek

Het onderzoek richt zich op de veranderingen voor de IT auditor die een datagerichte aanpak met zich meebrengt. Het onderzoek is niet ingestoken om een oordeel te vormen over het huidige kennisniveau van de IT auditor, dan wel om de huidige manier van werken te beoordelen. Verder richt het onderzoek zich niet inhoudelijk op data analyse, maar op de randvoorwaarden en methodologie voor zover relevant voor de IT auditor.

1.5 Onderzoeksmethode

Het onderzoek is van kwalitatieve aard en is op te delen in twee deelonderzoeken conform de onderzoeksvragen 1 en 2. Het eerste onderzoeksobject heeft een ontwerpende onderzoeksfunctie. De onderzoeksmethode voor het eerste deelonderzoek is op de volgende pagina nader beschreven.

- Literatuuronderzoek
- Uitgewerkte casuïstiek
- Tien in praktijk toegepaste data analyses in kaart gebracht
- Documentanalyse
- Analyse op aanpak, vaststellen van betrouwbaarheid data
- Eigen analyse gericht op de uitgevoerde werkzaamheden
- Typeren/definiëren van data
- Opstellen aanpak voor data analyse
- Opstellen conceptueel normenkade\
- Interviews met experts
- Validatie/vaststellen van data typen, aanpak en normenkader
- Delen van resultaten



Een literatuuronderzoek is de basis van het onderzoek. Daarbij geldt een specifieke focus op maatregelen om de integriteit van data vast te stellen binnen het kader van de jaarrekening.

Er zijn tien toegepaste vormen van data analyse uitgewerkt. Ieder scenario betreft een in de praktijk toegepaste vorm van data analyse. Per scenario zijn de organisatorische kenmerken, het doel van data analyse en de werkmethode beschreven. Het scenario en bijbehorende documentatie (analyse/resultaten, dataverzoeken, scripts, data, etc.) is vervolgens geanalyseerd. Verder is onderzocht of de uitgevoerde werkzaamheden voldoende zijn geweest om de juistheid en volledigheid van data vast te stellen. De oordeelsvorming van een scenario is ook gereflecteerd op andere scenario's om zo een best-practice af te leiden.

Vervolgens is een aanpak uitgewerkt voor het uitvoeren van data analyse in het kader van de jaarrekeningcontrole. Als onderdeel van de aanpak zijn de verschillende data typen bepaald. Vervolgens is een conceptueel normenkader opgesteld om de juistheid en volledigheid van data vast te kunnen stellen.

De aanpak, data typen en het normenkader (hierna: conceptueel raamwerk) worden gevalideerd op basis van interviews met vijf subject matter experts. Deze experts hebben ervaring met data analyse en hebben een achtergrond in IT audit en/of accountancy. De interviews zijn semi-gestructureerd afgenomen. Het conceptueel raamwerk is aan de geïnterviewden toegelicht, waarna deze het concept hebben bevestigd of bekritiseerd. Om een suggestief vraaggesprek te voorkomen zijn eveneens tegenstrijdige stellingen ingenomen om een constructieve discussie te bewerkstelligen. Tegenstrijdigheden of aanvullingen op het conceptueel raamwerk – die door de geïnterviewden zijn aangedragen – zijn onderzocht binnen de 10 scenario's en tijdens de interviews nogmaals besproken. Indien consensus is bereikt is dit verwerkt in de resultaten. De samengevatte interviews zijn afgestemd. Onderzoeksresultaten zijn aan collega's gepresenteerd en besproken.

Het tweede onderzoeksobject kent een evaluerende onderzoeksfunctie. Gezien de scope en onderzoekintensiteit van het eerste onderzoeksobject, wordt het tweede onderzoeksobject beperkt tot een oriënterend onderzoek. Hiermee wordt bedoeld dat literatuuronderzoek wordt uitgevoerd en interviews worden

afgenomen teneinde een initieel antwoord te kunnen geven op de vragen die voortvloeien uit het eerste onderzoeksobject.

2 Accountantscontrole

In dit hoofdstuk wordt de aanpak van de accountantscontrole samengevat voor zover relevant geacht.

2.1 Gegevensgerichte aanpak

Een gegevensgerichte aanpak is van oudsher de aanpak voor het controleren van een financiële administratie of de jaarrekening. Met een gegevensgerichte controle worden de resultaten en producten van een proces getoetst en niet zozeer de totstandkoming – het procesverloop – zelf. Een gegevensgerichte aanpak bestaat voornamelijk uit het integraal doorlopen van de grootboekmutaties. Het gaat hier om specifieke transacties, dan wel specifieke onderdelen van bepaalde rekeningen die van bijzonder belang zijn in het beeld van de jaarrekening. Hierbij wordt gezocht naar vreemde transacties, zoals negatieve debiteuren, memoriaalboekingen of opvallende omschrijvingen. Daarnaast worden detailcontroles (voortgezette controle, afloopcontrole, beoordeling van afschrijvingen, etc.), steekproeven en cijferbeoordelingen uitgevoerd.

2.2 Systeemgerichte aanpak

In Nederland bestond bij de accountantscontrole een noodzaak voor de systeemgerichte aanpak omdat gegevensgerichte maatregelen uit economische overwegingen niet meer haalbaar zijn (Frielink & De Heer, 1987). Als de accountantscontrole zo veel mogelijk op systeemgerichte werkzaamheden wordt gebaseerd, hoeven zo min mogelijk gegevensgerichte werkzaamheden te worden uitgevoerd.

Een systeemgerichte aanpak heeft als visie de totstandkoming van resultaten en producten te beoordelen (University of Washington, 2013). Met name de jaarrekeningposten die bestaan uit transacties resulterende uit bedrijfsprocessen worden systeemgericht gecontroleerd. Hierbij worden de belangrijkste interne beheersmaatregelen van deze processen in kaart gebracht. Systeemgerichte werkzaamheden kunnen omvatten (Deckers & van Kollenburg, 2002):

- Onderzoek van documenten die ten grondslag liggen aan bepaalde transacties om controle-informatie te verkrijgen waaruit blijkt dat de maatregelen van interne beheersing juist hebben gewerkt.
- Informeren naar en het waarnemen van bepaalde maatregelen van interne controle.
- Het opnieuw uitvoeren van maatregelen van interne controle.

Er wordt onderscheid gemaakt tussen drie typen beheersmaatregelen voor bedrijfsprocessen:

- **Applicatiecontroles**. Applicatiecontroles betreffen specifieke geautomatiseerde beheersmaatregelen op transactieniveau binnen applicaties, zoals invoercontroles, blokkades, rekenregels, functiescheiding, afdwingen van autorisatieregels en andere geprogrammeerde controlemaatregelen.
- **IT-afhankelijke manuele controles**. IT-afhankelijke manuele controles zijn beheersmaatregelen welke door medewerkers, maar met behulp van een applicatie, worden uitgevoerd, zoals monitoring en handmatige controles aan de hand van rapporten (gegenereerd door de applicatie).
- **Manuele controles**: Manuele controles worden volledig handmatig door functionarissen uitgevoerd.

Zoals gezegd helpt een systeemgerichte aanpak inzicht te verkrijgen in een juiste, tijdige en volledige totstandkoming van transacties. Maar een beoordeling van de interne beheersing sec is niet voldoende om jaarrekeningposten te beoordelen. De systeemgerichte controle wordt dus altijd uitgevoerd in combinatie met gegevensgerichte werkzaamheden.

2.2.1 Traditionele IT audit

Starreveld (2002) claimt dat interne beheersmaatregelen ingericht moeten zijn om de betrouwbaarheid van informatieverwerking in informatiesystemen te borgen. Om te kunnen waarborgen dat applicatiecontroles of IT-afhankelijke controles effectief hebben gefunctioneerd gedurende de controleperiode, moet aan een aantal randvoorwaarden worden voldaan. Deze randvoorwaarden betreffen algemene IT-beheersmaatregelen. De betrouwbaarheid van de applicatie is gebaseerd op de volgende kwaliteitsaspecten:

- Exclusiviteit: De mate waarin uitsluitend geautoriseerde personen of apparatuur via geautomatiseerde procedures en beperkte bevoegdheden gebruikmaken van IT-processen.
- Integriteit: De mate waarin het object (gegevens en informatie-, technische- en processystemen) in overeenstemming is met de afgebeelde werkelijkheid.
- Controleerbaarheid: De mate waarin het mogelijk is kennis te verkrijgen over de structurering (documentatie) en werking van een object. Tevens omvat dit kwaliteitsaspect de mate waarin het mogelijk is vast te stellen dat de informatieverwerking in overeenstemming met de eisen ten aanzien van de overige kwaliteitsaspecten is uitgevoerd.
- Continuïteit: De mate waarin een object continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben. Belangrijk aspect van continuïteit is tevens het voorkomen van dataverlies bij storingen en calamiteiten.

De categorieën IT-beheersmaatregelen die de betrouwbaarheid van applicaties of delen daarvan borgen, betreffen (EY, 2014):

- Wijzigingenbeheer: Algemene IT-beheersmaatregelen die waarborgen dat wijzigingen in applicaties op een beheerste wijze beoordeeld, getest en in productie worden genomen. Daarnaast is het uiteraard van belang dat deze stappen binnen het wijzigingsproces in voldoende mate worden nageleefd en met voldoende functiescheiding.
- Logische toegangsbeveiliging: Algemene IT-beheersmaatregelen die waarborgen dat gebruikers de juiste toegang en bevoegdheden in systemen hebben.
- Continuïteitsbeheer: Algemene IT-beheersmaatregelen die de continuïteit van de geautomatiseerde gegevensverwerking binnen de organisatie waarborgen.

De drie categorieën hebben betrekking op de applicatie en de ondersteunende database en besturingssysteem. De categorieën bestaan uit meerdere IT beheersmaatregelen, welke nader zijn beschreven in bijlage A. In de praktijk blijkt dat de IT beheersmaatregelen niet altijd in zijn volledigheid worden beoordeeld op het niveau van de database en het besturingssysteem (c.q. netwerk). Dit heeft te maken met de frequentie dat wijzigingen (o.a. gebruikers, instellingen, beveiliging) worden doorgevoerd of de relevantie in het kader van data integriteit.

Indien de algemene IT beheersmaatregelen als toereikend worden beoordeeld, dient de applicatiecontrole of het IT aspect van een IT-afhankelijke controle één keer te worden getoetst. Als de IT beheersmaatregelen ontoereikend blijken kan ervoor worden gekozen om een applicatiecontrole of IT-afhankelijke controle volgens een statistisch representatieve deelwaarneming (maximaal 25 items) te toetsen.

2.3 Een datagerichte aanpak

Een systeemgerichte controle geeft de accountant niet alleen meer zekerheid over de financiële verslaglegging. Het was ook een noodzakelijke innovatie binnen de accountancy. Het aantal transacties was door de introductie van informatiesystemen namelijk dermate gegroeid dat een gegevensgerichte controle té arbeidsintensief en grotere risico's met zich mee bracht.

Door de toenemende digitalisering en internettoepassingen groeide het percentage bedrijfsdata en transacties aanzienlijk de afgelopen jaren. Accountants vragen zich af of het hierdoor statistisch nog verant-

woord is om 25 transacties te toetsen (om de effectiviteit van IT controles aan te tonen) wanneer er sprake is van tienduizenden transacties die het bedrijfsproces doorlopen. Tezamen met de kritiek op de kwaliteit van de uitvoering van de accountantscontrole, ontstaat de noodzaak om meer inzicht te verkrijgen in de risicobeheersing van organisaties en een integrale blik van de boekingen.

Data analyse biedt de mogelijkheid om middels speciale tools of standaard dataverwerkers een geavanceerd inzicht te krijgen in een organisatie. De toepasbaarheid en populariteit van data analyse neemt toe. Data analyse is in verschillende fasen van de jaarrekeningcontrole toe te passen:

- Planning: Data analyse kan een goed beeld geven van de risico's van bepaalde posten. Eventuele liquiditeitsrisico's, verhoogde inkoopkosten of stagnerende verkoop is eenvoudig in kaart te brengen. Dit kan helpen om te bepalen welke posten meer aandacht behoeven tijdens de interim controle of jaareinde controle.
- Interim controle: Data analyse helpt in kaart te brengen hoe processen werkelijk verlopen en welke wijze transacties worden geboekt. Daarnaast kan op basis van data extracties selecties worden gemaakt van transacties om (manuele) controles te toetsen.
- Jaareinde controle: Gegevensgerichte werkzaamheden kunnen integraal worden uitgevoerd op basis van data analyse. Applicatiecontroles en IT-afhankelijke controles kunnen op gegevensgerichte wijze worden geanalyseerd (lees: data analyse). Daarnaast kunnen specifieke analyses worden uitgevoerd ter vervanging van manuele steekproeven of cijferbeoordelingen.

Omdat data analyse geen gefragmenteerd element in de controle is, maar tijdens het gehele jaarrekeningcontroletraject kan worden toegepast, wordt de datagerichte aanpak geïntroduceerd. Een datagerichte aanpak kan gedefinieerd worden als:
'Een datagerichte aanpak behelst het toepassen van data analyse gedurende de jaarrekeningcontrole teneinde een integraal beeld te krijgen van de risico's, risicomanifestatie en de betrouwbaarheid van transacties van een organisatie.'

3 Scenario analyses

Zoals benoemd is het accountantsberoep onderhevig aan veranderingen waarbij de fundamentele controleaanpak door de jaren heen van gegevensgericht naar systeemgericht naar datagericht is geëvolueerd. De datagerichte aanpak is een nieuwe aanpak. De nieuwe aanpak is echter nog onvoldoende uitgekristalliseerd kijkende naar de methodologische onderbouwing. In de theorie en beroepsvoorschriften zijn beperkte richtlijnen aanwezig voor het vaststellen van de betrouwbaarheid van data.

De basis van dit onderzoek rust op een scenario analyse van een tiental data analyses met de daarbij behorende vaststelling van de betrouwbaarheid van de data. Deze data analyses zijn uitgevoerd tussen 2012 en 2015. De analyse is gericht op de kwaliteitsaspecten juistheid en volledigheid. Voor onderbouwing van de geanalyseerde kwaliteitsaspecten zie paragraaf 4.2.

De tien scenario's zijn:

1 Three way match: een aansluiting van de inkooporders, goederenontvangst en inkoopfacturen.
2 Autorisatie van inkoopfacturen zijn conform het procuratieschema.
3 Het identificeren van onjuiste salarisbetalingen.
4 Het identiferen van onjuiste en ongeautoriseerde declaraties.
5 Functiescheiding bestaat tussen het wijzigen en autoriseren van crediteuren stamgegevens.
6 De omzet uit de benutting van het stroomnetwerk is volledig verantwoord in de financiële administratie.

7 Alle energie inkopen zijn geconfirmeerd via het trading platform. Alle geconfirmeerde sell deals zijn verantwoord in de financiële administratie.
8 Functiescheiding bestaat tussen het wijzigen en autoriseren van huurprijzen.
9 De omzet uit gewerkte uren (timesheet) is juist berekend op basis van het uurtarief. De uren zijn gefactureerd en volledig verantwoord in de financiële administratie.
10 Journal entry testing (standaard activiteit in de accountantscontrole).

Voor elk scenario is de context (situatieschets en risico), de aanpak van de analyse en de werkzaamheden om de betrouwbaarheid van de data vast te stellen beschreven. Ieder scenarioanalyse is afgesloten met een analyse van de onderschrijvingen en tekortkomingen om de data betrouwbaarheid vast te stellen. Omwille van deze samenvatting zijn de situatieanalyses weggelaten met uitzondering van onderstaande – een voorbeeld van scenario 2.

3.1 Scenario 2: Autorisatie van inkoopfacturen

Organisatie B: kenmerken	
Sector	Power & Utilities
Omzet	€ 48.700K
Controlejaar	2012
Scenario: context	
Situatieschets	De post overige bedrijfskosten en waterinkopen is opgebouwd uit transacties die geboekt worden vanuit het inkoopproces. Het inkoopproces bestaat simpel gezegd uit het bestellen van goederen en diensten, ontvangen van goederen en diensten, controleren van de factuur en het betalen en afletteren van de inkoopfactuur. Om de juistheid van de kosten te borgen is er één essentiële applicatiecontrole gedefinieerd: 1 Inkoopfacturen dienen goedgekeurd te worden volgens het procuratieschema. Facturen met een waarde lager dan 500 euro hoeven niet te worden goedgekeurd. Gezien de algemene IT beheersmaatregelen niet effectief zijn getoetst, kan niet worden gesteld dat de applicatiecontrole adequaat heeft gefunctioneerd over 2012.
Risico	Het risico bestaat dat facturen onterecht worden betaald. Voor de jaarrekening bestaat het risico ten aanzien van de juistheid van kosten.
Scenario: data-analyse aanpak	
Applicatie / database	Agresso Business Warehouse / Oracle
Type data	Transacties
Aanpak	Doordat het inkoopproces één essentiële control kent, neemt het belang van de control toe. Data analyse is uitgebreid toegepast. Er wordt gecontroleerd of: - Er functiescheiding is tussen de invoerder en fiatteur van de inkoopfacturen; - Volgens de procuratieschema facturen worden goedgekeurd; - Dubbele facturen zijn geboekt/betaald; - Er wordt een analyse gedaan op bijzondere transacties: - Inkoopfacturen net onder het limiet van de gebruiker;

	- Gebruikers met buitenproportioneel veel transacties met een waarde lager dan 500 euro. - Incidentele betalingen aan crediteuren. - Meerdere betalingen onder het limiet die samen één betaling zijn.
Data extractie	Er is een data download gemaakt van alle inkoopfacturen uit de crediteuren sub administratie over een periode van 1-1-2012 tot en met 31-12-2012. Er is geselecteerd op basis van effectieve boekingsdatum. Dit is het moment dat de factuur in het grootboek is geregistreerd. De data is middels een directe extractie op de database onttrokken en door de klant aangeleverd.
Datavoorbeeld	Zie tabel 3.
Scenario: validatie van gegevens	
Juistheid	De auditor heeft change management en user access management (het toekennen, wijzigen en ontnemen van rechten) ontoereikend beoordeeld. De overige beheersmaatregelen zijn toereikend.
Volledigheid	De query waarmee de data is gedownload is beoordeeld door een IT auditor. De totale waarde van inkoopfacturen kan niet direct worden aangesloten met een grootboekrekening of jaarrekeningpost.
Analyse van werkzaamheden	
De data is mogelijk aangeleverd door een medewerker met hoge rechten. Deze zou gebaat kunnen zijn bij datamanipulatie om bepaalde acties te verbergen. Er is niet vastgesteld dat data niet is gemanipuleerd nadat dit is gedownload. Dit heeft betrekking op zowel de juistheid en volledigheid van data. <u>Juistheid</u> De belangrijkste datavelden betreffen: - Extern factuurnummer: Het externe factuurnummer betreft een invoerwaarde en is dus onderhevig aan fouten. Wel geldt dat een gebruiker een factuur fiatteert als deze heeft gecontroleerd of de factuur ook juist is ingevoerd. Er is derhalve een visuele controle op de ingevoerde waarden. - Gebruikersnaam invoerder: Om functiescheiding inzichtelijk te maken, dient de gebruikersnaam juist te zijn. De gebruikersnaam wordt automatisch met de rest van de transactie gegeven ingegeven in het systeem. De invoer is gebaseerd op de ingelogde gebruiker. Om de authenticiteit van de gebruiker te verifiëren dienen de wachtwoordinstellingen op – tenminste applicatieniveau – adequaat te zijn. - Gebruikersnaam fiatteur: Idem aan de vorige - Bedrag: Het bedrag is een invoerwaarde. Deze is dus mogelijk onjuist. Wel geldt dat een gebruiker een factuur fiatteert als deze heeft gecontroleerd of de factuur ook juist is ingevoerd. - Crediteurnummer: Het crediteurnummer is nodig om dubbele facturen en bijzondere transacties te analyseren. Het crediteurnummer is een invoerwaarde. Deze is dus mogelijk onjuist. Wel geldt dat een gebruiker een factuur fiatteert als deze heeft gecontroleerd of de factuur ook juist is ingevoerd. - Effectieve datum: De boekingsdatum is van belang aangezien dit de basis is voor het bepalen van de factuurpopulatie. De boekingsdatum wordt ingevoerd. De functionaliteit van de applicatie borgt dat een juiste datum wordt geboekt. De auditor kan aansluiting maken met het grootboek. Indien de totale waarde van de geselecteerde populatie aansluit met de totale waarde dat in het grootboek is opgenomen is de volledigheid vastgesteld. Dat is het doel van dit veld in het kader van deze analyse. <u>Volledigheid</u> De volledigheid is enkel op basis van een query beoordeling vastgesteld. Hiermee is wel vastgesteld of de	

query alle benodigde data selecteert. Door aansluiting te leggen met alle inkoopfacturen in het grootboek, had de volledigheid vastgesteld kunnen worden.

Tabel 1: Analyse scenario 2.

Datavoorbeeld scenario 2: Autorisatie van inkoopfacturen

Leverancier-nummer	Factuur nummer	Factuur bedrag	Intern factuur-nummer	Ingevoerd op	Ingevoerd door	Datum getekend	Getekend door	Factuur datum	Vervald atum
987345	1402639	€ 58.267	85486	3-3-2012	ELHO	10-3-2012	SAKO	1-3-2012	31-3-2012

Tabel 2: Datavoorbeeld scenario 2.

Datatypen*	
Gegenereerde gegevens:	intern factuurnummer
Reproduceerbare gegevens:	vervaldatum
Invoergegevens:	leverancier nummer, factuurnummer, factuurbedrag, ingevoerd op, datum getekend, factuurdatum
Identificerende gegevens:	ingevoerd door, getekend door

* Gedefinieerd in hoofdstuk 4.2.

4 Resultaten

De randvoorwaarden voor het toepassen van data analyse verdienen de juiste aandacht. De randvoorwaarden bepalen namelijk in hoeverre een betrouwbare controle is uitgevoerd en daarmee de waarde die aan de analyse kan worden ontleend. Door het uitvoeren van scenario analyses is inzicht verkregen in hoe de data is gevalideerd en of daar nog onzekerheid in schuilt. Op basis van de scenario-analyses is het volgende gedefinieerd:

- Een aanpak voor het bepalen, verkrijgen, valideren en analyseren van data, zie paragraaf 4.1.
- De typering van data die voorkomen in datasets, zie paragraaf 4.2.
- IT beheersmaatregelen die passen bij de gedefinieerde data typen, zie paragraaf 4.3.

Er is een vijftal interviews afgenomen van experts op het gebied van data analyse in de jaarrekeningcontrole. De geïnterviewden hebben verschillende achtergronden, te weten register accountants (RA), register edp auditors (RE) en een combinatie van beide (RE RA). Tijdens de interviews zijn de voorlopige resultaten besproken. De resultaten van de scenario analyses en de interviews zijn beschreven in navolgende paragrafen.

4.1 Aanpak

Op basis van de scenario analyses, de ervaringen in de praktijk en de interviews met experts wordt de volgende aanpak voorgesteld om de analyse van data op een verantwoorde wijze uit te voeren:

1 Verken de situatie van de organisatie: processen en procedures. De organisatie dient voorschriften te hebben voor haar interne beheersing (zogenaamde entity level controls, business rules en beheersmaatregelen). De auditor dient kennis te nemen van beheersmaatregelen die de organisatie kenmerken. Deze dient de auditor te relateren aan de bedrijfsprocessen of de routines (bijvoorbeeld schattingen) waarmee andere jaarrekeningposten tot stand komen.

2 Stel de risico-hypothese. Op basis van de opgedane kennis, kunnen risico's worden bepaald die de accountant wil onderzoeken.
3 Bepaal de uit te voeren analyses en de daarvoor benodigde data. Het gestelde risico bepaalt op welke wijze data geanalyseerd dient te worden en welke data hiervoor nodig is. Dit kan leiden tot een extractie uit slechts één bron, maar ook meerdere bronnen die vervolgens het onderzoeksobject vormen. Het is daarom essentieel om vooraf te bepalen welke analyses nodig zijn.
4 Verken de applicatie en de database. Stel vast welke data typen van belang zijn te onderzoeken. Wanneer duidelijk is welke analyse(s) moet(en) plaatsvinden, is het zaak de haalbaarheid vast te stellen. Een verkenning van de applicatie en/of database is nodig indien de werking hiervan niet bekend is. Hiermee wordt bedoeld het bepalen van de totstandkoming van data en daarmee het identificeren van de data typen (zie paragraaf 4.2).
5 Bepaal hoe de juistheid en volledigheid kan worden vastgesteld van onttrokken data. Als het duidelijk is welke data typen van belang zijn voor de analyse en hoe deze tot stand zijn gekomen, kan worden bepaald welke activiteiten nodig zijn om de juistheid en volledigheid van data vast te stellen. Dit kunnen algemene IT beheersmaatregelen betreffen, maar ook activiteiten als query-beoordeling, aanwezigheid bij de data extractie, aansluiting met externe bronnen, etc.
6 Voer de data extractie uit. Als het duidelijk is welke data nodig is voor het uitvoeren van de analyse, kan de extractie plaatsvinden. De extractie dient plaats te vinden op een bron die onderwerp van de validatie is.
7 Valideer de juistheid en volledigheid van de extractie. Op basis van het vooraf opgestelde validatieplan, kan de data worden gevalideerd.
8 Voer de analyse uit. De analyse is vooraf bedacht en kan na extractie worden uitgevoerd. De analyse zelf kan in sommige gevallen ook bijdragen aan de validatie van gegevens. Dit dient derhalve goed op elkaar te worden aangesloten.
9 Onderzoek de uitkomsten. De analyse kunnen diverse bevindingen aan het licht brengen. Het is zaak om de mogelijk fout te onderzoeken - indien deze materieel is. Wanneer de mogelijke fout geverifieerd wordt met externe bronnen kan blijken dat de bevinding niet of slechts deels fout is.

De aanpak biedt het voordeel dat de accountant redelijke mate van zekerheid krijgt over data en daarom minder risico loopt bij het ondertekenen van de jaarrekeningcontrole. Het opzetten van data analyse kost tijd, maar de eerste vijf stappen van een analyse zijn een eenmalige investering. Deze hoeft niet jaarlijks herhaald te worden.

Een aanpak voor data analyse binnen de jaarrekeningcontrole is eerder geopperd door Wagenaar (2013). Deze aanpak mist de factoren waar dit onderzoek zich op richt: de validatie van gegevens. Als accountant dien je een kritische houding aan te nemen en geef je uiteindelijk een controleverklaring af waarbij je erkent dat de jaarrekening een getrouw beeld van de werkelijkheid geeft. Indien de integriteit van data niet kan worden vastgesteld bevat de analyse een onzekerheid. Derhalve dient data altijd gevalideerd te worden.

4.2 Data typen

Audit standards 2 van NOREA schrijft voor dat integriteit bestaat uit de kwaliteitsaspecten juistheid, volledigheid, actualiteit/tijdigheid en geoorloofdheid. Integriteit wordt gerelateerd aan bedrijfsprocessen en procedures. Dit onderzoek benoemt de juistheid en volledigheid van data. De tijdigheid en geoorloofdheid moet blijken uit de analyse zelf. Het tijdigheid aspect is natuurlijk afhankelijk van een datumveld. Echter in de validatie van data wordt bepaald of de datum juist is. Vervolgens kan in de analyse de tijdigheid van transacties worden bepaald. De analyse van transacties kan ook gericht zijn op het bepalen van de geoorloofdheid. Dit is echter op transactioneel niveau.

Er bestaan drie typen van data-integriteit, te weten: (1) relationele integriteit, (2) attribuut integriteit en (3) entiteit integriteit (Van Praat en Suerink, 2004). Het eerste type betreft de integriteit van relaties tussen data elementen. Een voorbeeld hiervan is het veld dat een inkooporder en een inkoopfactuur aan elkaar relateert. Middels data analyse kan deze vorm van integriteit worden vastgesteld. Het tweede type betreft de integriteit van een gegeven van een attribuut. We spreken hier van een dataveld. Dit is onderdeel van het onderzoek en hieronder beschreven. Het derde type betreft de integriteit van verschillende data elementen. Dit is het best te relateren aan de geoorloofdheid van transacties. Een voorbeeld hiervan is het autoriseren van een factuur met een bepaald bedrag door een bepaald persoon. De geoorloofdheid van de verhouding van de drie datavelden kan middels data analyse inzichtelijk worden gemaakt.

Tijdens de scenarioverkenning viel op dat de volledigheid van gegevens veelal wel wordt beschreven, maar de juistheid van gegevens in mindere mate. Het klassieke normenkader van IT beheersmaatregelen is bij geen enkel scenario volledig toegepast. Dit is onderschreven door de analyse van het scenario waarbij hiaten in de aanpak zijn geconstateerd. De analyse en interviews met experts vanuit de praktijk wijzen uit dat er sprake is van vier typen data:

1 Gegenereerde gegevens. Gegenereerde gegevens is data dat automatisch door de applicatie of daaraan gerelateerde componenten is gegenereerd en niet reproduceerbaar is. Een goed voorbeeld hiervan is een relationeel dataveld (ID), hash totalen, maar ook logging van mutaties.
2 Reproduceerbare gegevens. Reproduceerbare gegevens is data dat automatisch door de applicatie of daaraan gerelateerde componenten is gegenereerd en reproduceerbaar is. Een goed voorbeeld hiervan is een totaalprijsberekening. Twee componenten in de data kunnen het veld opnieuw berekenen.
3 Invoergegevens. Invoergegevens is data dat ingevoerd is door gebruikers van het systeem. Voorbeelden hiervan zijn ingevoerde prijzen, aantallen of persoonsgegevens.
4 Identificerende gegevens. Identificerende gegevens is data dat aangeeft door welke gebruiker de data is ingevoerd of gegenereerd. Simpel gezegd, de gebruikersnaam van de gebruiker die de mutatie heeft doorgevoerd. Het is van belang dat de gebruikersnaam correspondeert met de eigenaar van het account.

Er zijn applicatiecontroles die (1) volledig door het systeem worden uitgevoerd (interface, berekeningen, etc.) of (2) afhankelijk zijn van handelingen dan wel invoer van de eindgebruiker. Dit vertaalt zich ook naar de gedefinieerde data typen. Zowel gegenereerde, reproduceerbare als identificerende gegevens kunnen onder dezelfde twee noemers vallen. Het is namelijk data dat niet direct door de eindgebruiker kan worden beïnvloed en door het systeem wordt geregistreerd of gegenereerd. Met voortschrijdend inzicht zijn deze data typen echter opgesplitst omdat de randvoorwaarden voor de data niet gelijk zijn. De overige gegevens zijn invoergegevens. Concluderend, elk dataveld op een regel data kan worden gecategoriseerd met behulp van bovenstaande vier data typen.

4.3 Algemene IT beheersmaatregelen datagerichte aanpak

Voor de vier typen data genoemd in voorgaande paragraaf gelden verschillende randvoorwaarden. De categorieën IT beheersmaatregelen die minimaal overwogen dienen te worden, zijn in tabel 12 weergegeven met een vink. De categorieën bevatten IT beheersmaatregelen (zowel procedureel als door het systeem afgedwongen). Deze staan in deze sectie nader beschreven.

		Typen data			
		Gegenereerde gegevens	Reproduceerbare gegevens	Ingevoerde Gegevens*	Identificerende gegevens
IT beheersmaatregelen	Wijzigingsbeheer	√	x	x	?
	Databasebeheer	√	√	√	√
	Applicatiebeveiliging	√	x	x	√
	Netwerkbeheer en algemene beveiliging	√	√	√	√

* Ingevoerde gegevens kunnen door menselijk handelen onjuist zijn. IT beheersmaatregelen kunnen dit echter niet voorkomen. Indien de gegevens van belang zijn voor de analyse kunnen deze met externe bronnen worden geverifieerd.

Tabel 3: Algemene IT beheersmaatregelen datagerichte aanpak.

De categorieën per data type dienen overwogen te worden. Afhankelijk van de totstandkoming van data of andere risico analyse kan worden bepaald, geen of beperkte werkzaamheden uit te voeren. Idem aan het traditionele normenkader dient het effect van ontoereikende beheersmaatregelen op het geheel te worden geëvalueerd.

Wijzigingenbeheer

Wijzigingenbeheer omvat het proces van ontwerp tot aan de in productie name van wijzigingen. Indien wijzigingenbeheer niet adequaat is ingericht en nageleefd bestaat het risico dat er fouten ontstaan in systemen. De beheersmaatregelen die van belang zijn bij wijzigingenbeheer zijn:

- Wijzigingen worden geautoriseerd op basis van een ontwerp en impactanalyse;
- Wijzigingen worden adequaat getest in een testomgeving voorafgaand aan de in productie name;
- Wijzigingen worden geaccepteerd;
- Er is functiescheiding binnen het proces van wijzigingenbeheer;
- Het proces van wijzigingenbeheer wordt gecontroleerd.

Het genereren van gegevens is een automatische functie van een systeem. Om een adequate werking van de functie (altijd juist en volledig genereren van data) te borgen, dient wijzigingenbeheer effectief te zijn ingericht. Het is van belang te bepalen in welk systeem (applicatie, database, netwerk/ besturingssysteem) de functionaliteit is geprogrammeerd dat de gegevens genereert. De auditor beoordeelt de functionaliteit op dit systeem.

Een vorm van gegenereerde gegevens die niet reproduceerbaar is, is logging van mutaties. Een geïnterviewde stelt, dat loggingsfunctionaliteit kan worden verstoord door wijzigingen aan de programmatuur. Er bestaat het risico dat de loggingsfunctionaliteit niet alle mutaties opslaat of niet juist/tijdig opslaat. Logging kan configureerbaar zijn of ingebakken in de applicatie. Wijzigingenbeheer is met name van belang wanneer de functionaliteit ingeprogrammeerd is en de gecontroleerde organisatie zelf de bron kan aanpassen. De integriteit van de overige data typen is niet afhankelijk van wijzigingenbeheer. De beheersmaatregelen hoeven in dat geval niet worden overwogen en getoetst.

Databasebeheer

Databasebeheer behelst het beheer van het database management system en de inhoud van de database (toegang en omgang met data). Als databasebeheer niet toereikend wordt uitgevoerd, bestaat het risico op data manipulatie of verlies van data. Data mutaties zijn mogelijk onherleidbaar. Voor databasebeheer gelden de volgende normen:

- Toegang tot beheerprofielen is beperkt tot functionarissen die dit uit hoofde van hun functie nodig zijn.
- Er zijn voldoende maatregelen ingericht om ongeautoriseerde toegang te signaleren en te weren.
- Er is een procedure voor het muteren van data.
- Belangrijke data mutaties worden gelogd.
- Er vindt monitoring plaats op accounts met hoge rechten.

De categorie databasebeheer betreft normen die – indien effectief – het risico op manipulatie (onjuistheid) en verwijdering (onvolledig) van data. Dit is derhalve van toepassing op elke data type.

Een geïnterviewde stelt, dat als iedereen binnen een organisatie schrijftoegang heeft tot de database de integriteit in geding is. Gebruikers hebben namelijk een vrijbrief tot het manipuleren en verwijderen van data. Netwerkbeheer is in sommige gevallen verweven met databasebeheer. Met name wanneer het mogelijk is met hoge rechten op netwerkniveau toegang tot de databaseserver en database management systeem (DBMS) te verkrijgen, dient netwerkbeheer getoetst te worden. Als de database niet via netwerktoegangspaden kan worden verkregen, is het niet noodzakelijk om het netwerkbeheer en -beveiliging te toetsen.

Applicatiebeveiliging
Applicatiebeveiliging betreft wachtwoordinstellingen en beheerfuncties van een applicatie waarmee gebruikers onherleidbare mutaties kunnen doorvoeren. Als applicatiebeveiliging niet voldoende is ingericht, bestaat het risico op ongeautoriseerd gebruik van accounts en/of onherleidbare mutaties. Voor applicatiebeveiliging gelden de volgende normen:
- Voldoende maatregelen zijn ingericht om ongeautoriseerde applicatietoegang en gebruik te weren.
- Het aantal gebruikers met beheerfuncties waarmee data onherleidbaar kan worden gemuteerd is beperkt.

Identificerende gegevens zijn afhankelijk van adequaat ingerichte applicatiebeveiliging. Dit geeft redelijke mate van zekerheid dat accounts gebruikt worden door de eigenaar en borgt derhalve de juistheid van de data.

Applicatiebeveiliging is een voorwaarde om met redelijke mate van zekerheid te kunnen stellen dat gebruikersaccounts door de rechtmatig eigenaar wordt gebruikt. Daarnaast geeft het inzicht in de mate waarin er beheerfuncties zijn waarmee onherleidbare mutaties kunnen worden uitgevoerd. Een belangrijke afweging is dan of dit effect heeft op de data die gebruikt wordt als input voor de analyse. Een voorbeeld hiervan is de utility diagnostics functie in Oracle waarbij gebruikers data kunnen aanpassen zonder dat de laatste mutatiedatum wordt bijgewerkt en de gebruikersnaam niet wordt gelogd. Een ander voorbeeld is het aan en uit kunnen zetten van logging zonder dat dit wordt geregistreerd in de logging. In deze gevallen is het belangrijk te bepalen in hoeverre gebruik dan wel misbruik wordt gemaakt van deze functies. Als de applicatie op basis van single sign on functioneert, wordt netwerkbeheer en –beveiliging tevens randvoorwaardelijk om de authenticatie van gebruikers te kunnen bepalen.

Netwerkbeheer en -beveiliging
De beveiliging van de IT omgeving en het beheer ervan dient adequaat te zijn ingericht. Als de beveiliging zwak is en het beheer onzorgvuldig, kan misbruik gemaakt worden van netwerkaccounts met hoge rechten. Hiermee kan mogelijk toegang verkregen worden tot de database van een informatiesysteem. Voor netwerkbeheer en -beveiliging gelden de volgende normen:
- Voldoende maatregelen zijn ingericht om ongeautoriseerde netwerktoegang te weren.
- Er zijn richtlijnen en deze worden toegepast voor het beveiligen van de IT omgeving.

- Toegang tot beheerprofielen is beperkt tot functionarissen die dit uit hoofde van hun functie nodig zijn.
- Er vindt monitoring plaats op accounts met hoge rechten.

Afhankelijk van de beveiliging van de database zelf, dient netwerkbeheer en -beveiliging te worden beoordeeld. Beheersmaatregelen op netwerkniveau kunnen nodig zijn als deze ongeautoriseerde toegang op tot de database kunnen voorkomen.

Daarnaast kan de applicatie gebruik maken van het authenticatiemechanisme van het netwerk (single sign on). Indien de beheersmaatregelen op netwerkniveau direct bijdragen aan applicatiebeveiliging, borgen de maatregelen de juistheid van data.

5 De gevolgen van een datagerichte aanpak

5.1 De IT auditor

Commissie VISIE2020 heeft in september 2014 een rapport uitgebracht aan het bestuur van de Nederlandse Orde van Register EDP Auditors (NOREA) over de teloorgang van de IT auditor. Dit is te wijten aan de veranderende IT wereld waarin de IT auditor conservatief blijft. Dit geldt ook voor de rol van IT audit binnen het kader van de jaarrekeningcontrole.

De rol van de IT auditor verandert bij een datagerichte aanpak. Het normenkader van de algemene IT beheersmaatregelen is beperkter dan bij een traditionele aanpak en de reguliere werkzaamheden ten aanzien van het beoordelen van applicatiefunctionaliteit nemen af. Geïnterviewden hebben een eenduidige mening dat dit niet het einde van de IT auditor is. Er is een verschuiving van de verantwoordelijkheden, waarbij de IT auditor zich meer richt op gegevensgerichte werkzaamheden (data analyse) dan systeemgerichte werkzaamheden. Hierdoor moet de functie van IT auditor en accountant nog verder integreren. Over de invulling hiervan is verdeeldheid:

- Een nauwere samenwerking van beide beroepen en overname van werkzaamheden door de accountant van de IT auditor.
- Volledige uitvoer van de aanpak voor data analyse zoals beschreven in paragraaf 4.1.

De IT auditor zal minder routinematig werken doordat hij meer acteert op basis van risico analyse. De risico's ten aanzien van de jaarrekeningcontrole worden vertaald naar een aanpak voor data analyse. De risico's ten aanzien van de data worden vertaald naar beheersmaatregelen om de data te valideren.

Om een goede data analyse te kunnen uitvoeren moet de organisatie doorgelicht worden. Daarnaast moet de IT auditor de taal van de accountant spreken om de juiste data uit het systeem te downloaden. Een verschil in perceptie van datavelden die op elkaar lijken (een effectieve datum is anders dan een invoerdatum) is een valkuil. De rol van de IT auditor zal hierdoor verder in geïntegreerd moeten worden met die van de accountant. Om de juiste analyses te kunnen bepalen is ook gegronde kennis van het accountancyberoep nodig.

Dit onderzoek wijst uit dat voor het verantwoorden van een datagerichte aanpak een hoge mate van IT kennis nodig is. De praktijk leert dat de accountant een gebrek aan IT kennis heeft en het hiaat lijkt te groot om de IT audit werkzaamheden over te nemen.

Een ander groot verschil is de primaire insteek van controleaanpak. Momenteel is het uitgangspunt te steunen op applicatiecontroles. Wanneer sprake is van ineffectieve applicatiecontroles of ineffectieve IT beheersmaatregelen worden additionele werkzaamheden uitgevoerd door middel van data analyse. Bij

een datagerichte controle wordt data primair geanalyseerd. Door risk-based te analyseren kunnen resultaten aan het licht brengen dat de inrichting of werking van de applicatie ontoereikend is. De onderbouwing kan aan de klant worden gepresenteerd en biedt de kans om de klant te helpen bij het herinrichten van haar interne beheersing.

5.2 Oordeel over de interne beheersing: continuïteit en SOx

Wagenaar (2013) stelt dat interne beheersmaatregelen middels data analyse kunnen worden getoetst. Teeter en Brennan (2008) spreken dit tegen door te stellen dat de keuze voor de uit te voeren controles gebaseerd moet zijn op risico's. De praktijk en dit onderzoek wijzen uit dat interne beheersmaatregelen niet getoetst kunnen worden middels data analyse. Data analyse toont alleen aan of en in welke mate een risico zich heeft gemanifesteerd. Dit toont niet direct aan dat een specifieke beheersmaatregel heeft gewerkt. Het kan wel aantonen dat ingerichte maatregelen niet misbruikt of omzeild zijn. Het kan ook zijn dat gebruikers van het systeem correcties hebben doorgevoerd. Data analyse is dus in geen geval het toetsen van interne beheersmaatregelen, maar het uitvoeren van analytische werkzaamheden.

Met de toepassing van data analyse wordt de werking van de controls dus niet getoetst. Als controls van een organisatie niet worden getoetst, kan de controlerend accountant geen uitspraak doen over een adequate en continue werking van de interne beheersmaatregelen.

Vanuit het perspectief van de Sarbanes Oxley wet (SOx) lijkt een datagerichte controle niet haalbaar om uitspraak te kunnen doen over het control framework van een organisatie. Als accountant wordt een control afwijking gedocumenteerd als data analyse wordt toegepast. Vanuit de audit methodologie verdient het echter nog wel de nodige aandacht, want direct testing wordt wel gezien als gangbare manier van toetsen. Direct testing is het vaststellen dat een x-aantal transacties op een juiste en consistente wijze het proces c.q. de control hebben doorlopen. Het te controleren aantal transacties is afhankelijk van het volume: 10% met een maximum van 25 items. Direct testing kan dan ook worden vertaald tot een beperkte vorm van data analyse.

De SOx wet zal derhalve doorontwikkeld moeten worden om aan te kunnen sluiten bij de hedendaagse ontwikkelingen. Een oplossing om data analyse toe te passen in de jaarrekeningcontrole en toch een uitspraak te kunnen doen over het controle framework van de organisatie, is het inrichten van data analyse controls bij de betreffende organisatie. Continuous monitoring is een vorm van continue data analyse waarbij een organisatie periodiek afwijkingen controleert.

Veel organisaties hebben deze vorm van auditing nog niet ingevoerd. Een afgezwakte vorm van continuous monitoring komt wel voor bij veel organisaties, waarbij maandelijkse controles zijn ingericht om bijvoorbeeld de facturatie te controleren.

Vanuit een jaarrekeningperspectief is de accountant verantwoordelijk het continuïteitsaspect in acht te nemen bij de accountantscontrole. De NBA Standaard 570 (2012) definieert de continuïteitsveronderstelling als volgt:

> "Onder de continuïteitsveronderstelling wordt een entiteit geacht haar bedrijfsactiviteiten in de voorzienbare toekomst voort te zetten. Financiële overzichten voor algemene doeleinden worden opgesteld op basis van continuïteit tenzij het management voornemens is de entiteit te liquideren of de activiteiten te staken dan wel hiervoor geen realistisch alternatief heeft. Financiële overzichten voor bijzondere doeleinden kunnen al dan niet worden opgesteld in overeenstemming met een stelsel inzake financiële verslaggeving waarvoor de continuïteitsbasis relevant is (bijvoorbeeld in bepaalde rechtsgebieden is de continuïteitsbasis niet van belang voor bepaalde financiële overzichten die zijn opgesteld op basis van een fiscale grondslag). Wanneer het hanteren van de continuïteitsveronderstelling passend is, worden activa en passiva opgenomen onder de veronderstelling dat de entiteit in staat zal zijn haar activa te realiseren en haar verplichtingen af te wikkelen bij een normaal verloop van haar bedrijfsactiviteiten."

De veronderstelling heeft geen directe betrekking heeft op de continuïteit van bedrijfsprocessen, maar meer op de financiële positie van de organisatie. Hierdoor kan de accountant bij een datagerichte controle in voldoende mate uitspraak doen over de continuïteit. Integrale data analyse maakt de continuïteit van een organisatie nog beter inzichtelijk met behulp van visuele trend analyses, correlaties en marge analyses.

5.3 Aftekenen op jaarrekening

Bij een datagerichte controle steunt de accountant in hoge mate op de integriteit van data. Daarmee is het in hoge mate afhankelijk van de kennis van de IT auditor. De IT auditor moet namelijk niet alleen bepalen of een analyse haalbaar en de data betrouwbaar is, maar moet ook de juiste data uit het systeem te downloaden.

Er is geen consensus over de vraag of een jaarrekening bij een datagerichte controle ook door een RE moet worden afgetekend. Er zijn twee meningen:

- In principe is er één iemand verantwoordelijk voor het tekenen van de jaarrekening. Deze roept de hulp in van specialisten waar nodig en bepaalt of deze kundig genoeg zijn. Derhalve is zijn handtekening als eindverantwoordelijke voldoende.
- Een accountant heeft een beperkte kennis van IT. Als in hoge mate wordt gesteund op IT, dan zou het een waardevolle toevoeging zijn om een RE af te laten tekenen.

Ondanks dat het belang van het oordeel van de IT auditor toeneemt, vindt een groep dat één handtekening van de eindverantwoordelijk accountant voldoende is. Deze geeft hiermee aan dat hij/zij en/of specialisten voldoende werkzaamheden hebben uitgevoerd om het gegeven oordeel te onderbouwen. Een handtekening van de RE is derhalve niet nodig.

6 Conclusie

De toekomst van de IT auditor verandert. De huidige standaarden voldoen niet meer of zijn niet langer relevant. De IT auditor zal in het kader van de jaarrekeningcontrole meer een data expert worden dan een applicatie expert zoals we die nu kennen.

De betrokkenheid van de IT auditor binnen de planningsfase van de jaarrekeningcontrole zal toenemen. De accountant wordt namelijk in hogere mate afhankelijk van de kennis en kunde van de IT auditor om de juiste controles te bepalen teneinde risico's te onderzoeken. Dit houdt tevens in dat de IT auditor voldoende accountancy kennis nodig heeft om van optimale waarde te kunnen zijn. De IT auditor heeft bij een datagerichte controle ook diepgaande(re) kennis nodig van data en de databases van applicaties. Het is niet alleen zaak de juiste data op een adequate manier vanuit het systeem te downloaden, maar ook om deze data op een adequate wijze te valideren.

Er is sprake van vier verschillende typen data, te weten (1) gegenereerde gegevens, (2) reproduceerbare gegevens, (3) ingevoerde gegevens en (4) identificerende gegevens. Per gegevensgroep dienen bepaalde maatregelen in overweging worden genomen om de juistheid en volledigheid hiervan te valideren. Continuïteitsmaatregelen maken geen deel meer uit van het normenkader en wijzigingenbeheer is mogelijk alleen van toepassing op gegenereerde gegevens. Daarnaast is het belang van maatregelen op applicatieniveau duidelijke verschoven naar maatregelen op databaseniveau. Additioneel kunnen – afhankelijk van

de situatie – acties nodig zijn om de data te valideren, zoals het genereren van data in het bijzijn van de accountant, querybeoordelingen of aansluiting met externe bronnen.

IT ontwikkelingen als cloud computing en datawarehousing beïnvloeden de nieuwe manier van werken niet, maar zijn wel waard om te overwegen in de aanpak voor datavalidatie. Hedendaagse IT audits steunen in bepaalde mate op een zogenaamde ISAE 3402 of SOC verklaring. Dit verandert niet bij een datagerichte aanpak. Indien de data afkomstig is uit een datawarehouse, dient het datawarehouse en mogelijk ook de bron van het datawarehouse onderwerp van onderzoek te zijn. Het is daarom aan te bevelen data direct uit de bron te downloaden.

Als de IT auditor geen uitspraak kan doen over de betrouwbaarheid van gegevens, dient de accountant kennis te nemen van een verhoogd risico ten aanzien van de getrouwheid van de financiële cijfers. Diepgaande en aanvullende analyses van data dienen plaats te vinden. Een volledig datagerichte controle lijkt ook niet mogelijk en zal er altijd een interne beheersing omgeving blijven bestaan die complementair is aan data analyses. De grijze gebieden die niet geverifieerd of gecontroleerd kunnen worden door de accountant, dienen gekenmerkt te worden in een controleverklaring met beperking.

Bij een datagerichte controle wordt in mindere mate gesteund op de interne processen. Het continuïteitsaspect wordt derhalve niet op procesniveau, maar op integraal transactieniveau bepaald. Echter sommige organisaties verstrekken een in control statement over hun interne beheersing. De accountant kan hier dan geen mening over vormen, tenzij zij additioneel de controls van de organisatie toetst. De accountancy kan data analyse dus wel omarmen, maar de volwassenheid van de klant dient ook toe te nemen door bijvoorbeeld de introductie van continuous monitoring. Anderzijds lijkt het nodig dat de visie van toezichthoudende instanties, maar ook wetgeving als Sarbanes-Oxley zich aanpassen naar de nieuwe situatie.

Een datagerichte aanpak leidt niet direct tot een vereiste om de jaarrekening door een RE te laten tekenen. De accountant steunt echter wel in verhoogde mate op het oordeel van de IT auditor, waar de accountant mogelijk zelf amper of geen beeld heeft of de verrichte werkzaamheden adequaat zijn.

7 Literatuurlijst

Ackoff, 1989, "From Data to Wisdom", Journal of Applied Systems Analysis,
Volume 16, 1989

AFM, 2013, Rapport naar aanleiding van AFM-onderzoek naar kwaliteit accountantscontrole en stelsel van kwaliteitsbeheersing en -bewaking bij negen OOB-vergunninghouders,
http://www.afm.nl/~/media/Files/accountants/2013/onderzoek-niet-oob-samenvatting.ashx

Biene-Hershey, 1997, "IT audit verdringt EDP audit",
http://www.computable.nl/artikel/ict_topics/ictbranche/1306962/2379258/itaudit-verdringtedpaudit.html

Commissie Visie2020, 2014, Hoe blijft de register IT-auditor (RE) van betekenis?,
http://www.norea.nl/readfile.aspx?ContentID=81012&ObjectID=1226619&Type=1&File=0000041910_Eindrapportage%20commissie%20VISIE2020.pdf

Deckers & van Kollenburg, 2002, Elementaire theorie accountantscontrole, Noordhoff Uitgevers B.V.

EY, 2014, Global Audit Methodolgy.

Frielink & De Heer, 1987, Leerboek accountantscontrole / 2a, De algemene controle, typologie accountantscontrole in het kader van de algemene controle, Stentfert Kroese

Knechel, 2007, The business risk audit: Origins, obstacles and opportunities. Accounting, Organizations and Society, 383-408.

NBA, 2012, https://www.nba.nl/HRAweb/HRA1A/201201/html/46986.htm

NBA, 2015, Het verhaal achter de controle, https://www.nba.nl/Documents/Publicaties-downloads/2015/NBA-onderzoek-Accountant-in-de-AvA-Het-verhaal-achter-de-controle.pdf

NV COS 200, 2012, https://www.nba.nl/HRAweb/HRA1A/201201/html/46982.htm

Teeter & Brennan, 2008, Aiding the Audit: Using the IT Audit as a Springboard for Continuous Controls Monitoring.

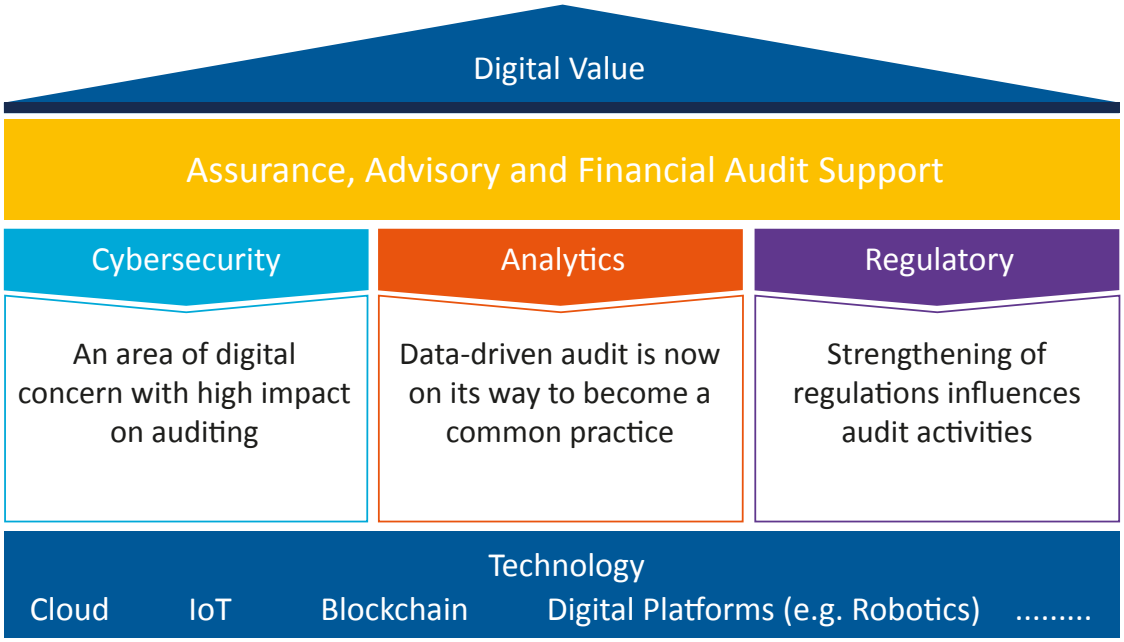
Starreveld, 2002, Bestuurlijke Informatieverzorging, Deel I, Algemene Grondslagen.

University of Washington, 2013, http://f2.washington.edu/fm/fa/internal-controls

Van Praat en Suerink, 2004, Inleiding EDP-auditing, ten Hagen Stam, ISBN 9044007599

Wagenaar, 2013, Methodiek voor gebruik data-analyse ter verbetering kwaliteit bij de jaarrekeningcontrole, http://www.vurore.nl/images/vurore/downloads/1082_Def_Lex_Wagenaar.pdf

HOUSE OF IT-AUDITING



9 789082 851700